

# Handbook of Research on Theory and Practice of Financial Crimes

Abdul Rafay

*University of Management and Technology, Pakistan*

A volume in the Advances in Finance, Accounting,  
and Economics (AFAE) Book Series



Published in the United States of America by

IGI Global  
Business Science Reference (an imprint of IGI Global)  
701 E. Chocolate Avenue  
Hershey PA, USA 17033  
Tel: 717-533-8845  
Fax: 717-533-8661  
E-mail: [cust@igi-global.com](mailto:cust@igi-global.com)  
Web site: <http://www.igi-global.com>

Copyright © 2021 by IGI Global. All rights reserved. No part of this publication may be reproduced, stored or distributed in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher. Product or company names used in this set are for identification purposes only. Inclusion of the names of the products or companies does not indicate a claim of ownership by IGI Global of the trademark or registered trademark.

Library of Congress Cataloging-in-Publication Data

Names: Rafay, Abdul, 1973- editor.

Title: Handbook of research on theory and practice of financial crimes /  
Abdul Rafay, editor.

Description: Hershey, PA : Business Science Reference, [2021] | Includes bibliographical references and index. | Summary: "This book examines the emergence and practice of black money and financial crime, including terrorism financing, money laundering, and corporate frauds"-- Provided by publisher.

Identifiers: LCCN 2020009675 (print) | LCCN 2020009676 (ebook) | ISBN 9781799855675 (hardcover) | ISBN 9781799855682 (paperback) | ISBN 9781799855699 (ebook)

Subjects: LCSH: Commercial crimes. | Fraud.

Classification: LCC HV6768 .T539 2021 (print) | LCC HV6768 (ebook) | DDC 364.16/8--dc23

LC record available at <https://lcn.loc.gov/2020009675>

LC ebook record available at <https://lcn.loc.gov/2020009676>

This book is published in the IGI Global book series Advances in Finance, Accounting, and Economics (AFAE) (ISSN: 2327-5677; eISSN: 2327-5685)

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: [eresources@igi-global.com](mailto:eresources@igi-global.com).



# Advances in Finance, Accounting, and Economics (AFAE) Book Series

Ahmed Driouchi  
Al Akhawayn University, Morocco

ISSN:2327-5677  
EISSN:2327-5685

## MISSION

In our changing economic and business environment, it is important to consider the financial changes occurring internationally as well as within individual organizations and business environments. Understanding these changes as well as the factors that influence them is crucial in preparing for our financial future and ensuring economic sustainability and growth.

The **Advances in Finance, Accounting, and Economics (AFAE)** book series aims to publish comprehensive and informative titles in all areas of economics and economic theory, finance, and accounting to assist in advancing the available knowledge and providing for further research development in these dynamic fields.

## COVERAGE

- Entrepreneurship in Accounting and Finance
- E-finance
- Economics of Innovation and Knowledge
- Borrowing and Lending
- International Trade
- Ethics in Accounting and Finance
- Applied Accounting
- Evidence-Based Studies
- Taxes
- Economic Policy

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at [Acquisitions@igi-global.com](mailto:Acquisitions@igi-global.com) or visit: <http://www.igi-global.com/publish/>.

The *Advances in Finance, Accounting, and Economics (AFAE) Book Series* (ISSN 2327-5677) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, [www.igi-global.com](http://www.igi-global.com). This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit <http://www.igi-global.com/book-series/advances-finance-accounting-economics/73685>. Postmaster: Send all address changes to above address. © 2021 IGI Global. All rights, including translation in other languages reserved by the publisher. No part of this series may be reproduced or used in any form or by any means – graphics, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems – without written permission from the publisher, except for non commercial, educational use, including classroom teaching purposes. The views expressed in this series are those of the authors, but not necessarily of IGI Global.

## Titles in this Series

For a list of additional titles in this series, please visit: [www.igi-global.com/book-series](http://www.igi-global.com/book-series)

### ***Comparative Research on Earnings Management, Corporate Governance, and Economic Value***

Elisabete S. Vieira (University of Aveiro, Portugal) Mara Madaleno (University of Aveiro, Portugal) and Graça Azevedo (University of Aveiro, Portugal)

Business Science Reference • © 2021 • 433pp • H/C (ISBN: 9781799875963) • US \$215.00

### ***Examining the Intersection of Circular Economy, Forestry, and International Trade***

Badri Narayanan Gopalakrishnan (University of Washington, USA) Taranjeet Duggal (Amity University, India) and Tavishi Tewary (Amity University, India)

Business Science Reference • © 2021 • 315pp • H/C (ISBN: 9781799849902) • US \$195.00

### ***Influence of FinTech on Management Transformation***

Amira Sghari (Faculty of Economics and Management, University of Sfax, Tunisia) and Karim Mezghani (Al Imam Mohammad Ibn Saud Islamic University, Saudi Arabia & University of Sfax, Tunisia)

Business Science Reference • © 2021 • 273pp • H/C (ISBN: 9781799871101) • US \$215.00

### ***Handbook of Research on Institutional, Economic, and Social Impacts of Globalization and Liberalization***

Yilmaz Bayar (Bandirma Onyedi Eylul University, Turkey)

Information Science Reference • © 2021 • 699pp • H/C (ISBN: 9781799844594) • US \$445.00

### ***Bridging Microeconomics and Macroeconomics and the Effects on Economic Development and Growth***

Pantelis C. Kostis (National and Kapodistrian University of Athens, Greece)

Business Science Reference • © 2021 • 340pp • H/C (ISBN: 9781799849339) • US \$195.00

### ***Machine Learning Applications for Accounting Disclosure and Fraud Detection***

Stylianios Papadakis (Hellenic Mediterranean University, Greece) Alexandros Garefalakis (Hellenic Mediterranean University, Greece) Christos Lemonakis (Hellenic Mediterranean University, Greece) Christiana Chimonaki (University of Portsmouth, UK) and Constantin Zopounidis (School of Production Engineering and Management, Technical University of Crete, Greece & Audencia Business School, France)

Business Science Reference • © 2021 • 270pp • H/C (ISBN: 9781799848059) • US \$225.00

### ***Corporate Governance and Its Implications on Accounting and Finance***

Ahmad Alqatan (University of Portsmouth, UK) Khaled Hussainey (University of Portsmouth, UK) and Hichem Khelif (University of Sfax, Tunisia)

Business Science Reference • © 2021 • 425pp • H/C (ISBN: 9781799848523) • US \$195.00



701 East Chocolate Avenue, Hershey, PA 17033, USA

Tel: 717-533-8845 x100 • Fax: 717-533-8661

E-Mail: [cust@igi-global.com](mailto:cust@igi-global.com) • [www.igi-global.com](http://www.igi-global.com)



*This handbook of research is dedicated to **Dr. Hafeez Ahmed Pasha**, a person of impeccable integrity and a visionary economist/social scientist in Pakistan. His scholarly and practical contribution in the respective fields made him a person of great depth and integrity.*

He holds Master's degree from the University of Cambridge (UK) and a PhD from Stanford University (USA). Internationally, he served as a United Nations Assistant Secretary General and the director of the Regional Bureau for Asia and the Pacific of UNDP (2001-2007). In Pakistan, he served as the Federal Minister for Finance and Economic Affairs, Minister of Education, Federal Commerce Minister and Deputy Chairman of the Planning Commission. He was also the Vice-Chancellor of the University of Karachi, Dean and Director of the Institute of Business Administration and Beaconhouse National University (BNU) in Pakistan. Currently he is the Professor Emeritus and is heading the Center for Public Policy at BNU.

He has published over 150 books and articles in the fields of governance, public finance, urban and regional economics, poverty and social development, industry, energy economics, etc. He is also a regular guest speaker at seminars organized around the globe by academic institutions, multilateral and bilateral financial institutions and NGOs.

## Editorial Advisory Board

Philippe Adair, *Université Paris-Est Créteil, France*  
Fábio Albuquerque, *Instituto Politécnico de Lisboa, Portugal*  
Mirjana Pejić Bach, *University of Zagreb, Croatia*  
Robert Beeres, *Netherlands Defense Academy, The Netherlands*  
Andy Borchers, *Lipscomb University, USA*  
Dickson K. W. Chiu, *The University of Hong Kong, Hong Kong*  
Maurice Dawson Jr., *Illinois Institute of Technology, USA*  
Christian de Peretti, *Ecole Centrale de Lyon, France*  
Rajendra Parsad Gunputh, *University of Mauritius, Mauritius*  
Laura L. Hansen, *Western New England University, USA*  
Mehboob ul Hassan, *King Saud University, Saudi Arabia*  
Amir Kia, *Utah Valley University, USA*  
Hazik Mohamed, *Stellar Consulting Group, Singapore*  
El Habib Nfaoui, *Sidi Mohamed Ben Abdellah University, Morocco*  
Nikolay Nikolov, *Central Election Commission, Bulgaria*  
John Winterdyk, *Mount Royal University, Canada*  
Sibo Yan, *KPMG LLC, UK*  
İsmail Yıldırım, *Hitit University, Turkey*

# List of Contributors

<b>Afzal, Ayesha</b> / <i>Lahore School of Economics, Pakistan</i> .....	62
<b>Albuquerque, Fábio</b> / <i>Instituto Politécnico de Lisboa, Portugal</i> .....	397
<b>Asadov, Alam I.</b> / <i>Prince Sultan University, Saudi Arabia</i> .....	271
<b>Asif, Aiman</b> / <i>Lahore School of Economics, Pakistan</i> .....	62
<b>Beeres, Robert</b> / <i>Netherlands Defence Academy, The Netherlands</i> .....	49
<b>Bohra, Narendra S.</b> / <i>Graphic Era University, India</i> .....	293
<b>Bollen, Myriame</b> / <i>Netherlands Defence Academy, The Netherlands</i> .....	49
<b>Cassiano Neves, Julija</b> / <i>Instituto Politécnico de Lisboa, Portugal</i> .....	397
<b>Dawson, Maurice</b> / <i>Illinois Institute of Technology, USA</i> .....	506
<b>Defosse, Delphine</b> / <i>Northumbria University, UK</i> .....	453
<b>Diodati, Jason</b> / <i>Mount Royal University, Canada</i> .....	477
<b>Esen, M. Fevzi</b> / <i>University of Health Sciences, Turkey</i> .....	313
<b>Güzel, Simla</b> / <i>Namik Kemal University, Turkey</i> .....	381
<b>Hamid, Kabir Tahir</b> / <i>Bayero University, Nigeria</i> .....	250
<b>Hansen, Laura Pinto</b> / <i>Western New England University, USA</i> .....	132
<b>Haron, Md Harashid</b> / <i>Universti Sains Malaysia, Malaysia</i> .....	196
<b>Hu, Yingzi</b> / <i>Independent Researcher, China</i> .....	172
<b>Karacaer Ulusoy, Merve</b> / <i>Ankara Yildirim Beyazit University, Turkey</i> .....	80
<b>Kurawa, Junaidu Muhammad</b> / <i>Bayero University, Nigeria</i> .....	196, 250
<b>Lawal, Sagir</b> / <i>Nigeria Police Academy, Nigeria</i> .....	250
<b>Leonard, Brian</b> / <i>Civil Rights University, USA</i> .....	506
<b>Morshed, Anika</b> / <i>International Islamic University Chittagong, Bangladesh</i> .....	428
<b>Nakitende, Marie G.</b> / <i>Uganda Martyrs University, Uganda</i> .....	21
<b>Nakitende, Marie Goretti</b> / <i>Uganda Martyrs University, Uganda</i> .....	525
<b>Nikolov, Nikolay Ivanov</b> / <i>Central Election Commission, Bulgaria</i> .....	105
<b>Oke, Tayo</b> / <i>Afe Babalola University, Nigeria</i> .....	39, 525
<b>Rafay, Abdul</b> / <i>University of Management and Technology, Pakistan</i> .....	21, 172
<b>Rashid, Md. Harun Ur</b> / <i>International Islamic University Chittagong, Bangladesh</i> .....	428
<b>Sethi, Mahak</b> / <i>Graphic Era University, India</i> .....	293
<b>Siddik, Md. Nur Alam</b> / <i>Begum Rokeya University, Rangpur, Bangladesh</i> .....	236
<b>Singh, Shailendra</b> / <i>Capital Market Consultants, India</i> .....	332
<b>Szakonyi, Annamaria</b> / <i>Saint Louis University, USA</i> .....	506
<b>Trad, Antoine</b> / <i>Institute of Business and Information Systems Transformation Management, France</i> .....	525
<b>Tuncali Yaman, Tutku</b> / <i>Beykent University, Turkey</i> .....	313

<b>Umar, Umar Habibu</b> / <i>Universiti Brunei Darussalam, Brunei</i> .....	196
<b>Ünlü, Hülya</b> / <i>Cankiri Karatekin University, Turkey</i> .....	80
<b>van Lieshout, Jan</b> / <i>Netherlands Defence Academy, The Netherlands</i> .....	49
<b>Vousinas, Georgios Loukas</b> / <i>National Technical University of Athens, Greece</i> .....	1
<b>Walker-Munro, Brendan</b> / <i>Swinburne University, Australia</i> .....	356
<b>Wanyama, Simeon</b> / <i>Uganda Martyrs University, Uganda</i> .....	149
<b>Waseem, Maimoona</b> / <i>University of Management and Technology, Pakistan</i> .....	21, 172
<b>Winterdyk, John</b> / <i>Mount Royal University, Canada</i> .....	477
<b>Yu, Poshan</b> / <i>Soochow University, China</i> .....	172
<b>Yücel, Elif</b> / <i>Bursa Uludag University, Turkey</i> .....	218

# Table of Contents

<b>Preface</b> .....	xxiii
----------------------	-------

## **Section 1** **The Theory and Discussion on Financial Crimes**

### **Chapter 1**

Understanding the Financial Fraud: An Extended Model .....	1
<i>Georgios Loukas Vousinas, National Technical University of Athens, Greece</i>	

### **Chapter 2**

Frauds in Business Organizations: A Comprehensive Overview .....	21
<i>Marie G. Nakitende, Uganda Martyrs University, Uganda</i>	
<i>Abdul Rafay, University of Management and Technology, Pakistan</i>	
<i>Maimoona Waseem, University of Management and Technology, Pakistan</i>	

### **Chapter 3**

Powerlessness as the Basis for Financial Crimes: A Brief Overview.....	39
<i>Tayo Oke, Afe Babalola University, Nigeria</i>	

### **Chapter 4**

The Power of Currency: Financial Coercion in the 21st Century .....	49
<i>Robert Beeres, Netherlands Defence Academy, The Netherlands</i>	
<i>Jan van Lieshout, Netherlands Defence Academy, The Netherlands</i>	
<i>Myriame Bollen, Netherlands Defence Academy, The Netherlands</i>	

### **Chapter 5**

Adam's Garden or Eve's? A Gender-Centric Analysis of Corruption Perceptions .....	62
<i>Ayesha Afzal, Lahore School of Economics, Pakistan</i>	
<i>Aiman Asif, Lahore School of Economics, Pakistan</i>	

### **Chapter 6**

Innovation and Corruption in Turkey: "Grease the Wheels" or "Sand the Wheels" .....	80
<i>Hülya Ünlü, Cankiri Karatekin University, Turkey</i>	
<i>Merve Karacaer Ulusoy, Ankara Yildirim Beyazıt University, Turkey</i>	

## Section 2

### Legislation for Financial Crimes

#### Chapter 7

- Conflict of Interest for Corruption and Abuse of Public Power: The Case of European Legislation..... 105  
*Nikolay Ivanov Nikolov, Central Election Commission, Bulgaria*

#### Chapter 8

- Regulatory Ambiguity: The Underbelly of Insider Trading ..... 132  
*Laura Pinto Hansen, Western New England University, USA*

#### Chapter 9

- Legislation for Public Procurements and Disposal of Public Assets: The Case of Uganda ..... 149  
*Simeon Wanyama, Uganda Martyrs University, Uganda*

#### Chapter 10

- Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds: The Case of China.... 172  
*Poshan Yu, Soochow University, China*  
*Yingzi Hu, Independent Researcher, China*  
*Maimoona Waseem, University of Management and Technology, Pakistan*  
*Abdul Rafay, University of Management and Technology, Pakistan*

## Section 3

### Frauds and Financial Reporting

#### Chapter 11

- Combating Fraud Through Forensic Accounting: The Case of Islamic Inheritance in Nigeria..... 196  
*Umar Habibu Umar, Universiti Brunei Darussalam, Brunei*  
*Md Harashid Haron, Universti Sains Malaysia, Malaysia*  
*Junaidu Muhammad Kurawa, Bayero University, Nigeria*

#### Chapter 12

- Forensic Audit Practices to Reduce Financial Frauds ..... 218  
*Elif Yücel, Bursa Uludag University, Turkey*

#### Chapter 13

- Forensic Audit for Financial Frauds in Banks: The Case of Bangladesh ..... 236  
*Md. Nur Alam Siddik, Begum Rokeya University, Rangpur, Bangladesh*

#### Chapter 14

- Determinants of Forensic Accounting: The Case of Northwestern States of Nigeria ..... 250  
*Sagor Lawal, Nigeria Police Academy, Nigeria*  
*Junaidu Muhammad Kurawa, Bayero University, Nigeria*  
*Kabir Tahir Hamid, Bayero University, Nigeria*

## **Section 4**

### **Investment Frauds**

#### **Chapter 15**

Financial Scams Through Ponzi Schemes: The Case of CIS Countries .....	271
<i>Alam I. Asadov, Prince Sultan University, Saudi Arabia</i>	

#### **Chapter 16**

Frauds in Unorganized Investment Schemes: The Case of India.....	293
<i>Narendra S. Bohra, Graphic Era University, India</i>	
<i>Mahak Sethi, Graphic Era University, India</i>	

#### **Chapter 17**

Approaches to Detect Securities Fraud in Capital Markets .....	313
<i>M. Fevzi Esen, University of Health Sciences, Turkey</i>	
<i>Tutku Tuncali Yaman, Beykent University, Turkey</i>	

#### **Chapter 18**

Capital Market Frauds: Concepts and Cases.....	332
<i>Shailendra Singh, Capital Market Consultants, India</i>	

## **Section 5**

### **Taxation and Frauds**

#### **Chapter 19**

Tax Enforcement in the Black Economy: Tackling Disruptive Challenge .....	356
<i>Brendan Walker-Munro, Swinburne University, Australia</i>	

#### **Chapter 20**

The Role of Tax Systems in Preventing Corruption .....	381
<i>Simla Güzel, Namık Kemal University, Turkey</i>	

#### **Chapter 21**

Tax Disclosures in Financial and CSR Reporting as a Deterrence for Evasion .....	397
<i>Fábio Albuquerque, Instituto Politécnico de Lisboa, Portugal</i>	
<i>Julija Cassiano Neves, Instituto Politécnico de Lisboa, Portugal</i>	

#### **Chapter 22**

Firms' Characteristics and Tax Evasion .....	428
<i>Md. Harun Ur Rashid, International Islamic University Chittagong, Bangladesh</i>	
<i>Anika Morshed, International Islamic University Chittagong, Bangladesh</i>	

## **Section 6**

### **Technology and Financial Crimes**

#### **Chapter 23**

Regulations for Cybercrimes: The Case of the EU Cybersecurity Act .....	453
<i>Delphine Defossez, Northumbria University, UK</i>	

#### **Chapter 24**

Dark Web: The Digital World of Fraud and Rouge Activities.....	477
<i>Jason Diodati, Mount Royal University, Canada</i>	
<i>John Winterdyk, Mount Royal University, Canada</i>	

#### **Chapter 25**

Dark Web: A Breeding Ground for ID Theft and Financial Crimes.....	506
<i>Annamaria Szakonyi, Saint Louis University, USA</i>	
<i>Brian Leonard, Civil Rights University, USA</i>	
<i>Maurice Dawson, Illinois Institute of Technology, USA</i>	

#### **Chapter 26**

Tech-Based Enterprise Control and Audit for Financial Crimes: The Case of State-Owned Global Financial Predators (SOGFP) .....	525
<i>Antoine Trad, Institute of Business and Information Systems Transformation Management, France</i>	
<i>Marie Goretti Nakitende, Uganda Martyrs University, Uganda</i>	
<i>Tayo Oke, Afe Babalola University, Nigeria</i>	

<b>Compilation of References .....</b>	<b>566</b>
--	------------

<b>About the Contributors .....</b>	<b>638</b>
-------------------------------------	------------

<b>Index.....</b>	<b>646</b>
-------------------	------------



# Detailed Table of Contents

<b>Preface</b> .....	xxiii
----------------------	-------

## **Section 1** **The Theory and Discussion on Financial Crimes**

### **Chapter 1**

Understanding the Financial Fraud: An Extended Model .....	1
<i>Georgios Loukas Vousinas, National Technical University of Athens, Greece</i>	

This chapter aims to elaborate on the theory of fraud by enhancing the existing theories that force people to commit fraud. The chapter reviews the most commonly used and widely accepted models for explaining why people commit fraud: the fraud triangle, the fraud diamond, the fraud scale, and the MICE model. The author argues that these models need to be updated to adapt to the current developments and the ever-growing fraud incidents, both in frequency and severity. The chapter identifies a major element, ego/entitlement, which plays a crucial role in compelling people to commit fraud and builds on the theoretical background to conclude in the formation of the SCORE model, which is graphically depicted in the fraud pentagon. It goes further by adding the factor of collusion for its better application in cases of white-collar crimes.

### **Chapter 2**

Frauds in Business Organizations: A Comprehensive Overview .....	21
<i>Marie G. Nakitende, Uganda Martyrs University, Uganda</i>	
<i>Abdul Rafay, University of Management and Technology, Pakistan</i>	
<i>Maimoona Waseem, University of Management and Technology, Pakistan</i>	

Fraud has been evolving and increasing with the change in the work environment, organizational structures, industrialization, and legislation. Money, greed, manipulation, job pressures, family needs, opportunity, politics, rationalization are the crucial reasons that lead people to behave fraudulently. The purpose of the chapter is to discuss a brief overview of theories of fraud. It presents causes that inspire individuals to commit fraud, methods for identifying fraud, and motives that encourage people to commit fraud. Management must try to eliminate the vulnerabilities that offer criminals the chance to commit fraud. Organizational leaders must be diligent, implement a robust anti-fraud strategy, and discourage all improper practices. Employee performance can also be strengthened through realistic anti-fraud preparation, and conformity with legal and regulatory obligations. Thus, fostering an ethical corporate culture is essential for fraud prevention.

### Chapter 3

Powerlessness as the Basis for Financial Crimes: A Brief Overview .....	39
<i>Tayo Oke, Afe Babalola University, Nigeria</i>	

Scholarly analysis of financial crime, its modus operandi, and the characters involved have almost exclusively been focused on the activities of the elite and the powerful for decades. Recommendations on how to minimise its debilitating impact have always, also, been focused on the elite, the powerful, and the state institutions they control. Corruption and financial crime are the pastime of people at the top only. This overview contends that perpetration of financial crime by the powerless can be just as corrosive and harmful as that perpetrated by the powerful. The quality of criminality and its pervasiveness is as relevant as its quantum and location. Exclusive focus on the higher echelons of financial crime subsumes its roots and significance within society, thereby leading to the lop-sidedness of proposed remedies. This chapter seeks to establish the nexus between low- and high-level financial crime as a way of providing a more holistic view of the depth of its effect, especially in less sophisticated economic environments.

### Chapter 4

The Power of Currency: Financial Coercion in the 21st Century .....	49
<i>Robert Beeres, Netherlands Defence Academy, The Netherlands</i>	
<i>Jan van Lieshout, Netherlands Defence Academy, The Netherlands</i>	
<i>Myriame Bollen, Netherlands Defence Academy, The Netherlands</i>	

This chapter explores the coercive power of currencies. The authors add to the existing literature on two strands. First, within the scope of the chapter, money encompasses all aspects of currency and financial relations – the processes and institutions of financial intermediation (mobilization of savings and allocation of credit) as well as the creation and management of money itself. The authors discuss as to what extent money can be deployed to prevent wars and conflicts, or, in other words, can money serve as a weapon of coercion? The chapter analyzes four scenarios of potential (fictional) financial wars between states. The authors find that, indeed, money yields coercive power. Based on proxies for the size of the economies of a deterring state and its adversary, the chapter shows how the potential impact of financial coercion may be estimated.

### Chapter 5

Adam's Garden or Eve's? A Gender-Centric Analysis of Corruption Perceptions .....	62
<i>Ayesha Afzal, Lahore School of Economics, Pakistan</i>	
<i>Aiman Asif, Lahore School of Economics, Pakistan</i>	

Corruption, or the misuse of public office, has become a major concern for governments in recent years. The purpose of this study is to identify how women, in an economic capacity, influence perception of corruption in a country, and how the relationship changes over time. Female empowerment movements have grown in the past decades, resulting in increased labour force participation of women. This chapter considers 167 countries from 1995 to 2018 to study the relationship. The results suggest that working women in an economy have a significant impact on reducing the perceived level of corruption, from 2007 to 2018, whereas this effect is not as strong in the earlier decade. These findings have implications for policies surrounding female employment. It is suggested that encouraging women to get higher education and become professionals can help curb the levels of corruption, especially in developing countries where corruption is widely prevalent.

## **Chapter 6**

Innovation and Corruption in Turkey: “Grease the Wheels” or “Sand the Wheels” ..... 80

*Hülya Ünlü, Cankiri Karatekin University, Turkey*

*Merve Karacaer Ulusoy, Ankara Yildirim Beyazıt University, Turkey*

In this chapter, one of the important financial crimes and its effect on the innovation success of firms has been investigated for Turkey. The business environment and enterprise performance survey is used to examine how the business perceives informal payments for the period between 2013-2014. The main concern of the chapter is that when corruption is the case, either “sand the wheels” or “grease the wheels” is the result of being unproductive or (even worse) destructive entrepreneurs. Moreover, different corruption levels are estimated and tested by using a PROBIT model. It is suggested that while the “sand the wheels” effect is strong, financial resources should be transferred to the innovation investments rather than corrupt activities. Even though corruption does not show a hindering effect on innovation, the time spent by the managers is the “grease the wheels” effect for innovation.

### **Section 2**

#### **Legislation for Financial Crimes**

## **Chapter 7**

Conflict of Interest for Corruption and Abuse of Public Power: The Case of European

Legislation..... 105

*Nikolay Ivanov Nikolov, Central Election Commission, Bulgaria*

The chapter presents a conflict of interest as a new pioneering measure for combating corruption and abuse of public power. The study is based on an analysis of the conflict of interest legislations of about 15 European countries. European legislators’ legislative decisions on several key criteria relating to conflict of interest have been analyzed. These criteria include the presence or absence of a special law, conflict of interest as a criminal or administrative offense, accountable persons, legal definition, prohibitions, competent authorities and procedures for ascertaining conflict of interest, sanctions, etc. A scientific definition of conflict of interest has also been proposed based on the characteristics of the phenomenon derived from the analysis of the national legislation in force on the European continent. The chapter also outlines the direction in which the phenomenon may develop in national legislations and includes examples of interesting cases of conflict of interest which have arisen in different European countries.

## **Chapter 8**

Regulatory Ambiguity: The Underbelly of Insider Trading ..... 132

*Laura Pinto Hansen, Western New England University, USA*

Ordinarily “black money” is considered a part of illegal transactions involving cash payments. However, in the case of illegal insider trading, illegal profits are often hidden in the purchase of luxury items and financial investments through offshore accounts. Aiding in this particular white-collar crime is the ambiguity of regulation, often dependent on the political whims of whatever party is in office at the time. Adding to the confusion is the fact that in some cases, “insider traders” are acting legitimately, as in the case of senior executives with stock buying options within their compensation or with lower-level employees participating in employee stock ownership programs (ESOPs). Though there are exhaustive ways by which illegal trading information is passed around, there are certain industries, including finance, that lend themselves to greater risk for employee involvement in illegal insider trading. This chapter includes discussions of mergers and acquisitions frenzies, as well as hedge funds and their contributions to illegal insider trading.

## **Chapter 9**

Legislation for Public Procurements and Disposal of Public Assets: The Case of Uganda ..... 149

*Simeon Wanyama, Uganda Martyrs University, Uganda*

This chapter is about corrupt practices in the public procurement cycle. Taking the example of Uganda, it identifies what takes place at each of the stages of public procurement and examines the perspectives of stakeholders regarding alleged corruption, misappropriation, and fraudulent practices during the public procurement process. It also reviews the governance systems that have been put in place to try and stem out these malpractices and ensure proper governance in the administration of public procurement. The research followed a qualitative approach aimed at getting the views of stakeholders and understanding whether what is in place is adhering to the principles of public procurement which foster good governance and value for money. The findings of the study indicate that the perception of the majority of the respondents is that corruption is pervasive in public procurement in Uganda despite good laws, regulations, and guidelines that have been put in place and that it manifests itself at all the stages of public procurement.

## **Chapter 10**

Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds: The Case of China .... 172

*Poshan Yu, Soochow University, China*

*Yingzi Hu, Independent Researcher, China*

*Maimoona Waseem, University of Management and Technology, Pakistan*

*Abdul Rafay, University of Management and Technology, Pakistan*

Internet lending is a unique form of the credit market for bypassing banks in which borrowers generate online microloans without leverage or intermediation from financial institutions. Unlike the UK and the US, the Chinese P2P lending market is broader. Although the regulations concerning P2P lending are more comprehensive since 2015, there remains some regulatory gaps and failures, thus identifying these remaining regulatory gaps can help perfect the regulatory framework. This chapter provides a more detailed analysis and an examination of the Chinese legal framework related to P2P lending and identifying the vacuums in the existing framework. The theoretical contribution is primarily to the implications of the latest development of regulatory changes and the established individual credit reference system in China. Furthermore, the chapter also discovered three new regulatory vacuums (i.e., platform exit, a case report of financial crime, and consumer education), thus concluding with detailed insights on future approach towards perfecting the regulatory framework.

## **Section 3**

### **Frauds and Financial Reporting**

## **Chapter 11**

Combating Fraud Through Forensic Accounting: The Case of Islamic Inheritance in Nigeria..... 196

*Umar Habibu Umar, Universiti Brunei Darussalam, Brunei*

*Md Harashid Haron, Universti Sains Malaysia, Malaysia*

*Junaidu Muhammad Kurawa, Bayero University, Nigeria*

This study examines the potential application of forensic accounting in detecting and preventing of fraudulent activities in the administration of Islamic inheritance in Kano State, Nigeria. Data were collected through semi-structured interviews with some selected experts who are aware of Islamic

inheritance and forensic accounting. Thematic analysis was used. The study established the nature and forms of the fraudulent activities committed in the administration of Islamic inheritance, such as non-compliance with the provision of Islamic inheritance law, hiding some inherited estate, the non-usage of professional valuers and the advice of experts, misappropriation of inherited cash, mismanagement of inherited wealth, etc. The key fraudsters include the eldest heirs, the parents of heirs (particularly mothers), court officials, estate valuers, relatives and the trustees of the deceased. The respondents strongly believe that forensic accounting could be used as a reliable instrument to detect and prevent such forms of fraudulent activities.

## **Chapter 12**

Forensic Audit Practices to Reduce Financial Frauds .....	218
<i>Elif Yücel, Bursa Uludag University, Turkey</i>	

International markets are highly competitive these days due to the globalization of the industry. Companies might manipulate this competition to gain some advantages. Also, technology has been the main force behind business growth in the past decade. The widespread use of technology and globalization also increased financial crimes. Accordingly, the auditing profession has entered into the process of institutionalization and embedded itself within institutions due to the enhanced complexity of frauds, corruption, and manipulations. One of the developments that have been happened in the field of auditing is the emergence of the “forensic auditing” profession. This chapter discusses the conceptual framework of the forensic audit and its essential role in preventing frauds and corruption.

## **Chapter 13**

Forensic Audit for Financial Frauds in Banks: The Case of Bangladesh .....	236
<i>Md. Nur Alam Siddik, Begum Rokeya University, Rangpur, Bangladesh</i>	

Traditional auditing has failed to control the jeopardy of increased financial frauds. Gradually, forensic auditing has been employed by organizations to control such frauds. Nonetheless, there is a dearth of studies examining the effects of forensic auditing on financial frauds. In particular, the impact of forensic auditing on financial frauds in Bangladesh is not examined. This study attempts to fill this gap. Using survey data of 182 respondents, this study applied logistic regression analysis. Findings indicate that forensic auditing has significant positive effects on the detection and prevention of financial fraud occurrences in the banking sector of Bangladesh. Findings also indicate that forensic auditing is competent to diminish financial frauds. Therefore, it is recommended to adopt forensic auditing in the banking sector of Bangladesh.

## **Chapter 14**

Determinants of Forensic Accounting: The Case of Northwestern States of Nigeria .....	250
<i>Sagir Lawal, Nigeria Police Academy, Nigeria</i>	
<i>Junaidu Muhammad Kurawa, Bayero University, Nigeria</i>	
<i>Kabir Tahir Hamid, Bayero University, Nigeria</i>	

This study examined the political and environmental factors as determinants to apply forensic accounting in the North-Western states of Nigeria. The study utilized primary data through the administration of questionnaires. Partial least squares (PLS) path modeling (using smart PLS3 statistical software) was employed for the main analysis. The findings of the study indicated that both political and environmental factors are positively related to applying forensic accounting in these states. The study recommended that

all political office holders and other government personnel should, even with the change of government, use their powers to ensure the right way to move forward and the continuity of state policies to apply forensic accounting. State governments should also provide an enabling environment for the applicability of forensic accounting through the provision of the required infrastructure to carry out the forensic services smoothly.

## **Section 4** **Investment Frauds**

### **Chapter 15**

Financial Scams Through Ponzi Schemes: The Case of CIS Countries ..... 271

*Alam I. Asadov, Prince Sultan University, Saudi Arabia*

This chapter investigates the relationship between financial literacy, financial sector development, and Ponzi schemes in the commonwealth of independent states (CIS) countries. It begins with an overview of the early cases of Ponzi schemes in the CIS countries by examining circumstances which formed fertile ground for the schemes to develop during initial years of independence. The study then scrutinised the situation in the member states during the later years which revealed no improvements. A closer examination of the problem discovered that the main triggers are low level of financial literacy and scarce investment alternatives. The chapter suggests that unless the level of financial literacy is raised and the financial sector is developed, Ponzi schemes will continue to thrive in the region. It concludes by providing some policy recommendations to enhance financial literacy and financial sector development, as well as necessary steps to improve financial regulations.

### **Chapter 16**

Frauds in Unorganized Investment Schemes: The Case of India..... 293

*Narendra S. Bohra, Graphic Era University, India*

*Mahak Sethi, Graphic Era University, India*

Innumerable unorganized collective investment schemes' fraud cases have surfaced over time in India. However, there exists minimal descriptive literary text divulging these scams and frauds, which have drowned away the hard-earned money of millions of people. This chapter has been contributory in identifying the working models, administration, and organization of unorganized collective investment schemes (UCIS), where UCIS frauds remain the keystone of groundwork concerning the cases that have transpired over the last decade in India. The chapter aims to interpret the UCIS working models concerning UCIS fraud cases in India by exploring the various models of frauds adopted by UCIS organizers.

### **Chapter 17**

Approaches to Detect Securities Fraud in Capital Markets ..... 313

*M. Fevzi Esen, University of Health Sciences, Turkey*

*Tutku Tuncali Yaman, Beykent University, Turkey*

Financial markets are vibrant and fragile in terms of structure and mechanism and more prone to risks, failures, and exploitations than the other markets. This motivated the researchers to discuss and analyse the backstage of fraudulent activities in the capital markets. This chapter explains the main characteristics of securities markets and certain types of securities fraud which encompass a wide range of deceptive practices in capital markets. Traditional and modern approaches are reviewed which are used to detect and

prevent fraudulent activities using qualitative and data-driven techniques. It is concluded that investors, market professionals, and regulators seek autonomous data mining techniques to combat securities fraud, especially stock market manipulation.

## **Chapter 18**

Capital Market Frauds: Concepts and Cases..... 332

*Shailendra Singh, Capital Market Consultants, India*

In recent times there has been a significant development in financial markets that include global integration, internet-based trading, and financial innovation to name a few. Now financial markets are more sophisticated, diversified, and internationalized than ever. During the last decade, as a result of the Enron and WorldCom scandals, numerous legislations, amendments, and restructuring policies are introduced across the world. This chapter mainly covers various aspects of capital market frauds, manipulation practices, and country case studies from global financial markets. The chapter also highlights international regulatory frameworks, guidelines, and challenges being faced by the regulatory authorities. Fraud detection mechanisms and opportunities for the future are also discussed.

## **Section 5**

### **Taxation and Frauds**

## **Chapter 19**

Tax Enforcement in the Black Economy: Tackling Disruptive Challenge ..... 356

*Brendan Walker-Munro, Swinburne University, Australia*

The black economy—also called the hidden, covert, underground, grey, illicit, or cash economy—is used to describe the aspect of a country’s economy that is not visibly subject to taxation. However, it is also a useful measure of behavioral disruption to the taxation system, as the scale and tactics of black economy participants vary over time. The purpose of this chapter is to suggest that existing tax policy (where legal constraints alone are used) is insufficient to affect black economy behaviour. It suggests that by adopting responses that are “more than law,” revenue administrations can deploy a more advanced and effective approach to improve tax compliance and can decrease the negative impacts of the black economy.

## **Chapter 20**

The Role of Tax Systems in Preventing Corruption ..... 381

*Simla Güzel, Namık Kemal University, Turkey*

The determinants of corruption have long been an important subject for research in the fields of economics and political science. Corruption was not deemed as a significant issue in the pre-democratic era and has become a serious issue later on. Corruption can be defined as “exploitation of public power to gain private gain.” It is a problem that occurs for various reasons and causes various effects. It may occur due to the occurrence of illegal activities in the political and economic system, as well as due to social and individual moral issues. Corruption has disruptive effects on the functioning of the economic, political, and social system. The aim of this study is to determine the duties of states towards a tax system to combat financial corruption. Corruption in the tax system affects the investment environment negatively, which slows down economic growth.

## **Chapter 21**

Tax Disclosures in Financial and CSR Reporting as a Deterrence for Evasion .....	397
--	-----

*Fábio Albuquerque, Instituto Politécnico de Lisboa, Portugal*

*Julija Cassiano Neves, Instituto Politécnico de Lisboa, Portugal*

This chapter is about the mandatory disclosure of income tax as required by international financial reporting standards (IFRS) and standards issued by Portuguese regulatory bodies. The chapter also elaborates the most relevant disclosures from the perspective of corporate social responsibility (CSR). Furthermore, it highlights the most influential CSR reporting standards to answer the question that whether these standards adequately address the issue of income tax payment as a factor of CSR. Finally, it also reviews the international and Portuguese theoretical and empirical academic research available about income taxes and related subjects, such as disclosures, corporate tax as a CSR matter, and tax aggressiveness of corporations. Future research may be conducted geographical reporting of income tax expense and its relationship with the effective tax rate (ETR) and other independent variables.

## **Chapter 22**

Firms' Characteristics and Tax Evasion .....	428
--	-----

*Md. Harun Ur Rashid, International Islamic University Chittagong, Bangladesh*

*Anika Morshed, International Islamic University Chittagong, Bangladesh*

The study investigates whether the firms' characteristics, including ownership structure, audit, and familiarity affect tax evasion. The study has used the ordinary least square (OLS) to analyze cross-sectional data of 85 countries between 2007 and 2015 collected from the world enterprise survey. The study finds that the domestic, foreign, and government ownership in the firm increases tax evasion, whereas proprietorship and female ownership decreases the tax evasion. Further, the results show that familiar firms with international recognition are less inclined to evade tax. Similarly, the negative relationship between audit and tax evasion implies that the government should make it compulsory to check the financial statements of the firms by the external auditors, which, in turn, reduces the firms' tax evasion. Moreover, the firms that face more financial constraints evade more tax than the firms with access to the bank loan and solvent ones. The tax authorities should also consider reducing the corporate tax rate as the higher tax rates stimulate the firms to evade more tax.

## **Section 6**

### **Technology and Financial Crimes**

## **Chapter 23**

Regulations for Cybercrimes: The Case of the EU Cybersecurity Act .....	453
---	-----

*Delphine Defossez, Northumbria University, UK*

The internet has made all types of information readily available, and this wealth of knowledge has opened up a whole new world of problems: cybercrimes. Despite the enactments of various legislation at both national and international level, cybercriminals are still mostly unpunished. The continued development of new technologies and mechanisms to protect anonymity on the Internet makes finding any response much harder. The lack of a common definition further impedes the finding of a global solution to eradicate the phenomenon. This creates an enforcement gap that allows cybercriminals to operate with near impunity. Over the years, the EU has taken steps to develop an adequate legal framework to strengthen the existing legislation. This chapter discussed that in EU, the adoption of The Cybersecurity Act 2019 would be enough to resolve some of the lingering issues of cybercrimes.



## Chapter 24

Dark Web: The Digital World of Fraud and Rouge Activities..... 477

*Jason Diodati, Mount Royal University, Canada*

*John Winterdyk, Mount Royal University, Canada*

There is a pressing need for understanding blockchain, cybercrime, and dark web-based fraud. As the world continues to turn digital, uses of cryptocurrencies are becoming mainstream. With this technological adoption becoming a reality, crime is adapting to the times. “Click here for free Bitcoin,” “set up an account and earn 100BTC instantly” are merely anecdotal examples of the ways the act of fraud is innovating. Deeper into this proliferation of technology lies the dark web, where your social security and identity may be offered for a small sum as we speak. Blockchain technology fueled dark web marketplaces’ enormous growth, which facilitated identity fraud and many other cybercrimes taking place as we speak. This chapter and its authors aim to provide a thorough yet simplified explanation of these technologies while expressing current trends and theories surrounding dark web fraud trading of fraud guides and the use of social engineering. This chapter aims to explain all aspects of this area of cybercrime for all to understand.

## Chapter 25

Dark Web: A Breeding Ground for ID Theft and Financial Crimes..... 506

*Annamaria Szakonyi, Saint Louis University, USA*

*Brian Leonard, Civil Rights University, USA*

*Maurice Dawson, Illinois Institute of Technology, USA*

The explosion of the internet has given rise to cybercrimes, online identity theft, and fraud. With the internet, these crimes are able to occur anywhere in the world and limitless to whatever selected target. The anonymity of the internet allows criminal activity to flourish, and the number of unsuspecting victims is growing. From script kiddies to nation-states, this new method of internet-enabled crimes has strained governments. This chapter provides insight into how crimes related to online identity theft and fraud are carried out. Examined within this chapter are the evolution of cybercrime, history of identity theft, applications for internet anonymity, and discussion on effects caused by romance scams and data breaches. Finally, recommendations are provided on what organizations and individuals can do to protect themselves against these vicious crimes.

## Chapter 26

Tech-Based Enterprise Control and Audit for Financial Crimes: The Case of State-Owned Global Financial Predators (SOGFP) ..... 525

*Antoine Trad, Institute of Business and Information Systems Transformation Management, France*

*Marie Goretti Nakitende, Uganda Martyrs University, Uganda*

*Tayo Oke, Afe Babalola University, Nigeria*

Due to the global financial and societal crisis, a societal or business transformation project is important. A well-designed financial services automation process is the need of the hour. This automation process depends on measurable critical success factors (CSF) which characterize the progress and evaluation of societal or organizational transformation processes. This chapter discussed in detail the concept of an applied tech-based enterprise control and audit for financial crimes (ECAFC) framework, which is significant for the detection of financial crimes. In the context of financial crimes analysis (FCA), a strategic vision is required for the integration of financial engineering related to risk and controls. This

analysis is fundamental for the enterprise's long-term business longevity and to avoid/combat state organized global financial predators (SOGFP). Moreover, the chapter also highlighted that the detection mechanisms are essential for the enterprise, in order to integrate the local and global economies in a sustainable, controlled, and iterative manner.

<b>Compilation of References .....</b>	<b>566</b>
<b>About the Contributors .....</b>	<b>638</b>
<b>Index.....</b>	<b>646</b>

# Preface

The editing of a *Handbook of Research on Theory and Practice of Financial Crimes* is more exciting and challenging than ever before. The past few decades have been eventful one for the financial crimes especially money laundering and terrorism financing. These terminologies have become a buzzword from G20 to World Economic Forum to global and national economic agendas. Today tackling the financial crimes is being considered as a key issue in developed and developing countries alike. It has enabled the birth of new regulatory regime based on strict compliance, robust processes and technology.

## INTRODUCTION

*“Corruption is the abuse of entrusted power for private gain which eventually hurts everyone who depends on the integrity of people in a position of authority.” (TI, 2021)*

*“Fraud is a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment” (Garner, 2004)*

Regardless of the size of business, industry, or country, financial crime is one of the biggest problems that countries and organizations are facing today at macro and micro level. As a law infringement, financial crimes are the most troublesome obstacles to economic growth and may create catastrophic consequences for the state and the public at large (Azim & Azam, 2016). The legal definition of financial crimes can be different in different countries and regions. The classical form of financial crimes is the white-collar crimes, a term introduced by Sutherland (1983); however, financial crimes cover a wide range of frauds including money laundering, conflict of interest, corruption, bribery, misappropriation of assets, embezzlement, evasion, manipulation of information, false statements, window dressing, stealing, theft, conspiracy, dishonesty, ethical misconduct, extortion, misconduct, shoplifting, digital crimes, forgery, deception, cheating, kickbacks to name a few. According to a survey, 47% of the global companies experienced a fraud in last two years, 6 is the average number of frauds reported per company and total losses due to frauds reported at USD42 billion (PwC, 2020).

## THEORIES OF FINANCIAL CRIMES

Financial Crime Theories have been evolved with the change in the production, work environment, organizational structures, industrialization, and legislation. The relevant fraud theories in this regard are the Fraud Triangle Theory (Cressey, 1953), the Fraud Scale (Albrecht *et al.*, 1984), the Fraud Diamond Theory (Wolfe and Dana, 2004), the MICE Model (Kranacher *et al.*, 2010), the New Fraud Triangle Model (Kassem, R. & Higson, A., 2012), the SCORE Model-The Fraud Pentagon (Vousinas, 2019) and the extended SC(C)ORE Model-The Fraud Hexagon (Vousinas, 2021). The elements discussed in these financial crime theories include Financial Pressure, Rationalization, Opportunity, Capability, Incentive, Integrity, Money, Ideology, Coercion, Ego, Entitlement, Motivation, Stimulus and Collusion. Reasons of repeated frauds are identified as addiction (Potato Chips), a small part of the phenomena (tip of Ice burg), leader's fraudulent behavior (Rotten apple), low-risk fraud potentials (low-hanging fruit) and short memory syndrome (Biegelman, 2013).

## ANTI-CORRUPTION/FRAUD ORGANIZATIONS, CONVENTIONS, AND INDICES/INDICATORS

Eradication of frauds, corruption and all of its forms through a holistic approach of awareness, prevention and enforcement is the need of the hour. Since few years, national and international organizations based in different countries positions themselves in the global fight against fraud and corruption (Table 1). These bodies have been working with the governments to streamline the legal frameworks, regulatory institutions, capacities of state and standardization. Similarly, many international Conventions/Treaties/Standards for Anti-Fraud/Corruption have been signed and implemented (Table 2). Various indices/indicators/frameworks are used to measure the level of financial crimes and related issues (Table 3).

*Table 1. Organizations working for anti-fraud/corruption*

	Organization	Status	Based in	Purpose
1988	Association of Certified Fraud Examiners (ACFE)	World's largest anti-fraud professional organization	US	Provision of Anti-fraud tools, research, training, education and certification.
1993	Transparency International (TI)	Non-governmental organization	Germany	Development of tools, strategies and indices for fighting public and private sector corruption
1999	European Anti-Fraud Office (OLAF)	EU Body	Belgium	Protection of EU financial Interests including EU Budget, corruption and Anti-Fraud legislation
1999	The Group of States against Corruption (GRECO)	Anti-corruption monitoring body of the Council of Europe	France	Capacity building to fight against corruption by monitoring and compliance
2001	Fraud Advisory Panel	Charitable organization	UK	Offering advice and education to the general public on how to mitigate and avoid fraud.
2010	The International Anti-Corruption Academy	International inter-governmental organization	Austria	Training of government officials and professionals about anti-corruption measures

## Preface

*Table 2. International conventions/treaties/standards for anti-fraud/corruption*

Date of Enforcement	Convention/Treaty	Parent Organization	Purpose
1999	Convention on Combating Bribery of Foreign Public Officials in International Business Transactions	OECD	To criminalize all acts of offering or giving bribes to foreign public officials by companies or individuals
2005	United Nations Convention against Corruption (UNCAC)	UNO	To ascertain preventive and punitive measures for cross-border corruption, return of the proceeds of corruption, international asset recovery

*Table 3. Indices/indicators for measuring fraud/corruption*

Year(s)	Indices/ Indicators	Organization	Based in	Purpose
1995	Corruption Perceptions Index (CPI)	Transparency International	Germany	Ascertainment of a country's status based on public sector corruption indicators.
1996-2019	Worldwide Governance Indicators (WGI)	Brookings Institution and World bank	US	Ascertainment of a country's status based on voice & accountability, political stability, absence of violence, government effectiveness, regulatory quality, rule of law and control of corruption.
1999	Bribe Payers Index (BPI)	Transparency International	Germany	Ascertainment of multinational businesses of leading exporting countries to use bribes when operating abroad.
2003	Global Corruption Barometer (GCP)	Transparency International	Germany	Ascertainment of the public opinion about corruption or bribe in a public body.
2005	Fragile State Index (FSI)	Fund for Peace	US	Ascertainment of a country's status using cohesion, social, economic and political indicators like security threat, factionalized elites, group grievances, economic issues, human flight, brain drain, writ of state, provision of public services, human rights, rule of law, population, refugees, internally displaced persons and external intervention etc.
2019	Capacity to Combat Corruption Index (CCC)	Americas Society/ Council of the Americas (AS/COA)	US	Assessment of the ability of the Latin American countries to uncover, punish, and prevent corruption.

The focus of these anti-corruption regulators is on detection, investigation and prosecution of white-collar crimes. Normally all these regulators have the mandate to prosecute all including citizens, politicians, public servants who either through gross abuse of powers, or through corruption had deprived the national exchequer of legitimate money. According to a survey, six in every ten organizations don't have a program to address bribery and corruption (PwC, 2020). The United Nations Office on Drugs and Crime (UNODC) has been working with the Governments to strengthen frameworks and capacities of state and regulatory institutions that are performing key roles in fight against financial crimes including corruption, money laundering and terrorist financing. According to a survey, in terms of direct losses, top five costliest frauds are anti-trust, insider trading, tax fraud, money laundering and bribery/corruption (PwC, 2020).

## PREVENTION AND INVESTIGATIONS FOR FINANCIAL CRIMES

There is a dire need to invest in new technologies including machine learning, behavioral biometrics and real time fraud alerts. Robust processes and technology have proved effective for the prevention of financial crimes, although it may be expensive to introduce, create, and retain these prevention controls for financial crimes (PwC, 2020; Deloitte, 2020). The benefits are high enough to warrant these preventive control expenses, although, it is also identified that fraud costs are increasing at a faster rate than fraud risk management spending (Hicks, 2019). As financial crime prevention strategies cannot deter all possible perpetrators, companies should ensure that monitoring mechanisms are in place that will promptly identify fraud occurrences. According to a survey, three types of fraud perpetrators are identified; internal, external and hybrid (collusion of internal and external fraud perpetrators). Almost 50% of the reported financial crimes are committed by internal perpetrators resulted in a loss of USD100 million (PwC, 2020). Similarly, most of global banking frauds are originated by someone working inside the bank (KPMG, 2019). Financial crime prevention steps alone are not adequate enough since a foolproof financial crime prevention mechanism cannot be enforced (Kim & Kogan, 2014).

Financial Investigation is a multi-faceted approach and its objective is to generate evidence, recovery of crime proceeds and disrupting crime markets (van Duyne *et al.* 2001). Fraudsters and Fraud Investigators have kept their pace relentlessly. Fraudsters always try to make their schemes opaque and complex (Biegelman, 2013). Despite various initiatives, financial crime investigation outcome either in the form of prosecution, conviction or confiscation remains low. According to a survey, 56% of the companies conducted investigations out of which 60% ended up in a better place. 44% took disciplinary action against employees (PwC, 2020).

## WHAT THE GURUS SAID?

Donald R. Cressey (1919 – 1987), an American socialist/criminologist, is famous for primitive scholarly work on organized crimes. His outstanding book “*Theft of the Nation: The Structure and Operations of Organized Crime in America*”, published in 1969, remains the most widely cited book on organized crime. The final hypothesis of another book “*Other People’s Money: A Study in the Social Psychology of Embezzlement*” reads as follows:

*“Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by a violation of the position of financial trust and can apply to their conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property”. (Cressey, 1953)*

Edwin Hardin Sutherland (1883 – 1950), another American sociologist, is considered as one of the most influential criminologists of the 20<sup>th</sup> century. He introduced the term white collar crimes in 1939 during a speech to the American Sociological Association. His most interesting work was “*The Professional Thief*”, written by a professional thief and annotated by him. His views about professional theft as an organized crime are valid for organized financial and technology crimes in today’s world.

## Preface

*“The essential characteristics of the profession of theft are technical skill, status, consensus, differential association and organization (p.197). Professional theft is an organized crime in the sense that it is a system in which informal unity and reciprocity may be found (p. 209). Recognition as a professional thief by other professional thieves is the absolutely necessary, universal, and definitive characteristic of the professional thief (p. 211).” (Sutherland, 1937)*

Professor Naylor is a political economist, criminologist, and historian par excellence. In his book *“Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy”*, he writes about financial crimes:

*“Although there are torrents of funny money floating around the globe, most of it comes from tax and exchange control evasion, particularly in developing countries. For that kind of loot, Western countries and their banks roll out the red carpet, even though the loss of money from fiscal offenses does far more damage to the socioeconomic fabric of developing countries than the laundering of drug money does to that of the major industrialized ones. The real threat to economic morality comes from seemingly legitimate business types intent on seeing how far they can bend the rules before they have to pay politicians to rewrite them (p. 10).” (Naylor, 2002).*

Martin T. Biegelman is one of the renowned fraud investigators of modern times. While in leadership roles in law enforcement, consulting and the corporate sector, he has over 40 years of experience of complex and high-risk investigations relating to fraud, corruption, kickbacks, conflict of interest, and whistle blower retaliation in more than 70 countries. As an ACFE Regent Emeritus, he is the recipient of Cressey Award bestowed annually by the Association of Certified Fraud Examiners (ACFE) for lifetime achievements in the detection and deterrence of fraud.

*“Fraud is gender and race neutral. What does a fraudster look like? The aura of fraud comes not from how a person looks or where they come from but from their criminal intent and the resulting self-serving actions, ruthlessness, and arrogance. The faces of fraud are burned into the memories of the victim (p.1)” (Biegelman, 2013)*

## CONTEXT AND ORGANIZATION OF THIS VOLUME

Regardless of whether you are a beginner or a seasoned researcher, this handbook of research will deepen the discourse about the financial crimes in a modern-day environment. I am hopeful that this handbook of research is a fascinating and invaluable guide for understanding the theory, practice and cases of financial crimes.

This handbook of research is organized into six sections that consist of twenty-six chapters by writers from nineteen countries. Forty-three authors contributed from disparate parts of the world; USA, UK, Canada, France, The Netherlands, Greece, Portugal, Bulgaria, Australia, China, Turkey, Pakistan, India, Malaysia, Brunei, Bangladesh, KSA, Nigeria and Uganda.

Section 1 addresses the Theory and Discussion on Financial Crimes with a set of six chapters authored by writers from Greece, The Netherlands, Turkey, Uganda, Nigeria and Pakistan. Section 2 addresses the Legislation for Financial Crimes with a set of four chapters contributed by authors from USA, China,

Bulgaria, Uganda and Pakistan. Section 3 addresses the Frauds and Financial Reporting with a set of four chapters authored by writers from Turkey, Malaysia, Bangladesh, Brunei and Nigeria. Section 4 is about the Investment Frauds with a set of four chapters authored by writers from Turkey, India, and Saudi Arabia. Section 5 addresses the Taxation and Frauds with a set of four chapters contributed by authors from Australia, Portugal, Turkey, Malaysia and Bangladesh. Section 6 is about the Technology and Financial Crimes with a set of four chapters contributed by authors from the USA, UK, Canada, France, Uganda and Nigeria.

In Section 1, the first chapter, “Understanding the Financial Fraud: An Extended Model,” by Georgios Loukas Vousinas, (National Technical University of Athens, Greece), elaborated the theory of fraud by enhancing the existing theories that force people to commit fraud. The chapter reviews the most commonly used and widely accepted models for explaining why people commit fraud - the Fraud Triangle, the Fraud Diamond, the Fraud Scale, and the MICE model. The chapter identifies a major element - Ego / Entitlement and Collusion which plays a crucial role in compelling people to commit fraud and builds on the theoretical background to conclude in the formation of the SCORE model. The second chapter, “Frauds in Business Organizations: An Overview,” by Marie G Nakitende (Uganda Martyrs University, Uganda), Abdul Rafay (University of Management & Technology, Pakistan) and Maimoona Waseem (University of Management & Technology, Pakistan), discusses a brief overview of theories of fraud. It presents causes that inspire individuals to commit fraud, methods for identifying fraud and motives that encourage people to commit fraud. The discussion concluded that fostering an ethical corporate culture is essential for fraud prevention. The third chapter, “Powerlessness as the Basis for Financial Crimes: A Brief Overview,” by Tayo Oke of Afe Babalola University, Nigeria, contends that perpetration of financial crime by the powerless can be just as corrosive and harmful as that perpetrated by the powerful. The quality of criminality and its pervasiveness is as relevant as its quantum and location. The fourth chapter, “The Power of Currency: Financial Coercion in the 21<sup>st</sup> Century” by Robert Beeres, Jan van Lieshout, and Myriame Bollen of Netherlands Defence Academy, The Netherlands, explores the coercive power of currencies and to what extent money can be deployed to prevent wars and conflicts. Based on proxies for the size of the economies of a deterring state and its adversary, the chapter shows how the potential impact of financial coercion may be estimated. The fifth chapter, “Adam’s Garden or Eve’s? A Gender-Centric Analysis of Corruption Perceptions,” by Ayesha Afzal and Aiman Asif of Lahore School of Economics, Pakistan, suggests that currently working women in an economy have a significant impact on reducing the perceived level of corruption, whereas this effect is not as strong in the earlier decade. These findings have implications for policies surrounding female employment. The chapter identifies how women, in an economic capacity, influence perception of corruption in a country, and how the relationship changes over time. The sixth chapter, “Innovation and Corruption in Turkey: Grease the Wheels or Sand the Wheels,” by Hülya ÜNLÜ (Cankiri Karatekin University, Turkey) and Merve Karacaer Ulusoy (Ankara Yildirim Beyazit University, Turkey), discussed that when corruption is the case, either “Sand the wheels” or “Grease the wheels” is the result of being unproductive or (even worse) destructive entrepreneurs. The chapter concluded even though corruption does not show a hindering effect on innovation, the time spends by the managers is the “Grease the wheels” effect for innovation.

In Section 2, the seventh chapter, “Conflict of Interest for Corruption and Abuse of Public Power: The Case of European Legislation,” by Nikolay Ivanov Nikolov of Central Election Commission, Bulgaria, is based on an analysis of the conflict-of-interest legislations of about fifteen European countries. The chapter also outlines the direction in which the phenomenon may develop in national legislations and includes examples of interesting cases of conflict of interest which have arisen in different European



## **Preface**

countries. The eighth chapter, “Regulatory Ambiguity: The Underbelly of Insider Trading,” by Laura Pinto Hansen of Western New England University, USA, discusses that in the case of illegal insider trading, illegal profits are often hidden in the purchase of luxury items and financial investments through offshore accounts. Aiding in this particular white-collar crime is the ambiguity of regulation, often dependent on the political whims of whatever political party is in office at the time. The ninth chapter, “Legislation for Public Procurements and Disposal of Public Assets: The Case of Uganda,” by Simeon Wanyama of Uganda Martyrs University, Uganda, is about the corrupt practices in the public procurement cycle, taking the example of Uganda. It also reviews the governance systems that have been put in place to try and stem out these malpractices and ensure proper governance in the administration of public procurement. The findings indicate corruption is pervasive in public procurement in Uganda despite good laws. The tenth chapter, “Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds: The Case of China,” by Poshan Yu (Soochow University, China), Yingzi Hu (Independent Researcher, China), Maimoona Waseem (University of Management & Technology, Pakistan) and Abdul Rafay (University of Management & Technology, Pakistan), highlights that unlike the UK and the US, the Chinese P2P lending market is broader. This chapter provides a more detailed analysis and an examination of the Chinese legal framework related to P2P lending and identifying the vacuums in the existing regulatory framework.

In Section 3, the eleventh chapter, “Combating Fraud through Forensic Accounting: The Case of Islamic Inheritance in Nigeria,” by Umar Habibu Umar, (Universiti Brunei Darussalam, Brunei), Md Harashid Haron, (Universiti Sains Malaysia, Malaysia) and Junaidu Muhammad Kurawa (Bayero University, Nigeria), explains the nature and forms of the fraudulent activities committed in the administration of Islamic inheritance, such as non-compliance with the provision of Islamic inheritance law, hiding some inherited estate, the non-usage of professional valuers and the advice of experts, misappropriation of inherited cash, mismanagement of inherited wealth. The twelfth chapter, “Forensic Audit Practices to Reduce Financial Frauds,” by Elif Yücel of Bursa Uludag University, Turkey, highlights that the widespread use of technology and globalization during the last decade also increased financial crimes and one of the developments that have been happened in the field of auditing is the emergence of the “forensic auditing” profession. The thirteenth chapter, “Forensic Audit for Financial Frauds in Banks: The Case of Bangladesh,” by Md. Nur Alam Siddik, of Begum Rokeya University, Bangladesh, examines the effects of forensic auditing on financial frauds in Bangladesh. Findings indicate that forensic auditing has significant positive effects on the detection and prevention of financial fraud occurrences in the banking sector of the country. The fourteenth chapter, “Determinants of Forensic Accounting: The Case of Northwestern States of Nigeria,” by Sagir Lawal (Nigeria Police Academy, Nigeria), Junaidu Muhammad (Kurawa, Bayero University, Nigeria) and Kabir Tahir Hamid (Bayero University, Nigeria), examines the political and environmental factors as determinants to apply forensic accounting in the North-Western states of Nigeria. The study recommends that all political office holders and other government personnel should, even with the change of government, use their powers to ensure the right way to move forward and the continuity of state policies to apply forensic accounting.

In Section 4, the fifteenth chapter, “Financial Scams Through Ponzi Schemes: The Case of CIS Countries,” by Alam I. Asadov of Prince Sultan University, Saudi Arabia, discusses an overview of the early cases of Ponzi schemes in the CIS countries by examining circumstances which formed fertile ground for the schemes to develop during initial years of independence. Finally, the chapter suggests that unless the level of financial literacy is raised and the financial sector is developed, Ponzi schemes will continue to thrive in the region. The sixteenth chapter, “Frauds in Unorganized Investment Schemes:

The Case of India,” by Narendra S. Bohra and Mahak Sethi of Graphic Era University, India, specifically identifies the working models, administration and organization of Unorganized Collective Investment Schemes (UCIS) in India. The chapter concluded that UCIS frauds remain the keystone of groundwork concerning the cases that have transpired over the last decade. The seventeenth chapter, “Approaches to Detect Securities Fraud in Capital Markets,” by M. Fevzi Esen (University of Health Sciences, Turkey) and Tutku Tuncalı Yaman (Beykent University, Turkey), highlights the main characteristics of securities markets and certain types of securities fraud which encompass a wide range of deceptive practices in capital markets. The chapter suggests that investors, market professionals and regulators seek autonomous data mining techniques to combat securities fraud, especially stock market manipulation. The eighteenth chapter, “Capital Market Frauds: Concepts and Cases,” by Shailendra Singh of Capital Market Consultant, India, covers various aspects of capital market frauds, manipulation practices and country case studies from global financial markets. The chapter also highlights international regulatory frameworks, guidelines and challenges being faced by the regulatory authorities.

In Section 5, the nineteenth chapter, “Tax Enforcement in the Black Economy: Tackling Disruptive Challenge,” by Brendan Walker-Munro of Swinburne University, Australia, discusses that existing tax policy (where legal constraints alone are used) is insufficient to affect black economy behaviour. The chapter suggests that by adopting responses that are “more than law”, revenue administrations can deploy a more advanced and effective approach to improve tax compliance and can decrease the negative impacts of the black economy. The twentieth chapter, “The Role of Tax Systems in Preventing Corruption,” by Simla Güzel of Tekirdag Namik Kemal University, Turkey, highlights that corruption was not deemed as a significant issue in the pre-democratic era and has become a serious issue later on. The chapter determines the duties of states towards a tax system to combat financial corruption. The twenty-first chapter, “Tax Disclosures in Financial and CSR Reporting as a deterrence for Evasion,” by Fábio Albuquerque and Julija Cassiano Neves of Instituto Politécnico de Lisboa, Portugal, highlights the most influential CSR reporting standards to answer the question that whether these standards adequately address the issue of income tax payment as a factor of CSR. The chapter also discusses the mandatory disclosure of Income Tax as required by International Financial Reporting Standards (IFRS) and standards issued by Portuguese regulatory bodies. The twenty-second chapter, “Firms’ Characteristics and Tax Evasion: A Cross-Country Investigation,” by Md. Harun Ur Rashid and Anika Morshed of International Islamic University, Bangladesh, investigates whether the firms’ characteristics, including ownership structure and funding behaviour, affect tax evasion. In order to reduce the level of tax evasion, the regulatory bodies are suggested to design the rules and regulations in such a way that the firms can easily access to finance.

In Section 6, the twenty-third chapter, “Regulations for Cybercrimes: The Case of EU Cybersecurity Act,” by Delphine Defossez of Northumbria University, UK, discusses that despite the enactments of various legislations, cybercriminals are still mostly unpunished. This chapter highlights that in EU, would it be enough to resolve some of the lingering issues of cybercrimes after the adoption of The Cybersecurity Act 2019. The twenty-fourth chapter, “Dark Web: The Digital World of Fraud and Rouge Activities,” by Jason Diodati and John Winterdyk of Mount Royal University, Canada, aims to provide a thorough yet simplified explanation of dark web technologies while expressing current trends and theories surrounding trading of fraud guides and the use of social engineering. The twenty-fifth chapter, “Dark Web: A Breeding Ground for ID Thefts and Financial Crimes,” by Annamaria Szakonyi (Saint Louis University, USA), Brian Leonard (Civil Rights University, USA), and Maurice Dawson (Illinois Institute of Technology, USA), provides insight into how crimes related to online identity theft and fraud are carried out. Examined within this chapter are the evolution of cybercrime, history of

## Preface

identity theft, applications for Internet anonymity, and discussion on effects caused by romance scams and data breaches. The twenty-sixth chapter, “Tech-Based Enterprise Control and Audit for Financial Crimes: The Case of State-Owned Global Financial Predators (SOGFP),” by Antoine Trad, (Institute of Business and Information Systems Transformation Management, France), Marie G Nakitende (Uganda Martyrs University, Uganda) and Tayo Oke (Afe Babalola University, Nigeria), discusses the concept of an applied tech-based framework of Enterprise Control and Audit for Financial Crimes (ECAFC) framework, which is significant for the detection of financial crimes. The chapter focusses on Financial Crimes Analysis (FCA), the enterprise’s long-term business longevity and the role of State Organized Global Financial Predators.

I thank the contributors and also the external reviewers who have patiently critiqued these chapters to meet the minimum acceptable standard. While the publisher and the Editor (myself) have used their best efforts in preparing this book, they make no representations and warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. The strategies or suggestions or whatsoever contained in this book may not be suitable for any specific situation for which anyone should consult with a professional, where appropriate. Neither the publisher nor the Editor shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

*Abdul Rafay*

*University of Management and Technology, Pakistan*

*March 2021*

## REFERENCES

- Albrecht, S., Howe, K., & Romney, M. (1984). *Deterring Fraud: The Internal Auditor’s Perspective*. Institute of Internal Auditors Research Foundation.
- Azim, M., & Azam, S. (2016). Bernard Madoff’s ‘Ponzi Scheme’: Fraudulent Behaviour and the Role of Auditors. *Accountancy Business and the Public Interest*, 15(1), 122–137.
- Biegelman, M. T. (2013). *Faces of Fraud: Cases and Lessons from a Life Fighting Fraudsters*. Wiley. doi:10.1002/9781118556917
- Cressey, D. R. (1953). *Other People’s Money: A Study in the Social Psychology of Embezzlement*. Free Press.
- Deloitte. (2020). Key Observations. In *Anti Money Laundering Preparedness Survey Report*. Deloitte.
- FATF. (2013). *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems*. Financial Action Task Force. Retrieved from <https://www.FATF-gafi.org/>
- Garner, B. (Ed.). (2004). s.v., “fraud.” In *Black’s Law Dictionary* (8th ed.). Academic Press.
- Hicks, D. (2019). *Global Banking Fraud Survey*. KPMG.

- Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Science*, 3(3), 191.
- Kim, Y., & Kogan, A. (2014). Development of an anomaly detection model for a bank's transitory account system. *Journal of Information Systems*, 28(1), 145–165. doi:10.2308/isis-50699
- KPMG. (2019). Key Findings. In *Global Banking Fraud Survey*. KPMG.
- Kranacher, M. J., Riley, R., & Wells, J. T. (2010). *Forensic accounting and fraud examination*. John Wiley & Sons.
- Naylor, R. T. (2002). *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*. Cornell University Press.
- PwC. (2020). *Fighting Fraud: A never ending battle*. PwC's Global Economic Crime and Fraud Survey. PricewaterhouseCoopers.
- Sutherland, E. H. (1937). *The Professional Thief*. The Chicago University Press.
- Sutherland, E. H. (1983). *White collar crime: The uncut version*. Yale University Press.
- TI. (2021). *Corruption*. Transparency International. Retrieved from <https://www.transparency.org/en>
- van Duyn, P. C., Pheijffer, M., Kuijl, H. G., van Dijk, A. T. H., & Bakker, G. J. C. M. (2001). *Financial Investigation of Crime: A Tool of the Integral Law Enforcement Approach*. The Hague: Koninklijke Vermande.
- Vousinas, G. L. (2019). Advancing theory of fraud: The SCORE model. *Journal of Financial Crime*, 26(1), 372–381. doi:10.1108/JFC-12-2017-0128
- Vousinas, G. L. (2021). Understanding the Financial Fraud: An Extended Model. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Financial Crimes*. IGI Global.
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.

## Section 1

# The Theory and Discussion on Financial Crimes

# Chapter 1

## Understanding the Financial Fraud: An Extended Model

**Georgios Loukas Vousinas**

*National Technical University of Athens, Greece*

### **ABSTRACT**

*This chapter aims to elaborate on the theory of fraud by enhancing the existing theories that force people to commit fraud. The chapter reviews the most commonly used and widely accepted models for explaining why people commit fraud: the fraud triangle, the fraud diamond, the fraud scale, and the MICE model. The author argues that these models need to be updated to adapt to the current developments and the ever-growing fraud incidents, both in frequency and severity. The chapter identifies a major element, ego/entitlement, which plays a crucial role in compelling people to commit fraud and builds on the theoretical background to conclude in the formation of the SCORE model, which is graphically depicted in the fraud pentagon. It goes further by adding the factor of collusion for its better application in cases of white-collar crimes.*

### **1. INTRODUCTION**

While fraud is a well-known term worldwide, its features cannot be regularly recognized and not until it is too late, that's why it is considered an activity both very hard to detect and even harder to justify. There are many definitions of fraud, but for the purpose of this chapter<sup>1</sup> will be used the one given by the Institute of Internal Auditors (IIA), according to which fraud is any illegal act that is characterized by deceit, violation of trust or concealment and is not dependent upon the threat of violence or physical force<sup>2</sup>. Fraud is committed by individuals as well as companies for many reasons, the most common of which are to obtain money, property and/or services, to avoid payment or to ensure personal and/or business benefit. Fraud includes, among others, false statement, misrepresentation or deceitful conduct.

DOI: 10.4018/978-1-7998-5567-5.ch001

The most difficult issue with combating fraud is to address its dynamic nature as it is an activity that is multi-layered and goes deep into business procedures, while the fraudsters always find new ways to perpetrate fraud and cover their traces so as not to be caught. That is the reason behind the complexity in confronting fraud activity, making it a long-last and complicated process that requires a deep understanding of the reasons why it occurs as well as the ways by which it can be mitigated. The recent global financial crisis of 2008 and the numerous corporate scandals behind it (mainly in the financial industry) brought into surface the severe negative effects of fraud and highlighted it as a major international problem. This is justified by the Association of Certified Fraud Examiners (ACFE)'s 2018 Report to the Nations on Occupational Fraud and Abuse, which calculated the fraud cost to an annual 5% of total business revenues<sup>3</sup>. This percentage may seem negligible, but if applied to that year's estimated Gross World Product (GDP) of \$75 trillion, results in a potential total fraud loss of about \$3.9 trillion worldwide.

In addition, one of the most common fraud types is financial fraud (or financial crime), which is defined as the fraud that is specifically committed against property. The term is also known as white-collar crime i.e., economic offenses committed with a combination of fraud, dishonesty and/or collusion. These types of frauds are usually committed for the personal benefit of the fraudster and encompass an illegal transfer of ownership of the property that is involved. Typical examples of such fraud incidents that emerged from the global crisis of 2008 are the cases of Societe Generale<sup>4</sup> and UBS<sup>5</sup>. The former (Societe Generale) involved a sequence of unapproved, undetected speculative positions for over a year period and the latter (UBS) was a rogue trader scandal that caused a loss of over \$2 billion US dollars.

Some of the most common types of financial fraud are identity theft, forgery, electronic crimes, money laundering, terrorist financing, bribery and corruption and market abuse (Saeed, Mubarik & Zulfiqar, 2021; Ibrahim, 2021). These crimes are committed on a daily basis and the authorities as well as companies around the world are engaged in an endless fight against fraud incidents while continuously trying to prevent new ones. The main groups of people that commit financial fraud are listed below: `

- Organised fraudsters, including terrorists, are gradually committing large-scale frauds in order to fund their operations worldwide.
- Business leaders or senior-level executives handle accounting data so as to improve the appearance of firms' financial statements (e.g., as a mean of improving stock performance).
- Employees from junior to senior level perpetrate fraudulent actions.
- From outside the firm, fraud can be executed by customers, suppliers or even individuals without any kind of linkage to the organization.
- External fraud in most cases also includes collusion with inside employees, in order to achieve bigger as well as better results more easily.

According to the proceedings of the World Economic Forum in 2018 financial fraud was a trillion-dollar industry, and private companies spent approximately \$8 billion on anti-money laundering (AML) controls solely in 2017, as frauds themselves (detected or not) have become more frequent and costly than ever. In particular, based on accurate estimates for every dollar of fraud, organizations lose nearly three dollars, once related costs are added to the fraud loss itself<sup>61</sup>.

Banking institutions are complicated financial organizations that operate in an ever-changing business environment and deal with high levels of risk, while facing fraudulent activities on a regular basis (Vousinas, 2016). Risks for banks arise from diverse factors, including vulnerabilities to financial fraud inherent in automation and digitization, massive growth in transaction volumes, and the greater inte-

## ***Understanding the Financial Fraud***

gration of financial systems both domestically and internationally. Moreover, that is the reason behind the continuous revision of the rules by regulators worldwide, in order to address illegal trafficking and money laundering, and the enforcement of economic sanctions by governments, aiming at countries, public and private entities, and even individuals (Jayasekara, 2021).

Institutions nowadays discover that their existing practices against such incidents cannot handle the various threats in a satisfactory way. As any employee is able to commit fraud, both within or outside of a company, it is vital to operate an efficient and effective anti-fraud program to protect the assets and reputation of the firm (Vousinas, 2016).

The previous analysis justified that financial fraud is a critical issue as it affects all aspects of business activity so trying to mitigate it is essential, particularly under crisis conditions. Thus, this chapter's purpose lies on both reviewing the existing theory on the motives behind fraud perpetration and providing insights regarding the major factors that force people to commit financial fraud.

## **2. THEORETICAL BACKGROUND**

### **2.1 The Fraud Triangle**

The most widely accepted model behind the reasons that compel people to perpetrate fraud activity is the so-called fraud triangle, a model developed by the criminologist Donald Cressey (1953). The model is based on research in a sample of “trust violators” (as Cressey called fraudsters) and is graphically depicted in the following figure:

*Figure 1. The fraud triangle*  
*Source: Cressey (1953)*



As seen in the above figure financial pressure rationalization and perceived opportunity are the three sides of the triangle. More analytically:

Pressure (also known as incentive or motive) is generally defined as a situation that occurs in the life of individuals that creates a stressful need, motivating them to fraudulent actions. According to Cressey's (1953) more specialized definition, pressure is defined as a recognized, non-shareable financial motive or problem that forces people to commit fraud. And his main hypothesis was that when individuals face such situations, they breach the trust thus, becoming “trust violators”. This happens also in cases of just



believing they have these problems (even not real) as pressure pushes them to fraudulent actions. The findings of his research showcase various examples of trust violations such as emergency situations, high living standards, difficulties in the working environment, status gaining, personal failure and increased economic needs. The common place in all these situations seems to be some kind of status-seeking or status-maintaining activities by the fraudsters. More specifically, the non-shareable pressure threatened the current status or the achievement of a higher one of the perpetrators.

The financial dimension in the pressure that forces people to commit fraud is attributed to the fact that the solution to this kind of problems lies in cash (or other assets) thefts. Typical examples are the gambling debt and bank loans that both require cash to be paid back.

The second leg of the fraud triangle is opportunity i.e., the perceived ability to perpetrate fraud. In other words, the person must realize that he has an opportunity to commit fraud without being caught. But the existence of financial pressure alone will not lead an individual to fraud activity, as all three parts must be present for such situation to occur. According to the fraud triangle theory, there are two parts of the perceived opportunity, general information and technical knowledge. General information is the knowledge that one person's position of trust can be violated. This knowledge might come from experiencing dishonest behavior by other employees, from hearing of other embezzlements or just from generally knowing that one person is in a working position where he could take advantage of the trust his employer has showed to him. On the other hand, technical skills refer to the required capabilities to commit fraud. It must be pointed out that based on Cressey's (1953) research findings it seems that most fraudsters stick to their job skills as well as their daily routine to commit their criminal actions. Basically, the type of fraudsters' job is linked with the type of fraud he will perpetrate.

The third leg of the fraud triangle is rationalization i.e., the mental process of self-justification (Marin, 1979; Rahn, Krosnick, & Breuning, 1994; Scheufele, 2000). In Cressey's hypothesis rationalization is the force that enables the fraudster to understand his illegal activity, while it gives him the illusion of a trusted person. Rationalization is considered a main component of the motivation for fraud commitment thus, being a vital part of the triangle. It takes place before the fraud occurs and is justified by the fact that fraudsters do not view themselves as criminals, so they must defend their offenses before they perpetrate them. The results of Cressey's (1953) study also showed that the fraudsters rationalized their crimes by considering them as essentially non-criminal or justified. In conclusion, the fraud triangle theory reveals that specific characteristics will increase the probability of fraud occurrence, but it does not provide absolute and holistic guidance.

## **2.2 Criticism on the Fraud Triangle**

The fraud triangle provides a theoretical framework that explains the nature of many occupational criminals, but the main problem is that it is not suitable for all cases. Even more, although academicians and practitioners have tested the fraud triangle theory, there are no practical applications e.g., using it in designing proper anti-fraud mechanisms, as it seems impossible to have a single model to fit in any circumstance. Furthermore, the fraud triangle theory is over 50 years old, and there has been considerable socio-economic change in the interim. For example, according to many anti-fraud experts there is a new kind of occupational fraudster, those who simply lack morality to ignore temptation.

In addition, while the second fraud triangle element i.e., opportunity enables white-collar crimes for a violator of trust (Rierner, 1941) However, the critical point is that not many of such opportunities will be exploited, as opportunity is a necessary, but not a sufficient condition for the occurrence of fraud.

Irrespective of how powerful the managers' motivation may be (Coleman, 1987), fraud activity is not possible without opportunity. Coleman (1992, 2001) characterizes opportunity as attractive or unattractive from a fraudster's perspective via the expectation of potential risks and future benefits. As stated by the author, the attractiveness of an opportunity for fraud perpetration (However rationalized by the individuals) frequently increases as the availability and attractiveness of a legal opportunity decreases.

Different types of financial and non-financial, corporate and private incentives can represent the motivational part of the fraud triangle. For example, an urgent need for external financing, living beyond one's means, greed, desire to avoid reputational damage, demonstration of power, status maintenance, various types of addictions and so on (Bussmann and Werle, 2006; Gill, 2011a, b.). In another aspect, Spencer (1959) places the focus to individuals who prefer to look for risky activities because of the so-called 'gambling instinct'. Indeed, there is strong evidence that some individuals in managerial positions are 'risk seekers' and 'risk lovers' (Weisburd, 1992; Bussmann and Werle, 2006). According to Punch (2000), this type of attitude is considered a part of a successful managerial image.

Recent empirical research findings on the role of opportunity as a fraud motivator (Marden and Edwards, 2005; Howe and Malgwi, 2006; Dorminey *et al.*, 2010; Sinha, 2021) showcase as critical risk factors within organizations, the existence of weak internal control systems due to lack of monitoring, proper security measures and an efficient authorization system. Moreover, other factors that are also considered as accountable for additional opportunities for financial fraud perpetration are (Loebbecke *et al.*, 1989; Farber, 2005; Howe and Malgwi, 2006; Lou and Wang, 2009):

- a complex company structure,
- ineffective preventive anti-fraud mechanisms e.g., anti-fraud training programs
- excessive trust e.g., among the external auditor and the firm and
- a leak of knowledge e.g., board members are not capable of detecting irregularities.

In their study, Dorminey *et al.* (2010) reconsider the fraud triangle and while showcasing its significance as a model for generally assessing fraud risk, they claim that it is only one part of an overall risk assessment plan and thus, it must not be examined alone (in such case it will prove to be an ineffective anti-fraud tool), but instead should be part of a complex fraud management system so as to be able to help in both preventing and detecting fraud incidents.

### **2.3 The Fraud Diamond**

Wolfe and Dana (2004) added a fourth element to the fraud triangle in order to enhance its value in improving both fraud prevention and detection. In addition to addressing incentive, opportunity, and rationalization, the authors' "fraud diamond" also considered a person's capability i.e., personal characteristics and capabilities that play a critical role in whether fraud may actually occur even with the presence of the other three elements. By incorporating the capability factor into Cressey's (1953) theory, the triangle was transformed into a diamond (Figure 2), as seen in the next figure.

The authors suggest that many frauds, especially those concerning financial statements, would not have ever happened if it wasn't for the right person with the required capabilities to design and commit fraud. Essentially, opportunity paves the way to fraud, and incentive along with rationalization can force a person toward this direction. But an individual must have the capability to recognize this way as an opportunity and to take advantage of it repeatedly. The authors identified a number of significant observ-

Figure 2. The Fraud Diamond

Source: Wolfe and Dana, 2004



able traits regarding the individuals' capability to perpetrate fraud. In particular, a common characteristic is the working position of a person e.g., a senior manager has the ability to perform fraudulent activity owing to his role in an organization. Another ability is when a person has the knowledge of an operating system as well as the intelligence to exploit the existing weaknesses in a company's internal control system for his fraud intentions e.g., a trader knows that some transactions do not require authorization (four eyes principle). Even more, an oversized ego and high levels of confidence that fraud action won't be detected or noticed can lead to fraud e.g., a CEO in order to maintain his status and gain even more work benefits is prone to fraud due to his ego.

In conclusion, while there is a clear overlap among the four elements of the fraud diamond, its main contribution is the clear separation of a person's capabilities in an overall fraud risk assessment. And that helped in broadening the concept of opportunity beyond the myopic view of conditional or environmental factors that prevailed till then in auditing practices (Khan *et al.*, 2020; Ramzan *et al.*, 2020). At this point it should be emphasized that in earlier research than that of Wolfe and Hermanson e.g., Weisburd (1992), Croall (2001), Ones and Viswesvaran (2001) and Schnatterly (2003), there were some references to the idea of capability, but mostly referred to as part of opportunity.

## 2.4 The Fraud Scale

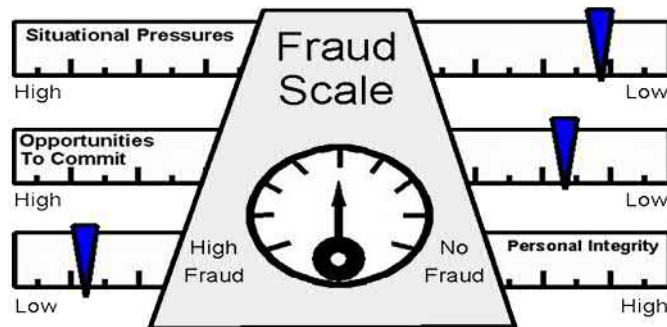
Another significant theory on the motives behind fraud activity is that of the fraud scale, introduced by Albrecht *et al.* (1984), which identifies three factors that lead to such actions: situational pressure, opportunity and personal integrity (Figure 3).

As the authors believed that fraud is a very tough activity to predict due to the fact that there does not exist a single, reliable profile of occupational fraud perpetrators, they replaced the third leg of the fraud triangle i.e., rationalization with personal integrity as the former is more abstract to be known by other people, while the latter can be traced from the past behavior of individuals. More specifically, the benefit of using personal integrity is that by observing the decision-making process of a person along with his final decisions, his commitment to ethical decision making becomes measurable.

And central to the idea of deterrence, according to Rezaee and Riley (2012), is the dependence on personal decision-making as well as responsibility. Violations of ethics, trust and responsibility are at the heart of fraudulent activities. Ethics is behind rationalization and by setting the conditions under which a potential fraudster might decide whether an action is right or wrong, the pressure (to a certain degree) that leads to fraud. As a result, individuals who consider the ethical side of their decisions

Figure 3. The Fraud Scale

Source: Albrecht *et al.*, 1984.



might be able to evaluate integrity and thus, the relative possibility of an individual committing fraud. It should be pointed out that the fraud scale supports that all three factors - pressure, opportunity and personal integrity have to be considered simultaneously in order to be able to determine whether a situation incorporates a higher probability of fraud.

### 2.5 The Mice Model

Kranacher *et al.* (2010) provided another approach behind the incentives of a typical fraudster by proposing a set of motives, beyond the financial pressure (as defined in the fraud triangle theory), which are included in the acronym MICE: money, ideology, coercion and ego. Ideology motivates people to justify fraudulent behavior by considering it consistent with their beliefs. Coercion happens when individuals are persuaded to participate in fraudulent activity by others. Ego can also be a powerful incentive behind fraud due to the fact that people, in order to keep their ego, desire to maintain their reputation or current position against their families and their social environment. Conclusively the MICE model is an easily remembered theory, which may not apply in all fraud cases, but offers practitioners with a broader framework to assess the probability of fraud.

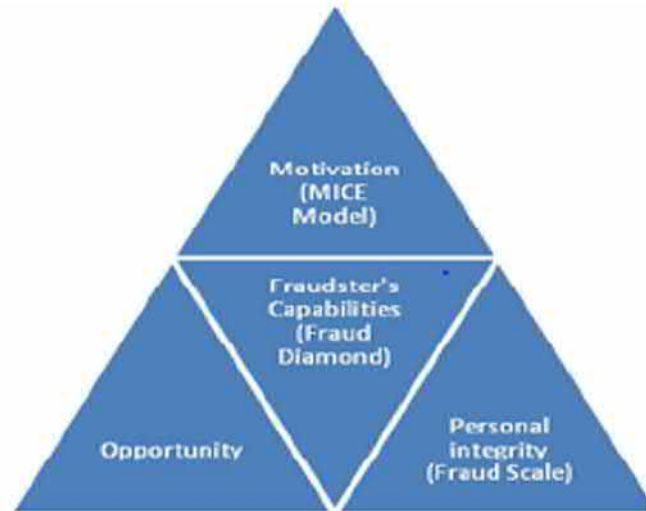
### 2.6 The New Fraud Triangle Model

Kassem, R. & Higson, A. (2012) suggest that in order to better assess the likelihood of fraud occurrence, professionals should consider all the dominant fraud models - the Fraud Triangle, the Fraud Diamond, the MICE Model and the Fraud Scale- together. All these models should be viewed as an extension to the fraud triangle and must be integrated in one single model called “the New Fraud Triangle Model” (Figure 4).

In this proposed model all the factors of the aforementioned models are included i.e., motivation, opportunity, fraudsters’ capabilities and integrity and as a result fraud risk is more effectively assessed by fraud examiners, auditors and all related stakeholders.

Figure 4. The New Fraud Triangle Model

Source: Kassem, R. & Higson, A., 2012



### 3. CONCEPTUAL FRAMEWORK

#### 3.1 The Score Model

After the extensive review of the theoretical background regarding the factors that compel people to perpetrate fraud, it is crystal clear that the current business developments and the continuously evolving fraud incidents (both in frequency and severity), require the update of the existing fraud models. In order to advance the existing fraud theory and enhance the practitioners' knowledge behind the major factors which lead to fraud perpetration, the author proposes a new model, the SCORE model, which is the abbreviation of the words: Stimulus, Capability, Opportunity, Rationalization and Ego / Entitlement (Vousinas, 2019). The first four elements of the model (Stimulus, Capability, Opportunity & Rationalization) stem from the Fraud Triangle and the Fraud Diamond while the fifth is added in order to enhance fraud detection and prevention, to extend our understanding regarding the major factors that lead to fraudulent acts as well as to contribute to the design of more effective anti-fraud mechanisms. The analysis of the five factors of the SCORE model is provided below:

##### Stimulus

Stimulus or incentive is the pressure behind fraud perpetration and in this model, it has both financial and non-financial nature, in contrast to the fraud triangle model that focuses only on the financial one. Pressure takes different forms e.g., economic needs, problems related to work environment, requirement to report quicker and better results due to the pressure to meet business targets and deadlines (especially under crisis conditions), professional ambition, status maintenance, while sometimes just a person's desire (driven by oversized ego) to prove he / she can defeat the system etc. Especially in times of crisis, the probability of fraud activity is substantially higher due to the economic downturn on one hand and

## ***Understanding the Financial Fraud***

the pressure put on employers to meet business objectives on the other, along with cost reductions due to tighter budgeting, so that their professional status and/or financial situation not to be negatively affected.

### **Capability**

Capability, given the presence of three legs of the fraud triangle - pressure, opportunity and rationalization, is defined as the personal characteristics and abilities that play a critical role in whether fraud will actually take place. Many fraud incidents, among them some of the largest financial frauds, would not have occurred if it was not for the right person with the proper capabilities to perform fraud. Opportunity paves the way and incentive and rationalization attract the potential fraudsters toward this direction. To do so an individual must also have the capability to walk through that opening. This includes self-confidence, the capability to recognize internal control weaknesses and “blind spots”, to override existing anti-fraud mechanisms and so on. As a result, companies along with internal and external auditors must monitor, evaluate and document on a constant basis the capabilities of all staff, including board members, senior executives and those in key positions that may perform and conceal fraud.

### **Opportunity**

When we refer to opportunity, we mean the circumstances that allow fraud to occur. e.g., weak internal controls, inadequate anti-fraud policy, poor tone at the top and unsatisfactory accounting policies. The fraudster strongly believes that can create and perform fraudulent acts without being detected. It should be emphasized that opportunity is not implicitly real i.e., opportunities must be considered as real by the fraudster. The opportunity for fraud is the most straightforward causal factor for companies to deal with due to the fact that it stems from the company itself. Unlike the other factors of the fraud triangle -motivation and rationalization- opportunity does not depend on the circumstances the potential fraudster faces or his personal state of mind. Studies on frauds have also highlighted that opportunity is provided also by the individuals’ position within an organization e.g., senior executives have the authority to override controls and consequently the opportunity to perform fraudulent acts.

### **Rationalization**

Rationalization is generally defined as a defense of ego in which apparently logical reasons are given to justify behavior that is motivated by unconscious instinctual impulses and is unacceptable<sup>7</sup>. In fraud theory it refers to the justification of fraud perpetration by an individual. More specifically, people rationalize their behavior by accepting that committing fraud is a normal situation for a number of reasons. In case of dishonest persons, it is easier for them to rationalize fraud acts, while for those with higher moral standards might be more difficult. But in both cases fraudsters have to convince themselves that fraud is an acceptable activity, using a variety of “excuses” for in order to “approve” their behavior. Even more it is common practice for individuals to reframe their definition of unlawful behavior so as to exclude their own actions and rationalize their fraudulent activity. If the rationalization is successful, the fraudsters will not feel guilt or remorse, but he may even rationalize themselves as the victim. And this justification is what allows the fraudster to keep the fraud going over a long period of time, which is one of the signs of many organizational frauds.

Examples of typical rationalizations include, among others, making up for not being fairly, “borrowing” money from the firm now and pay them back later, while some frequently used statements are listed below:

- The end justifies the means
- Everyone is doing it
- I’ll take the money now and pay them back in the future
- I was entitled to the money
- I’m only human
- Doesn’t everybody cheat?
- No one will notice
- Ethics is a luxury I can’t afford right now
- I was just trying to support my family
- I deserve this after all these years with this company.

## **Ego / Entitlement**

Criminal behavior, according to psychoanalytic theories, is the result of mental processes (Aichorn, 1935; Toch, 1979; Andrews and Bonta, 1994; DiNapoli, 2002). And according to the groundbreaking ideas of Freud (1923) in each individual there is a coherent organization of mental processes that is called ego. Ego, from the psychoanalytic perspective, is defined as the part of the personality that deals with the external world and its practical demands<sup>8</sup>. Essentially, the ego enables the individual to perceive, reason, test reality, solve problems and adjust the instinctual impulses of the id to the demands of the superego. The terms id and superego are coined by Freud (1923) who identified a three-part structural id-ego-superego model to human personality as follows:

- the id i.e., the force for food, sex, and other life-sustaining things,
- the super-ego i.e., the conscience that grows when learned values become incorporated into an individual’s behavior, and
- the ego i.e., the “I” or the product of the collaboration among what a person desires and what his conscience will let him to do to achieve what he wants.

Based on the above, ego, as one of the main human mental processes, is proven to be a critical factor behind fraudulent activity.

In another study, Spencer (1977) claims that one of the main motives behind the perpetration of white-collar crimes (Weisburd and Waring, 2001) seems to be the sense of superiority, mastery and the admiration of others, all driven by ego. More specifically, he argues that *“as people who committed fraud were successful at one crime, they began to gain some secondary pleasure in the knowledge that they are misleading the world and that they are displaying their superiority to others”*. Those people are called “egotists” (Allan, 2003) i.e., “people who are forced to succeed at all costs, self-absorbed, self-confident and often narcissistic. According to the Diagnostic and Statistical Manual of Mental Disorders<sup>9</sup>, *“narcissistic personality disorder is a pervasive pattern of grandiosity, a strong need for admiration and a lack of empathy for others. People with this kind of disorder believe they are superior or unique and they are likely to have inflated views of their own accomplishments and abilities”*.

Ego is also indicated by Duffield and Grabosky (2001) as an aspect of motivation that may apply to some or all types of fraud. The authors point out that ego is connected to both power over people and situations. In the case of people, the sensation of power over another individual or individuals is proven to be a strong encouraging force for a number of fraud perpetrators to the point that it becomes an end in itself.

The importance of ego as a major incentive behind fraud perpetration is emphasized in one of the most commonly used models, the previous analyzed MICE model (Kranacher, *et al.*, 2010), too. In particular, the social burden not to lose their reputation forces people to commit fraud in order to satisfy their ego. Those individuals, driven by the oversized ego, are self-confident that their fraudulent acts will not be detected so they are more prone to criminal behavior. So, a person should have a strong ego and high levels of confidence not to be detected (Pedneault S. *et al.*, 2012) in order to commit fraud. And the oversized ego, frequently characterized by greed and self-exaggeration, is also supported by Ramamoorti (2008) that points out that among the critical factors that compel people to commit fraud is the so called “catch me if you can” attitude, an ego-driven personality trait that white collar fraudsters display and that reinforces their fraudulent activity.

Personality, in general, which refers to the attributes that characterize a unique person, is considered one of the most influential factors behind frauds, and some individuals are by nature less ethical than others, according to Geis (2011). For example, if somebody is by nature arrogant or power lover, it is more likely to commit fraud compared to another that is humble. In this direction, the author identifies the desire for power and ego as one of the most common motives for perpetrating fraud. He also highlights that under crisis conditions persons and business entities with power will at times take advantage of loose or nonexistent regulatory frameworks to overcome the demands of the criminal law and perform fraudulent acts.

Except from the literature, there are also numerous practical examples that justify that ego is behind some of the most notorious financial frauds in the recent recorded criminal history. For example, Russell Wasendorf, the founder of Peregrine Financial Group, a commodity brokerage firm based in Iowa, was one of the first fraudsters to actually acknowledge the role ego played in his crimes. This declaration was recorded in his suicide note written back in 2012 in which he stated, “*I guess my ego was too big to admit failure, so I cheated*”. Wasendorf’s fraud involved creating phony bank statements for almost 20 years, sending them to a post office box controlled by him, and then presenting them to regulators as evidence that his company was financially healthy. At the same time However, he was stealing millions of dollars in customer funds and his total scam reached approximately the amount of \$200m<sup>10</sup>.

In an oversized ego is also attributed one of the biggest financial crimes of all time, the \$7bn global Ponzi scheme developed by Robert Allen Stanford, through his firm Stanford Financial Group<sup>11</sup>. And the most notorious fraud of all time, Bernie Madoff’s \$65bn swindle (it is considered the largest financial fraud in USA history) that involved a massive Ponzi scheme, was also supercharged by ego. Madoff stated that “*I refused to accept the fact that I failed for once in my life*” However, while he famously apologized to his victims, most of his statement was about himself and all he was feeling as he prepared to head to prison for the rest of his life. In his nearly 600-word statement he utilized the words “I” or “me” over 40 times justifying his ego-driven personality<sup>12</sup>.

The above analysis brought into surface a new factor - Ego - that plays a crucial role in explaining why people perpetrate (not only) financial fraud. Both literature and practical evidence were presented to support the role of ego and the author proposed a new theoretical framework, the SCORE model, to broaden our understanding behind fraud motivators and update the prevailing but outdated existing



models (mainly the fraud triangle and the fraud diamond). At this point it should be highlighted that the five components of the SCORE model do not exist in isolation but must be all present for frauds to occur. Ann in order to be easily memorized the model is depicted in the Fraud Pentagon graph presented below:

The sequence from the existing models i.e., the Fraud Triangle and the Fraud Diamond to the suggested Fraud Pentagon can be seen in the next graph:

Figure 5. The Fraud Pentagon

Source: Author's design.



Figure 6. The Sequence to the Fraud Pentagon



### 3.2 The Extended SC(C)ORE Model

As the fraud examination theory has predominantly based on the fraud triangle, which in most cases assumes that a person committing fraud acts in isolation (Dorminey *et al.*, 2010), it has fallen behind other scientific areas related to theoretical research on the phenomenon of collusion (Trompeter *et al.*, 2013, 2014; Dorminey *et al.*, 2010, 2012). Even more, the recent financial fraud history has highlighted collusion as a main factor behind many complicated as well as pricey organizational crimes. For example, two of the most well-known white-collar crime incidents, those involving Enron and WorldCom, implicated multiple members from inside the company.

The term collusion refers to a dishonest agreement among two or more individuals, for the one party to bring an action against the other for some evil purpose, as to defraud a third party of his rights<sup>13</sup>. And the fraudsters participating in collusion may be of the following three types according to Venter (2007):

## ***Understanding the Financial Fraud***

1. workers from inside a firm,
2. a group of people working in multiple companies or
3. members of a devoted criminal group.

Once collusion takes place among employees, or between employees and an external party, fraud is getting more difficult to detect and deal thus, making it an ever-growing type of financial fraud, especially under crisis conditions. For example, criminal groups nowadays actively pursue to place their own person in a firm as a temporary employee or even a contractor. And once a fraud initiates, even honest personnel can then be pulled in as a fraudulent environment is created as well as a dishonest culture. It is also a common practice for fraudsters with a very influential personality to convince others to commit or even conceal fraud.

The required theoretical framework that justifies collusion as a main factor behind fraud is provided by the relevant criminological research.

More specifically, the following four theoretical perspectives regarding the role of collusion are identified by Weerman (2003):

1. the influence perspective that conceives collusion to be the result of the group influence promoting criminal behavior
2. the social selection perspective that assumes collusion to be a by-product of the offenders' inclination to seek each other out proactively as friends and companions
3. the instrumental perspective considers collusion as the outcome of a judgement that collusion leads to an easier, more profitable or less risky fraud perpetration and
4. the social exchange perspective that conceptualizes collusion as an inter-personal exchange of material and non-material goods in which each offender has something to gain from the co-operation of the other.

Allan (2003) points out that a common personality type among fraudsters is the “bully,” who *“makes unusual and important demands of those who work for him or her, cultivates fear rather than respect ... and consequently avoids being bound by the same rules and procedures as others.”*, making him prone to commit fraud. A significant number of financial frauds is committed by subordinates reacting to an act from above to “make your numbers at all costs.” There is also an involuntary form of collusion as fraudulent activity spreads out inside a company. In such cases criminals exploit their capabilities to take advantage of the positions of others and use unsuspecting people for their own benefit.

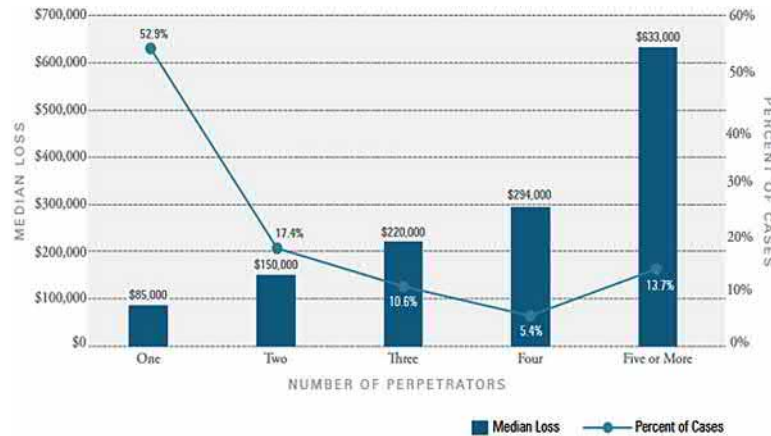
Beyond theoretical contributions there are also several empirical studies on the crucial role of collusion as a major factor behind financial fraud perpetration. For example, in a recent interview study of convicted fraudsters from the three largest US Federal prisons, it was found that 59% of the respondents (37 out of 63) argued that their fraudulent actions clearly involved more than one person.

But the most reliable empirical study is the recent ACFE's 2018 Report to the Nations on Occupational Fraud and Abuse. According to the results of this benchmark report in the fraud field nearly half of the examined cases involved collusion of several individuals in perpetrating fraudulent acts. Additionally, the greater the number of fraudsters involved; the higher losses tended to be (Figure 7):

As shown in the above figure when only one fraudster is involved the median loss is \$85.000 while in the case of two criminals the amount is almost doubled (\$150.000) and when there are five or more individuals committing fraud (a considerable 13.7% of the cases) the loss is skyrocketed to \$633.000. A

Figure 7. Number of Perpetrators - Frequency and Median Loss

Source: "2018 Report to the Nations on Occupational Fraud and Abuse. Copyright 2018 by the Association of Certified Fraud Examiners, Inc.", available at: <https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf>



possible reason behind this boost in losses associated with multiple fraudsters lies in the fact that most of the anti-fraud controls are built on the basis of separation of duties and independent checks thus, been unable to prevent fraudulent activity. In particular, when multiple fraudsters work together, they are capable of overriding existing independently verifying mechanisms or other anti-fraud mechanisms (for example those based on the four eyes principle<sup>14</sup>). Another explanation for the larger median loss in cases of collusion could be the fact that the perpetrators' proceeds had to split in more portions i.e., with more fraudsters expecting a payoff, those involved required to steal more money to satisfy everyone.

The results of the ACFE study also examined how the impact varied based on perpetrators' relationship to the victims. More specifically, there were related frauds in which all the fraudsters worked for the victim company to frauds in which an inside employer conspired with an outside partner at one of the victim's customers. The aim was to check if it was more common for insiders to collaborate with an outside party or to conspire with one another, and also to examine whether there were differences in the types of fraud performed or the size of the losses depending on the group involved. The results showed that the two types of collusion (inside and outside) were practically the same both in terms of occurrence and median loss, as depicted in the next figure:

So, by adding the element of collusion the SCORE model becomes the SC(C)ORE model, that is graphically depicted in the Fraud Hexagon, as shown below:

It must be pointed out that regarding the SC(C)ORE model there is no need for all six elements to exist for the perpetration of financial fraud to take place, but the five initial elements of the SCORE model should be all present. The overall purpose of this extension to the initial model is to capture the reasons why white-collar crimes take place by highlighting the significance of collusion that is justified to play a crucial role in such cases.

## Understanding the Financial Fraud

Figure 8. Collusion - Frequency and Median Loss Based on Perpetrators' relationship to Victim

Source: "2018 Report to the Nations on Occupational Fraud and Abuse. Copyright 2018 by the Association of Certified Fraud Examiners, Inc.", available at: <https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf>

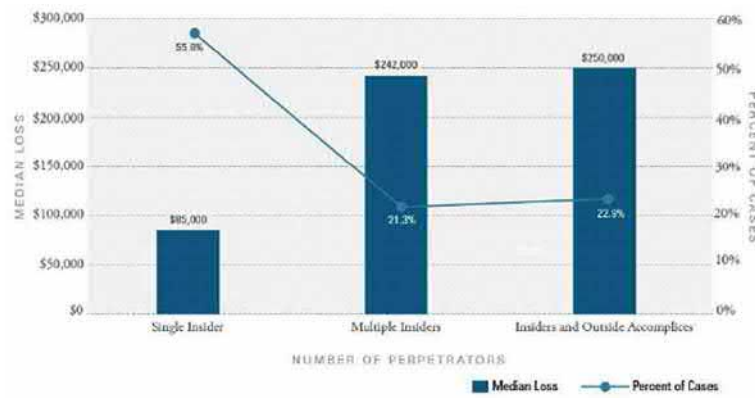


Figure 9. The Fraud Hexagon

Source: Author's design.



## 4. CONCLUDING REMARKS

In the current globalized environment organizations around the world have to deal with high levels of risks of all kind e.g., financial risk, operation risk, legal risk, reputation risk etc., which all have a negative effect on them. But in spite of the fact that financial fraud is just another type of risk it is an ever-growing international problem, particularly under crisis conditions (as shown by the recent global financial crisis of 2008), affecting both public and private entities as well as all the business sectors of the economy.

Fraud is both a complicated and dynamic procedure that constantly adapts to the current situations, that's the reason why it is so difficult to detect and even harder to prevent. Even more, taking into consideration that not only there are many different definitions, but also various fraud models that try to shed light on the reasons behind fraud perpetration, it becomes clear that fraud is a tough nut to crack. The review of the theoretical background presented in this chapter justified that there is no single model to fit in any case, while showcasing that the fraud theory has left behind the current developments in the field as well as the ever-growing fraud incidents. For this reason, the author states that the existing theories have to be updated and proposes a new model, the SCORE model. The name of the model is the acronym

of the words: Stimulus, Capability, Opportunity, Rationalization and Ego, and can be considered as an extension to the Fraud Triangle and the Fraud Diamond. The model identifies Ego, which is justified, theoretically and practically, to play a crucial role in explaining why people perpetrate financial fraud. The SCORE model is graphically depicted in the Fraud Pentagon and can be further improved by adding the element of collusion to better apply in financial fraud incidents.

The overall aim of this chapter is to broaden our understanding behind the main factors that compel people to commit fraud and propose a reference model that will serve as a theoretical benchmark. The author also hopes to initiate a fruitful academic and professional discourse on this crucial issue, which not only remains a severe global problem, but the occurrence of financial fraud is growing exponentially, especially under crisis conditions.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in his personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## **REFERENCES**

- Aichorn, A. (1935). *Wayward Youth*. Viking Press.
- Albrecht, S., Howe, K., & Romney, M. (1984). *Deterring Fraud: The Internal Auditor's Perspective*. Institute of Internal Auditors Research Foundation.
- Allan, R. (2003). Fraud-the human face of fraud: Understanding the suspect is vital to any investigation. *CA Magazine-Chartered Accountant*, 136(4), 39–40.
- American Psychological Association. (2009). *APA concise dictionary of psychology*. American Psychological Association.
- Andrews, D. A., & Bonta, J. (1994). *The Psychology of Criminal Conduct*. Anderson.

## ***Understanding the Financial Fraud***

- Bussmann, K. D., & Werle, M. M. (2006). Addressing Crime in Companies: First Findings from a Global Survey of Economic Crime 1. *British Journal of Criminology*, 46(6), 1128–1144. doi:10.1093/bjc/azl072
- Coleman, J. W. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology*, 93(2), 406–439. doi:10.1086/228750
- Coleman, J. W. (1992). Crime and money: Motivation and opportunity in a monetarized economy. *The American Behavioral Scientist*, 35(6), 827–836. doi:10.1177/0002764292035006017
- Coleman, J. W. (2001). The causes of white-collar crime and the validity of explanation in the social sciences. In S.-A. Lindgren (Ed.), *White-collar Crime Research: Old Views and Future Potentials*. National Council for Crime Prevention.
- Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Free Press.
- Croall, H. (2001). *Understanding White Collar Crime*. Open University Press.
- DiNapoli, P. P. (2002). Adolescent violent behavior and ego development. *The Journal of Adolescent Health*, 31(6), 446–448. doi:10.1016/S1054-139X(02)00450-0 PMID:12457576
- Dorminey, J., Fleming, S., Kranacher, M., & Riley, R. (2010). Beyond the fraud triangle. *The CPA Journal*, 80(7), 17–23.
- Dorminey, J., Fleming, S., Kranacher, M., & Riley, R. Jr. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555–579. doi:10.2308/iace-50131
- Duffield, G., & Grabosky, P. (2001). *The psychology of fraud Trends and Issues in Crime and Criminal Justice*. Australian Institute of Criminology.
- Free, C., & Murphy, P. R. (2015). The ties that bind: The decision to co-offend in fraud. *Contemporary Accounting Research*, 32(1), 18–54. doi:10.1111/1911-3846.12063
- Freud, S. (1923). The Ego and the Id. *The Standard Edition of the Complete Psychological Works of Sigmund Freud, Volume XIX (1923-1925): The Ego and the Id and Other Works*, 1 – 66.
- Geis, G. (2011). *White-collar and corporate crime: a documentary and reference guide*. ABC-CLIO.
- Gill, M. (2011a). Fraud and recessions: Views from fraudsters and fraud managers. *International Journal of Law, Crime and Justice*, 39(3), 204–214. doi:10.1016/j.ijlcj.2011.05.008
- Gill, M. (2011b). Learning from fraudsters' accounts of their offending. *Prison Service Journal*, 194, 27–32.
- Howe, M. A., & Malgwi, C. A. (2006). Playing the ponies: A \$ 5 million embezzlement case. *Journal of Education for Business*, 82(1), 27–33. doi:10.3200/JOEB.82.1.27-33
- Ibrahim, A. R. (2021). Religio-Spiritual Implications of Corruption and Money Laundering: The Case of Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

- Jayasekara, S. F. S. D. (2021). Risk-based AML/CFT Regulations for Effective Supervision. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Science*, 3(3), 191.
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Kranacher, M. J., Riley, R., & Wells, J. T. (2010). *Forensic accounting and fraud examination*. John Wiley & Sons.
- Loebbecke, J. K., Eining, M. M., & Willingham, J. J. (1989). Auditors' experience with material irregularities: Frequency, nature, and detectability. *Auditing*, 9(1), 1–28.
- Lou, Y. I., & Wang, M. L. (2009). Fraud risk factor of the fraud triangle assessing the likelihood of fraudulent financial reporting. *Journal of Business & Economics Research*, 7(2), 61–78.
- Marden, R., & Edwards, R. (2005). Internal controls for the small business: Skimming and the fraud triangle. *Internal Auditing*, 20(1), 3–10.
- Markin, R. J. (1979). The role of rationalization in consumer decision processes: A revisionist approach to consumer behavior. *Journal of the Academy of Marketing Science*, 7(4), 316–334. doi:10.1007/BF02729682
- Ones, D., & Viswesvaran, C. (2001). Integrity tests and other criterion-focused occupational personality scales (COPS) used in personnel selection. *International Journal of Selection and Assessment*, 9(1/2), 31–39. doi:10.1111/1468-2389.00161
- Pedneault, S., Silverstone, H., Rudewicz, F., & Sheetz, M. (2012). *Forensic accounting and fraud investigation for non-experts*. John Wiley & Sons.
- Punch, M. (2000). Suite violence: Why managers murder and corporations kill. *Crime, Law, and Social Change*, 33(3), 243–280. doi:10.1023/A:1008306819319
- Rahn, W. M., Krosnick, J. A., & Breuning, M. (1994). Rationalization and derivation processes in survey studies of political candidate evaluation. *American Journal of Political Science*, 38(3), 582–600. doi:10.2307/2111598
- Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education*, 23(4), 521–233. doi:10.2308/iace.2008.23.4.521
- Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.
- Rezaee, Z., & Riley, R. (2012). *Financial Statement Fraud: Prevention and Detection*. Wiley. doi:10.1002/9781119198307
- Rierner, S. H. (1941). Embezzlement: Pathological basis. *The Journal of Criminal Law and Criminology*, 32(4), 411–423. doi:10.2307/1136639

## ***Understanding the Financial Fraud***

- Saeed, S., Mubarik, F., & Zulfiqar, S. (2021). Money Laundering: A Thought-Provoking Crime. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Scheufele, D. A. (2000). Agenda-setting, priming, and framing revisited: Another look at cognitive effects of political communication. *Mass Communication & Society*, 3(2-3), 297–316. doi:10.1207/S15327825MCS0323\_07
- Schnatterly, K. (2003). Increasing firm value through detection and prevention of white-collar crime. *Strategic Management Journal*, 24(7), 587–614. doi:10.1002/mj.330
- Sinha, A. (2021). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Spencer, E. (1977). White-collar criminals. *The Journal of Social Issues*, 33(4), 179–196. doi:10.1111/j.1540-4560.1977.tb02531.x
- Spencer, J. C. (1959). A study of incarcerated white-collar offenders. In G. Geis (Ed.), *White-collar Criminal: The Offender in Business and the Professions*. Atherton Press.
- Toch, H. (1979). *The Psychology of Crime and Criminal Justice*. Holt, Rinehart and Winston.
- Trompeter, G., Carpenter, T., Desai, N., Jones, K., & Riley, D. Jr. (2013). A synthesis of fraud related research. *Auditing*, 32(1), 287–321. doi:10.2308/ajpt-50360
- Trompeter, G., Carpenter, T., Jones, K., & Riley, D. Jr. (2014). Insights for research and practice: What we learn about fraud from other disciplines. *Accounting Horizons*, 28(4), 769–804. doi:10.2308/acch-50816
- Venter, A. (2007). A procurement fraud risk management model. *Meditari Accountancy Research*, 15(2), 77–93. doi:10.1108/10222529200700012
- Vousinas, G. (2016). The critical role of Internal Auditing in addressing bank fraud: A conceptual framework. *International Journal of Case Studies*, 5(3), 67–81.
- Vousinas, G. L. (2019). Advancing theory of fraud: The SCORE model. *Journal of Financial Crime*, 26(1), 372–381. doi:10.1108/JFC-12-2017-0128
- Weerman, F. (2003). Co-offending as social exchange explaining: Explaining characteristics of co-offending. *British Journal of Criminology*, 43(2), 398–416. doi:10.1093/bjc/43.2.398
- Weisburd, D., & Waring, E. (2001). *White-collar crime and criminal careers*. Cambridge University Press. doi:10.1017/CBO9780511499524
- Weisburd, S. (1992). The problem of white-collar crime motivation. In K. Schlegel & D. Weisburd (Eds.), *White collar Crime Reconsidered*. Northeastern University Press.
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.



## ENDNOTES

- <sup>1</sup> Earlier version of this chapter was presented at International Conference on Business & Economics of the Hellenic Open University 2018, which later on published in the Journal of Financial Crime, Vol. 26 Issue: 1, pp. 372 - 381. This chapter is the extension and improvement of the previous versions.
- <sup>2</sup> Institute of Internal Auditors (IIA): International Professional Practices Framework (IPPF), 2013 Edition.
- <sup>3</sup> 2018 Report to the Nations on Occupational Fraud and Abuse. Copyright 2018 by the Association of Certified Fraud Examiners, Inc.”, available at: <https://s3-us-west-2.amazonaws.com/acfepublic/2018-report-to-the-nations.pdf>. Accessed: 21.10.2020.
- <sup>4</sup> Société Générale, Summary of PwC diagnostic review and analysis of the action plan, 23 May 2008. Accessed: 21.10.2020.
- <sup>5</sup> UBS Annual Report 2011. Accessed 21.10.2020.
- <sup>6</sup> World Economic Forum Annual Meeting, Davos-Klosters, Switzerland, January 23–26, 2018; LexisNexis risk solutions 2018 True Cost of Fraud study, LexisNexis, August 2018, risk.lexisnexis.com
- <sup>7</sup> American Psychological Association. (2009). *APA concise dictionary of psychology*. Washington, DC: American Psychological Association. Available at: <https://dictionary.apa.org/rationalization>. Accessed: 21.10.2020.
- <sup>8</sup> American Psychological Association. (2009). *APA concise dictionary of psychology*. Washington, DC: American Psychological Association. Available at: <https://dictionary.apa.org/ego>. Accessed: 21.10.2020.
- <sup>9</sup> The Diagnostic and Statistical Manual of Mental Disorders (DSM) is published by the American Psychiatric Association (APA) and offers a common language and standard criteria for the classification of mental disorders (available at: [https://www.psychiatry.org/psychiatrists/practice/dsm?\\_ga=2.50611305.1520553320.1510661060-359188563.1510661060](https://www.psychiatry.org/psychiatrists/practice/dsm?_ga=2.50611305.1520553320.1510661060-359188563.1510661060)).
- <sup>10</sup> “Special report: Iowa broker built empire on a lie concealed in a postal box”, accessed 21.10.2020, available at: [www.reuters.com/article/us-wasendorf-life-one/special-report-iowabroker-built-empire-on-a-lie-concealed-in-a-postal-box-idUSBRE88N0EJ20120924](http://www.reuters.com/article/us-wasendorf-life-one/special-report-iowabroker-built-empire-on-a-lie-concealed-in-a-postal-box-idUSBRE88N0EJ20120924)
- <sup>11</sup> “Top 10 Swindlers”, accessed 21.10.2020, available at: [http://content.time.com/time/specials/packages/article/0,28804,2104982\\_2104983\\_2105000,00.html](http://content.time.com/time/specials/packages/article/0,28804,2104982_2104983_2105000,00.html)
- <sup>12</sup> “Bernard L. Madoff’s Statement to the Court”, accessed 21.10.2020, available at: [www.nytimes.com/2009/06/30/business/30bernietext.html](http://www.nytimes.com/2009/06/30/business/30bernietext.html)
- <sup>13</sup> Bryan Garner, ed., Black’s Law Dictionary. 10th Ed. (2014), s.v., “collusion.”
- <sup>14</sup> the requirement that a business transaction be approved by at least two individuals, available at: <https://www.collinsdictionary.com/dictionary/english/four-eyes-principle>. Accessed: 21.10.2020.

## Chapter 2

# Frauds in Business Organizations: A Comprehensive Overview

**Marie G. Nakitende**

*Uganda Martyrs University, Uganda*

**Abdul Rafay**

 <https://orcid.org/0000-0002-0285-5980>

*University of Management and Technology, Pakistan*

**Maimoona Waseem**

*University of Management and Technology, Pakistan*

### ABSTRACT

*Fraud has been evolving and increasing with the change in the work environment, organizational structures, industrialization, and legislation. Money, greed, manipulation, job pressures, family needs, opportunity, politics, rationalization are the crucial reasons that lead people to behave fraudulently. The purpose of the chapter is to discuss a brief overview of theories of fraud. It presents causes that inspire individuals to commit fraud, methods for identifying fraud, and motives that encourage people to commit fraud. Management must try to eliminate the vulnerabilities that offer criminals the chance to commit fraud. Organizational leaders must be diligent, implement a robust anti-fraud strategy, and discourage all improper practices. Employee performance can also be strengthened through realistic anti-fraud preparation, and conformity with legal and regulatory obligations. Thus, fostering an ethical corporate culture is essential for fraud prevention.*

DOI: 10.4018/978-1-7998-5567-5.ch002

## **1. INTRODUCTION**

Fraud is a law infringement that is created by a person for his/her own gain. Fraud has been one of the most troublesome obstacles to economic growth (Azim & Azam, 2016). Fraud is an intentional act with an intention to damage anyone. Fraud includes stealing, corruption, conspiracy, embezzlement, money laundering, bribery, and extortion. The legal definition can be different in each country. Deception, dishonesty, and ethical misconduct are all common examples of fraudulent behaviors. Shoplifting, embezzlement, and other forms of digital crimes are everyday hazards for business owners. Businesses stand to lose a lot of profit and income as a result of fraud. Regardless of the size of business, industry, or country, fraud is one of the biggest problems that most organizations are facing today. Fraud has been evolving and increasing with the change in the production, work environment, organizational structures, industrialization, and legislation.

Business organizations with valuable property (i.e., cash, goods, information, or services) are likely to attract fraudsters. The ACFE (2016) report explains that small businesses (particularly those with less than 100 employees) suffer fraud more frequently than large organizations and are hit by higher average losses. Generally, once large fraud hits a small company, it is less likely to absorb the damage than a larger company. When looking at fraud through the small business proprietor and manager lens, there are many significant problems to address, such as interpersonal relationships. Unfortunately, many small business workers have betrayed their employers by taking advantage of their jobs for financial gain (Ding & Wu, 2014). Accounting fraud also results in significant monetary losses. There are catastrophic consequences for the economy and the state because of financial losses. In some cases, fraud is a result of poor controls or non-existent controls. Fraud affects many business sectors, including schools, charity, health care services, banks, manufacturing, and pharmaceutical sectors. Ever-changing and improved technology has made it easy for counterfeiters to produce fake products. For example, in late 2006, 14 Siberian towns declared a state of emergency due to mass-poisonings caused by fake vodka. Around 900 people were hospitalized with liver failure after drinking an industrial solvent sold as vodka.

## **2. BACKGROUND**

Trustworthiness in business is usually taken for granted because business owners believe workers can be trusted (Smith, 2016). This naive confidence causes business owners to become victims of workplace fraud which allows them to misappropriate properties. Both men and women commit fraud in every sector, except for the banking industry where women outnumber men (Bonny, Goode, & Lacey, 2015). If an employee is motivated to commit fraud, that person could be of any age or gender and may appear trustworthy. When companies know that they are not immune to occupational fraud, researchers need to continue research on occupational fraud and workplace monitoring procedures. Fraud is one of the most challenging issues to solve (Gullkvist & Jokipii, 2013). Van Gelder and DeVries (2016) indicated that there is a lack of facts regarding employee misconduct by ordinary employees, considering the incidence of employee theft. High-profile white-collar offences are more discussed in research although fraud in the workplace is more frequently committed. Occupational fraud now has gained relatively large research attention.

Sutherland (1983) introduced the term white-collar crime. White-collar fraud occurs when persons in senior positions use their power and position to manipulate legislation decisions in their favor (Fried-

richs, 2004). It is a classical form of fraud caused by employees as an abuse of power. This form of fraud occurs in the workplace environment if there are unclear policies or procedures to control deceitful behavior. White-collar crimes also involve acts like theft, false statements, evasion, manipulation of information, etc. Data from the Report released by the Association of Certified Fraud Examiners (ACFE, 2009) found that businesses had at least 5% of fraud-related revenue losses. Moreover, KPMG's (2010) Fraud Survey reported a marked rise in total fraud levels, with employee fraud being by far the most prevalent form of fraud.

The most frequently used operational definitions for fraud used in this discussion are the following.

- *Fraud*: It refers to deliberate misconduct which involves fraudulent financial reporting and theft, embezzlement or forgeries (Song, Lee & Cho, 2013).
- *Fraud Triangle*: Fraud Triangle has three aspects which are the opportunity to deceive, the pressure to deceive, and the reasoning for those who cheat. A fraudster's motivation is money, the pressure to perform, or fear of losing power or status (Morales, Gendron & Guénin-Paracini, 2014).
- *Asset misappropriation*: Asset misappropriation is the act of individual stealing and misusing the assets of another (Nia & Said, 2015).
- *Occupational fraud*: Occupational fraud is the act of an employee who misuses his power in business dealings in the manner that is against the teachings of his employer (Timofeyev, 2015).

### **3. FRAUD THEORIES – A BRIEF REVIEW**

#### **3.1. Fraud Triangle/Diamond Models and Rationalization**

The fraud triangle is helpful for assessing the most appropriate internal controls to discourage and track workplace fraud (Wright, Tibbetts, & Daigle, 2014). Boyle, Boyle, and Mahoney (2015) noted that the potential to conduct fraud inside an organization is ever-present. An organization's internal controls' primary role is to solve the fraud triangle's incentive aspect. Independent assessment of each aspect of the fraud triangle helps auditors to define the fraud risk exposure of an entity (Mock, Srivastava, & Wright, 2017). To break down a multifaceted fraud risk judgement, Mock *et al.* (2017) suggested a separate assessment of each fraud triangle portion. Poor internal controls render companies open to misappropriation of assets and other kinds of fraudulent acts. Since incentive, pressure, and rationalization are present when criminal conduct happens, external auditors need to use the fraud triangle model in combination with other fraud risk management measures (Schnader, Bedard, & Cannon, 2015). Murdock (2008) contends that social pressure, addictions, and lack of discipline can drive people to act unethically. Managers may use the Fraud Triangle as a tool for identifying and understanding the characteristics of perpetrators.

The rationalization of an employee to commit internal occupational fraud is a challenging feature of a fraud triangle. It is also unpredictable that the auditor does not observe the feelings of the fraudster (Boyle, Boyle, & Mahoney, 2015). Rationalization, therefore, is a key component of a fraud triangle and should not be ignored in the strategic assessment of fraud risk management procedures. Ishida, Chang, and Taylor (2016) argued that some individuals, who commit financial crimes, believe their actions are fair and make rationalizations to show to other parties that their acts are justified. The rationalizing

attitude of individual fraudsters is that of mindset, personality, or set of values that allow them to carry out fraudulent acts without knowingly and willingly showing regret.

Holtfreter (2015) argued that the same rationalization occurs when men and women deceive their employers. He found, however, that the motives for men and women were not the same. Cressey (1953) found that men's propensity to commit financial crimes was primarily caused by financial needs, including gambling debt or dependence. Another study by Cressey (1950) clearly indicates that fraud must be brought about by coercion, opportunity, or rationalization. Albrecht, Howe, & Romney (1984) show that rationalization leads managers to make aggressive accounts for their company's reputation. In essence, fraud behaviors force people to throw away their integrity. Rationalization is very common among first-time crime offenders. These are ordinary and honest people. In a bad situation, they explain the bad judgment to make it acceptable or justifiable. The widely publicized case of De-Laurey, the secretary, who robbed over £4.3 million of her employers at Goldman Sachs is an outstanding example of rationalization in motion. By convincing herself that she had earned the money she stole, De-Laurey rationalized her actions. De-Laurey believed that as a just reward for her dedication, discretion, and loyalty, she deserved the plundered amounts. She claimed she had the consent of her boss to make money in exchange for her essential services (ACFE, 2008). Some of these fraud cases, such as theft, embezzlement, resentment, or a feel of entitlement, stem from unfair policies.

Boyle, DeZoort, and Hermanson (2015) stated that the Fraud Triangle model had not been empirically tested compared to other frameworks to discuss its efficacy. Consequently, an alternate method was introduced to assess and contrast the efficacy of the triangle type of fraud. The diamond fraud model was an evolution of the fraud triangle (Wolfe & Hermanson, 2004). The rationalization is that the additional factor, capability, strengthens the fraud triangle by adding five cognitive capabilities (Schuchter & Levi, 2016). The first is individual expertise to locate a chance to conduct fraud. The second is the potential for stress to be endured. The third is an ego or confidence. The brain is the fourth since the fraudster needs to be smart enough to take advantage of vulnerabilities. The fifth aspect is coercion (Azrina, Ming & Bee, 2014). Wolfe and Hermanson (2004) claimed that a person's role or function leads to fraud cases. According to other studies, capabilities, including a personal ego and trust, often relate to fraud commitment. This suggests that theft suspects have a strong ego and trust, which motivates them to behave unlawfully. They assume that one cannot be easily identified or captured, and he/she can justify the issue and be appropriate even though the fraud is exposed.

### **3.2. Ethical Climate Theory**

Soltani (2014) claimed that an ethical environment encompassed the actions of management. Victor and Cullen (1988), who discovered the climate of ethical work, drew this idea from Soltani. They created the two-dimensional Ethical Climate Theory (ECT), which focused on a structure composed of ethical philosophy and community sociological theory (Simha & Stachowicz-Stanusch, 2015). Three behavioral constructs became the ethical aspect of the framework: egoism, benevolence, and principle; the sociological element consisted of human decision-making, organization, and culture (Simha & Stachowicz-Stanusch, 2015). Soltani (2014) concluded that the ethical climate was a multicultural notion that involved the tone, ethical community, and ethical leadership at the top. Soltani (2014) indicated that workplace crime's primary factors are of ECT rather than the elements of the fraud triangle. Trompeter, Carpenter, Jones, and Riley Jr (2014) indicated that several risk management frameworks might combat any fraud

incidence however, there is no specific model or system. Trompeter *et al.* (2014) believed that widening elements of the fraud triangle strengthen and help to organize a manager's discernment regarding fraud.

Clor-Proell, Kaplan, & Proell (2015) claimed that unwanted organizational goals expected by employers from employees encourage unethical activities. Morgan and Burnside (2014) concluded that executives' incentive to rationalize unethical conduct is only possible when the top management does not impose ethical behavior. Since the primary focus is on financial results, owners do what they believe is appropriate. The excuse that "everyone lies and cheats" may even be utilized by managers, telling themselves that their dishonest acts are reasonable and appropriate (Morgan & Burnside, 2014).

Research also depicts that employees face huge pressures to achieve their company's personal and corporate goals which ultimately cause them to look for methods of fraud (Mishra & Singh, 2017). Management, for example, can be pushed to meet or exceed stakeholders' standards. Management must meet deadlines, increase profits, but these factors contribute to dishonest behaviors. Increasing the willingness of managers and staff to commit fraud is triggered by the failure of the leading ethical culture (Sidorov, 2015).

### **3.3. Picoir Theory**

Many theories further explained the motives for fraud. PICOIR is a modern motivation theory for fraud. It is focused on the actions of managers. 'PICOIR' relates to pressure, integrity, capability, opportunity, integrity, and rationalization. It demonstrates that integrity is an important part of a person's response to fraud so it is used in the model twice. PICOIR believes that a person with high integrity is rational, whereas a person with low integrity is irrational. The PICOIR theory demonstrates that immorality may be difficult if an individual has a high degree of integrity. However, one with a low level of integrity can use his skills or profession to commit fraud offenses.

An individual's integrity is a crucial element in committing fraud (Albrecht *et al.*, 1984). Any individual may come under any strain, such as personal needs or gains, financial challenges, work frustration, and company results. Individuals with strong integrity will be less prone to perform a felony in those circumstances. Instead, employees with certain strong professional expectations will either ignore the scenario or demand recourse by their direct superiors over these deficiencies.

Murdock (2008) showed that financial difficulties or non-financial conditions might be the product of pressure that drives people to commit fraud. Non-financial pressure may emerge from a sense of political and social culture. For starters, if an individual does not want to seem to be a failure, that feeling would cause him/her to commit fraud. However, Rae, Subramaniam, & Sands, (2008) argued that people are driven to commit fraud by loss of personal integrity and other moral values. Murdock's (2008) research also suggested that wealth, ideology, manipulation, and ego cause people to commit fraud. Kranacher (2010) agreed that money, ideology, manipulation, and ego are critical variables that force fraudsters to go for fraud.

Manurung and Hardika (2015) examined pressure and fraud linked to financial stability, external pressure, and financial goals. The research found that inadequate monitoring, industry dynamics, and other factors such as non-rotation of auditors provide an incentive for fraud. Cohen, Ding, Lesage, and Stolowy (2010) analyzed the reasons that cause managers to commit fraud and described five circumstances that can lead managers to fraudulent activities. The incentives, opportunities, pressure, and expectations of an investment analyst, an institutional investor, and a major creditor are included in these

aspects. Achieving ambitious goals, a high degree of competitiveness and the desire to obtain equity to remain successful are other causes that contribute to fraud.

Cressey (1950) interviewed 250 criminals to identify factors that motivate individuals to commit fraud. The study clearly shows that for fraud to occur, pressure, opportunity, or rationalization must be present. Pressures arise from financial and non-financial factors. The financial pressures lead people to act fraudulently. It can arise from personal financial losses, declining sales, competition with other companies, greed, personal needs, desire to meet one's ends, personal debt, poor credit, the need to meet set goals, inability to meet financial forecasts, and unexpected financial needs. Non-financial pressures can be derived from the workplace environment, frustrations with work, or peer pressure that arise from setting unrealistic goals or pressure on employees to report better performance results (Murdock, 2008). For example, in 2007, a big construction company lost a huge amount of money through fraud committed by a manager at one of its subsidiaries. Sources explained that the manager made accounting irregularities for four years, including systematic misrepresentation of production volumes and sales in significant numbers (ACFE, 2008). The pressure varies depending on the individual's responsibility, disposition, or personality. It derives from personal discipline, social status, reputation, peers, groups, or work positions or responsibility. Those who have a high degree of integrity, confidence, or esteem often act ethically. Pressure creates opportunities that lead people to act illegally. Similarly, setting unrealistic demands or targets for employees in terms of production, profits, or sales increase can lead to a misrepresentation of financial statements or false accounting reports. Vinten (2004) explained that some managers could commit fraud to show escalating profits to avoid disclosing certain liabilities. Investors or businesses should set realistic objectives and goals to reduce pressure and demands imposed on their employees in production, profits, or sales increase.

#### **4. BUSINESS FRAUDS; TYPES AND IDENTIFICATION**

Fraud is not merely a domestic issue in developing and underdeveloped countries; it includes diverse players inside and outside the country (Murdock, 2008). Foreign organizations have made some attempts to alleviate suffering in developing and underdeveloped nations by providing development funds; however, their efforts have declined simply because they are sometimes robbed, rendering impoverished citizens much worse by refusing them their fair share of life-saving assistance (KPMG, 2016). Globally, abuse and bribery challenges still appear to challenge all the world's most influential organizations, donors and development agencies. In this respect, unethical conducts, dishonest practices, collusive practices, manipulative activities, and obstructive practices, compose the spectrum of behaviors that represent the modes and styles of corruption. Corruption as a mechanism entails selling, granting, accepting, or soliciting something of worth, explicitly or indirectly, to affect another person's actions inappropriately. For example, in African countries, corruption and frauds are one of the most critical barriers to growth. Public sector corruption and frauds are ranked as the most significant barrier to development and growth in many African countries. This has been observed in a survey of more than 150 high-ranking public officials and prominent civil society representatives from over 60 developing countries. African continent has made several attempts to combat graft. For example, in Uganda, The Avoidance of Abuse Act of 1970, The Law of the Inspector General of Government, 1988, the Anti-Corruption Act of 2009, and the Implementation of the Leadership Code of Conduct Act, 2002 have been enforced, however, the country's enforcement of anti-corruption activities has struggled (GIR, 2009).

## ***Frauds in Business Organizations***

Hussain, Kennedy, and Kierstead (2010) noticed that the most prevalent deceptive financial reporting practices are incorrect income identification, understatement of expenses/liabilities, and overstatement and misappropriation of funds. Financial and industrial crime statistics identify tax avoidance and money laundering as major financial crimes. KPMG (2013) obtained data from fraud investigations in Europe, the Middle East, Africa, the Americas, and the Asia-Pacific regions. A total of 596 fraudsters are examined that were engaged in criminal activities performed in 78 nations. Seventy percent of fraudsters were between 36 and 55 years. 61% of the cases were still workers, 41% having been employed with their company for more than six years. This study indicates that for many companies, workplace theft was a significant concern. The findings revealed that 56 percent of fraud cases emerge from asset misappropriation, 40 percent from embezzlement, 27 percent from acquisition fraud, and just 24 percent of fraud cases originate from other illegal actions. Similarly, the banking sector of India was investigated by Kundu & Rao (2014). The findings found that the banking industry was widely impacted by forged title-deeds, stolen controls, and worker theft. Deloitte's (2015) report on India's illicit practices found that line managers or senior managers' insufficient oversight leads to workers' corruption by deviating from standard procedures and controls. Other banking industry fraud threats involve online banking and ATM fraud, stealing credit cards and credentials, bribery and corruption. It takes a long time to detect instances of theft or to classify them. Swain and Pani (2016) researched the evolution of banking industry fraud and found that counterfeit money, search forgery, and loans without diligence are common banking frauds.

Fraud, especially asset misappropriation, has become a growing concern for business owners when internal controls have not been enforced (Lenz, 2016). One of the most common forms of workplace fraud, asset misappropriation, is second only to financial statement fraud (Kapardis & Papastergiou, 2016). Small firms frequently neglect internal controls, as such, they experience incredibly significant losses (Klein, 2015). The researcher said that 85% of workplace theft instances are due to the misappropriation of properties. Due to the financial obligation needed to enforce and retain controls, many small companies lack adequate internal controls (Alleyne & Amaria, 2013). However, the advantages of introducing internal controls outweigh the costs by avoiding asset misappropriation as losses are so costly for small businesses. Also, white-collar crimes have taken the form of misappropriation of assets based on employee privilege, notwithstanding the supervision of growing corporations by the owners over time (Lenz, 2016). Wolfe & Hermanson (2004) suggest that the employee's position and the task can violate organizational policies and regulations. A study by KPMG (2016) indicates that 60% of fraud cases emerge from poor organizational controls. In other words, when the practices, systems, or protocols of organizations are weak or not efficiently enforced, there are frauds, embezzlements, hostilities, corruption cases, or feelings of entitlement. Ghazali, Rahim, Ali, and Abidin (2014) noticed that due to inadequate organizational systems, fraudulent acts such as misappropriation of money, misleading statements for hours worked/overtime and bribery emerge that lead to severe financial losses for the companies.

Billing schemes are another type of fraud. This entails exploitation of the cash disbursement practices of a company for the benefit of an individual. For instance, to produce false records, a cashier may prompt payments to either an actual vendor or a shell corporation. Another type of employee fraud is payroll fraud. This can occur in multiple forms. An instance of payroll fraud entails handling a fake employee's payroll. Fictitious deception by workers happens when an individual manages time and attendance entries for an employee that may not work and, therefore, does not provide services to the organization. This suggests that different workers must split the primary work or activities related to financial management so that limited persons may have full access to the process, approve, and sign a



check. Another fraud concern is expense report fraud. According to the ACFE (2014), where an agent neglects to supply the original receipt, expenditure payment fraud happens, enabling workers to produce false receipts. For the criminals, technology has made theft far simpler to counterfeit. Fraudsters create incorrect merchandise and fake individuals who might be involved in buying their products or services. Overtime reporting fraud is another type of fraud that happens when workers overstate the hours employed, and the managers are unaware of it.

For fraud identification, knowing what motivates persons to commit fraud is essential. Perpetrators have a powerful propensity to conceal their acts. Fraudulent persons may be detected through such attitudes, such as social aloofness, work dissatisfaction, assets beyond means, ever increasing standard of living and changes in attitude. A form of a fraudster is the intermediate fraudster. These people start their job sincerely, but as things get rough or life circumstances modify their usual mode and transform them to deception. Fraud, like slippery-slope fraud, intimidation, deception, and tension, exists in several ways. Slippery-slope fraudsters seek to trade even though they are objectively unwilling to pay their loans or satisfy their contractual obligations. This could be relevant to everyday merchants or influential businesspersons. In this scenario, habits play an important role in one's desire to perform fraud interventions. The condition needs to be taken firmly, whether it is a trivial case such as petty robbery, expenses, or some other offence. Some predators are accidental fraudsters. It should be understood that in order to implement a strategy and attain personal advantage, a predator will foster fear. An individual may often use occupation or social standing to escape (Wolfe & Hermanson, 2004). Many of the most significant incidents of theft are perpetrated by workers or persons of experience. The study of the ACFE (2016) indicates that most of the fraud cases performed in companies are triggered by employees taking office supplies and cash.

Helenne Doody and Technical Information Service (2009) report show that an effective anti-fraud strategy has several components including prevention and detection. Organizations need to pay attention to the most common indicators, warning signs, and fraud alerts, to decrease fraudsters' likelihood.

## **5. FRAUD PREVENTION STRATEGIES**

One of the most efficient ways of coping with fraud is implementing tactics that will minimize incentives, restrict opportunities, and limit potential fraudsters' capacity to rationalize their acts. Preventive controls aim to decrease opportunities and minimize future criminals' temptation in the case of intentional acts of fraud. Prevention strategies include implementing laws/processes and activities to deter fraud from happening, such as training and fraud awareness. Implementing measures to deter fraud will help ensure a company's integrity.

In order to maintain an ethical organizational structure, avoiding fraud is economically profitable for society (Mishra & Singh, 2017). Research on questioning witnesses, seeking credible evidence, and their tendency to provide truthful information after a crime has been perpetrated, was undertaken by Vrij, Hope, & Fisher (2014). This voluntary interview testing is a technique that may be utilized by business owners during the recruiting phase. Owners can ask questions from the expected workers to judge their psychological state of mind. Interviewers should begin with open-ended questions to establish connections and move on to closed-ended questions to ask more precise responses relevant to the future employee's ethical expectations (Vrij *et al.*, 2014). In addition, individuals must have the ability to recognize frauds (Simser, 2014). Occupational violence continues its upward trend with the management and fraudulent

acts (Elliott, Marquis, & Neal, 2013). The tone of the management can be set by business owners. It is vital to enforce controls that management cannot circumvent because management usually is accountable for controlling internal controls and is comfortable with how the controls operate.

Hollow (2014) indicated that a division of roles and increased organizational communications are specific mechanisms. Kim and Kogan (2014) concluded that although it may be expensive to introduce, create, and retain fraud prevention controls, the benefit would be high enough to warrant the expense. Nevertheless, many companies do not have a systematic approach to fraud prevention based on recent surveys. The probability of retrieving stolen funds from the victim or insurance is also relatively low after a crime has already occurred. Prabowo (2014) believed that workplace fraud is prevalent and that new ways of doing business will continue to arise as technology continues to develop, and fraudsters would grow cleverer. According to Bardhan, Lin, & Wu (2015), smaller family-owned corporations appear to have weaker internal controls because of their priority to retain private profits, making them more susceptible to fraud than larger firms that impose tighter internal controls. Small company owners would also be liable for upholding a level of reasonability and ethics in reaching internal control targets (Gupta *et al.*, 2013). Internal controls of small business owners should have to be revisited and updated to ensure that their processes and practices remain successful in avoiding misappropriation of funds. In order to ensure successful theft mitigation measures, company owners can integrate background checks and regular staff training into their business plans (Leistedt & Linkowski, 2016). Gupta, Weirich, and Turner (2013) concluded that there is no complete system of internal controls for every sector and that there is a space for adjustments.

Employees should be allowed to set organizational priorities or decision-making to reduce their dissatisfaction and anger to eliminate falsified accounting records. Engaging workers in the decision-making process can also improve their efficiency and productivity while simultaneously minimizing mistakes. For checks and balances, companies should also have appropriate policies and procedures in place. Employees should be kept to the same requirements in order to minimize workplace theft. In terms of pay, benefits, job assignments, and promotion opportunities, preferring one employee over others leads to resentment or a sense of entitlement. It should handle excellent workers well, but this should be extended to other employees also. Management should further allow employees to participate in the decision-making process and goal setting to avoid such fraud cases of misrepresentation of accounting records. To reduce the fraud risks, occupational fraud, losses, or presentation of fake information, managers should support employees and reward them fairly.

Organizational managers should take the time to review and validate documentation for accuracy. Employees are tricky; they can lie and never pay for their expense accounts. Taking the example of Inventories, more efforts should be made to conduct routine inventory checks. Periodic reconciliations are required as a fraud control standard. It is also essential to cross-check the figures with the bank slip deposits to ensure that nothing is missing and that everything adds up. To ensure that there are no fraudulent transactions, organizations can also perform frequent checks of the online declaration. Managers must be prudent not to share their electronic signatures or delegate the signature authority to other people. It is also essential for the manager to make regular or random checks on what has been signed. When fraud is revealed, managers should act on the matter publicly, immediately, and directly. It will also help companies mitigate fraud risks by involving internal auditors, accredited fraud examiners, audit committees, and external auditors.

Grant Thornton (2016) indicated that companies can perform comprehensive background checks during new hiring, promotion, and work rotations. Duty segregation is important for the prevention

of fraud. Custody, consent, custody of source documents, bookkeeping, and records management are included in the division of duties. Therefore, one person should not have the sole power to initiate, authorize, or approve a transaction, complete the transaction without adequate sign-off procedures and various management approval levels. The lack of sufficient internal controls leads workers to fraud. Training programs for anti-fraud are also essential to raise awareness. Recruiting, selection, and risk management techniques should also include fraud awareness and training. Employees, administrators, and personnel working in high-risk sectors, such as finance, procurement, bill paying, and those with a role in fraud prevention and detection, like human resources and investigation-responsible internal auditors, should be given significant consideration (Petraşcu & Tieanu, 2014). In order to detect and avoid irregular employee activities, companies should perform fraud risk assessments annually. To evaluate the effect and probability of fraud, risk management should include all company divisions and processes. The anti-fraud policies should also concentrate on non-financial considerations, such as credibility and business relations. Finally, employee recruitment and selection should not be based on ability, experience, and merit, but the worker's morals, ethics, and honesty should also be checked. These procedures are essential for the prevention of fraud. Both 'overt' and 'covert' approaches and assessments should be implemented during the selection process.

It is also essential for fraud prevention to develop effective policies and procedures. In order to improve internal control mechanisms, regular reviews of organizational policies and processes are necessary to ensure fraud prevention on time. Management should adopt a risk evaluation strategic plan. The global fraud survey by KPMG (2016) revealed that fraudsters find openings in their lax internal controls and processes that encourages them to plan fraud. Furthermore, the study suggested that fraud can be minimized by providing workers with equal wages or prompt promotion (Olaniyi, Saad, Abiola, & Adebayo, 2013). Management should, however, ensure that such policies are communicated efficiently and that they are well known and accepted by all to minimize fraud risks. Organizations should also set up serious protocols to prevent future criminals from committing fraud.

## **6. FRAUD DETECTION MECHANISMS**

Fraud prevention steps alone are not adequate enough since a fraud prevention mechanism that is completely safe cannot be enforced (Kim & Kogan, 2014). As fraud prevention strategies cannot deter all possible perpetrators, companies should ensure that monitoring mechanisms is in place that will promptly identify fraud occurrences. Analytical and other techniques to highlight irregularities and implement monitoring systems that allow for the communication of alleged fraudulent activities should be part of a fraud detection strategy. Exception reporting, data mining, pattern analysis, and ongoing risk management should be included in a robust fraud detection framework. The use of routine internal audits, whistleblowing, fraud policy, IT protection, pre-employment criminal background checks, and training to identify and avoid fraud incidents are other fraud detection mechanisms (Ghazali *et al.*, 2014). Fraudsters can bypass the control systems. Therefore, organizations must act proactively and devise new methods and techniques to assess the integrity of employees. Organizations should use background checks and behavior analytics to assess existing employees to reduce fraud risks regularly. PWC (2014) researched that data visualization, behavioral analytics, deep learning, flexible audit plan are beneficial for fraud detection. Tools like benchmarking, automation, security, and cameras are adequate internal controls for fraud detection.

Warren, Moffitt, and Byrnes (2015) recommended the usage of big data to identify accounting frauds. However, these techniques may extend to every discipline. Warren *et al.* (2015) suggested the usage of video evidence, audio data, and written data such as e-mail. The fraud triangle components are beneficial in reviewing text in e-mails from dissatisfied workers to identify and forecast potential fraud. Potential drawbacks with this surveillance system might be overused, making ethical workers feel dissatisfied about more intensive surveillance. Management should determine whether more damage than benefit will be induced by this form of fraud detection. For example, if workers feel that leadership is too disruptive, they will become less empowered and less efficient. The skills of employees should be periodically reassessed because individuals will change over time. Mawanza (2014) illustrates that consistently monitoring the skills of workers increases comprehension of human behaviors.

Whistleblowing can be the most powerful fraud detection tool that may end an existing fraud scheme as was the case of Enron (Gao, Greenberg, & Wong-On-Wing, 2015; MacGregor & Stuebs, 2014). According to Ahmad, Yunus, Ahmad, & Sanusi (2014) whistleblowing is one of the most significant sources to expose corporate misconduct. However, for staff to be free to expose wrongdoing without fear of retaliation, the most efficient outlets, such as anonymous hotlines, should be open. Potential informants have the right to disclose a criminal act, they are aware of, as an ethical responsibility but should not be fearful of punishment from the fraudsters (Gao *et al.*, 2015; MacGregor & Stuebs, 2014). Whistleblowing is highly advocated to expose and discourage illegal corporate behavior as an internal management tool. It is challenging and burdensome to blow the whistle on peers or managers; thus, it will require a person with solid ethical values, bravery, and morality to blow the whistle. Some people are concerned about their integrity while others may criticize them for whistleblowing; suspect them of their organization's disloyalty by possibly ruining the organization's reputation and disclosing insider misconduct. In comparison, whistleblowers are often lauded for defending their organization from inside predators who undermined the organization's continuing concern (Zakaria, 2015).

Brown, Hays, and Stuebs Jr (2016) indicated three classifications of whistleblowers; accountants, women, and management at the senior level. As indicated by Gao *et al.* (2015) and MacGregor & Stuebs (2014), lower-level workers are less willing to blow the whistle out of fear of retribution, work loss, and risk to the jobs. Given the whistleblowing imperfections for certain people's inability to disclose wrongdoing, it remains one of the most effective fraud detection methods (Brown *et al.*, 2016). In the wake of major accounting misconduct in the early 2000s, whistleblowing programs became necessary for big companies, and whistleblowing was a method used to detect false financial statements (Johansson & Carey, 2016). Johansson and Carey (2016) argued that the fraud triangle offered a basis for explaining how whistleblowing was increased by anonymous reporting networks. An anonymous reporting network promotes whistleblowing because, without repercussion, staff may expose illegal actions such as asset misappropriation anonymously. They claimed that its use applies to other forms of fraud, such as wealth misappropriation. In companies where anonymous reporting exists; analysts say that workers disclose theft more commonly in smaller businesses than in large corporations (Johansson & Carey, 2016). Through the use of anonymous reporting networks, whistleblowing can become a more successful method for detecting fraud.

## **7. CONCLUDING REMARKS AND SUGGESTIONS**

The purpose of this chapter was to discuss the fraud theories and prevention/detection mechanism of fraud. Today, fraud is one of the biggest problems that exist and the number of cases has been increasing day by day (ACFE, 2014). Therefore, understanding the fraud prevention and detection is vital for the business organization. The key is good governance in order to reduce corruption in society. Unfortunately, due to the weak governance and inequality in some countries, corruption is proliferating and perpetuating. The temptation to transform public assets into private gains remains reasonably strong in most of the situations. Fraudsters must, regardless of their rank, be taken out in the open and disciplined. Therefore, cultural responsibility, honesty, dignity, morality, and ethical standards of corporate activities must be enforced.

Efforts have been made over the years to prevent and detect fraud. It presents causes that inspire individuals to commit fraud, offers methods for identifying fraud, avoidance, and motives to encourage people to commit fraud. Pressure, incentive, or rationalization must be present for fraud to occur, according to the Fraud Theory Triangle (Cressey, 1950). Money, greed, manipulation, job pressures, family needs, opportunity, politics, rationalization, belief in entitlement, rationalization, lack of integrity, poor oversight, and a lack of ethics are the important reasons that lead people to behave fraudulently.

Organizations should devote time and money to tackling fraud, considering the nature of fraud and the harmful effects correlated with it. To defend organizations from fraud, internal procedures, ethical codes, and regulatory legislation are necessary to strengthen the processes. To identify frauds, management must be cautious and therefore should develop processes to reduce fraud threats. Organizational leaders must be diligent, implement a robust anti-fraud strategy, and discourage all improper practices. Employee performance can also be strengthened through realistic anti-fraud preparation, and conformity with legal and regulatory obligations. Organizations that lack corporate governance systems, have poor IT security, and under-standard internal controls are more prone to find possible opportunities for fraud. Thus, management must ensure that internal control mechanisms, including their procedures, enforcement rules have been adequately developed, introduced, and managed. Management must also try to eliminate the vulnerabilities that offer criminals the chance to commit fraud. Organizations can use IT protection, anti-fraud programs, training, supervision, whistleblowing, background checks, auditing, division of duties, and other relevant mechanisms to deter fraud. Organizations must be equipped to solve significant issues impacting the equity of shareholders. Misappropriate assets are widely known to fraudsters, rendering fraudulent investments appear real to auditors. Organizations are also advised to minimize the number of vendors and periodically check vendors' list to reduce the possibility of vendor fraud. The segregation of duties is also essential and the organizations should adopt a law for the segregation of duties among employees to minimize frauds. In other terms, corruption is a concerted activity purposely committed by an actor. Organizations may use specific approaches and techniques like data visualization, predictive intelligence, and a versatile audit plan. In identifying fraudsters, benchmarking, automatic controls, decision trees, networking, and help vector machines are also useful (West, Bhattacharya, & Islam, 2014).

It is concluded that for fraud prevention and detection, fostering an ethical corporate culture is essential. It is often crucial within corporate processes and occupations to reinforce fundamental principles and ethical codes. Therefore, until it impacts corporate efficiency, every employee must tackle fraud and avoid it. In reality, the conduct of theft causes persons to give away their dignity.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## **REFERENCES**

ACFE. (2008). *Fraud risk management: a guide to good practice*. ACFE.

ACFE. (2009). *Fraud examiners manual*. ACFE.

ACFE. (2014). *Report to the Nation on Occupational Fraud and Abuse*. ACFE. Retrieved from <https://www.acfe.com/rtnn/docs/2014-report-to-nations.pdf>

ACFE. (2016). *Report to the Nations on Occupational Fraud and Abuse*. Global Fraud Study. Retrieved from <https://www.acfe.com/rtnn2016/docs/2016-report-to-the-nations.pdf>

Ahmad, S. A., Yunus, R. M., Ahmad, R. A. R., & Sanusi, Z. M. (2014). Whistleblowing behaviour: The influence of ethical climates theory. *Procedia: Social and Behavioral Sciences*, 164, 445–450. doi:10.1016/j.sbspro.2014.11.101

Albrecht, W. S., Howe, K. R., & Romney, M. B. (1984). *Deterring Fraud: The Internal Auditor's Perspective*. Institute of Internal Auditors Research Foundation.

Alleyne, B., & Amaria, P. (2013). The effectiveness of corporate culture, auditor education, and legislation in identifying, preventing, and eliminating corporate fraud. *International Journal of Business Accounting and Finance*, 7(1), 34–62.

Azim, M., & Azam, S. (2016). Bernard Madoff's 'Ponzi Scheme': Fraudulent Behaviour and the Role of Auditors. *Accountancy Business and the Public Interest*, 15(1), 122–137.

Azrina, M. Y. N., Ming, L. L., & Bee, W. Y. (2014). Tax non-compliance among SMCs in Malaysia: Tax audit evidence. *Journal of Applied Accounting Research*, 15(2), 215–234. doi:10.1108/JAAR-02-2013-0016

Bardhan, I., Lin, S., & Wu, S. L. (2015). The quality of internal control over financial reporting in family firms. *Accounting Horizons*, 29(1), 41–60. doi:10.2308/acch-50935

Bonny, P., Goode, S., & Lacey, D. (2015). Revisiting employee fraud: Gender, investigation outcomes and offender motivation. *Journal of Financial Crime*, 22(4), 447–467. doi:10.1108/JFC-04-2014-0018

Boyle, D. M., Boyle, J. F., & Mahoney, D. P. (2015). Avoiding the fraud mind-set. *Strategic Finance*, 96(8), 41–47.

Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, 34(6), 578–596. doi:10.1016/j.jaccpubpol.2015.05.006

Brown, J. O., Hays, J., & Stuebs, M. T. Jr. (2016). Modeling accountant whistleblowing intentions: Applying the theory of planned behavior and the fraud triangle. *Accounting and the Public Interest*, 16(1), 28–56. doi:10.2308/apin-51675

Clor-Proell, S. M., Kaplan, S. E., & Proell, C. A. (2015). The impact of budget goal difficulty and promotion availability on employee fraud. *Journal of Business Ethics*, 131(4), 773–790. doi:10.1007/10551-013-2021-7

Cohen, J., Ding, Y., Lesage, C., & Stolowy, H. (2010). Corporate Fraud and Managers' Behavior: Evidence from the Press. *Journal of Business Ethics*, 95(2), 271–315. doi:10.1007/10551-011-0857-2

Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review*, 15(6), 738–743. doi:10.2307/2086606

Cressey, D. R. (1953). *Other People's Money: The social psychology of embezzlement*. The Free Press.

Deloitte. (2015). *India Banking Fraud Survey-Edition II*. Deloitte. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fabanking-fraudsurvey-noexp.pdf>

Ding, S., & Wu, Z. (2014). Family ownership and corporate misconduct in U.S. small firms. *Journal of Business Ethics*, 123(2), 183–195. doi:10.1007/10551-013-1812-1

Elliott, T. L., Marquis, L. M., & Neal, C. S. (2013). Business ethics perspectives: Faculty plagiarism and fraud. *Journal of Business Ethics*, 112(1), 91–99. doi:10.1007/10551-012-1234-5

Friedrichs, D. (2004). Enron Et Al.: Paradigmatic White Collar Crime Cases for the New Century. *Critical Criminology*, 12(2), 113–132. doi:10.1023/B:CRIT.0000040258.21821.39

Gao, J., Greenberg, R., & Wong-On-Wing, B. (2015). Whistleblowing intentions of lower-level employees: The effect of reporting channel, bystanders, and wrongdoer power status. *Journal of Business Ethics*, 126(1), 85–99. doi:10.1007/10551-013-2008-4

- Ghazali, M. Z., Rahim, M. S., Ali, A., & Abidin, S. (2014). A Preliminary Study on Fraud Prevention and Detection at the State and Local Government Entities in Malaysia. *Procedia: Social and Behavioral Sciences*, 164(1), 437–444. doi:10.1016/j.sbspro.2014.11.100
- GIR. (2009). *Global Integrity Report: 2009-Key Findings*. Retrieved from <http://www.globalintegrity.org>
- Grant Thornton. (2016). *Financial and corporate frauds*. New Delhi: India. Retrieved from <https://www.grantthornton.in/globalassets/1.-member-firms/india/assets/pdfs/financialand-corporate-frauds.pdf>
- Gullkvist, B., & Jokipii, A. (2013). Perceived importance of red flags across fraud types. *Critical Perspectives on Accounting*, 24(1), 44–61. doi:10.1016/j.cpa.2012.01.004
- Gupta, P. P., Weirich, T. R., & Turner, L. E. (2013). Sarbanes-Oxley and public reporting on internal control: Hasty reaction or delayed action? *Accounting Horizons*, 27(2), 371–408. doi:10.2308/acch-50425
- Helenne Doody and Technical Information Service. (2009). *Corporate Fraud - Topic Gateway* (Series No. 57). London: CIMA. Retrieved from [https://www.cimaglobal.com/Documents/ImportedDocuments/cid\\_tg\\_corporate](https://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_corporate)
- Hollow, M. (2014). Money, morals and motives: An exploratory study into why bank managers and employees commit fraud at work. *Journal of Financial Crime*, 21(2), 174–190. doi:10.1108/JFC-02-2013-0010
- Holtfreter, K. (2015). General theory, gender-specific theory, and white-collar crime. *Journal of Financial Crime*, 22(4), 422–431. doi:10.1108/JFC-12-2014-0062
- Hussain, M. M., Kennedy, P., & Kierstead, V. (2010). Can audit prevent fraudulent financial reporting practices? Study of some motivational factors in two Atlantic Canadian entities. *Issues in Social and Environmental Accounting*, 4(1), 65–73. doi:10.22164/isea.v4i1.47
- Ishida, C., Chang, W., & Taylor, S. (2016). Moral intensity, moral awareness and ethical predispositions: The case of insurance fraud. *Journal of Financial Services Marketing*, 21(1), 4–18. doi:10.1057/fsm.2015.26
- Johansson, E., & Carey, P. (2016). Detecting Fraud: The Role of the Anonymous Reporting Channel. *Journal of Business Ethics*, 139(2), 391–409. doi:10.1007/10551-015-2673-6
- Kapardis, M. K., & Papastergiou, K. (2016). Fraud victimization in Greece: Room for improvement in prevention and detection. *Journal of Financial Crime*, 23(2), 481–500. doi:10.1108/JFC-02-2015-0010
- Kim, Y., & Kogan, A. (2014). Development of an anomaly detection model for a bank's transitory account system. *Journal of Information Systems*, 28(1), 145–165. doi:10.2308/isis-50699
- Klein, R. (2015). How to avoid or minimize fraud exposures. *The CPA Journal*, 85(3), 6.
- KPMG. (2010). *Fraud and Misconduct Survey 2010*. Retrieved from: <http://www.kpmg.com>
- KPMG. (2013). *KPMG Malaysia Fraud, Bribery and Corruption survey 2013*. Retrieved from: <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/fraud-survey-report.pdf>



- KPMG. (2016). *Global profiles of the fraudster: Technology enables and weak controls fuel the fraud*. Retrieved, from [https:// assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf](https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf)
- Kranacher, M. J. (2010). Bringing the world together on one standard. *The CPA Journal*, 80(10), 17.
- Kundu, S., & Rao, N. (2014). Reasons of Banking Fraud-A Case of Indian Public Sector Banks. *International Journal of Information Systems Management Research and Development*, 4(1), 11–24.
- Leistedt, S. J., & Linkowski, P. (2016). Fraud, individuals, and networks: A biopsychosocial model of scientific frauds. *Science & Justice*, 56(2), 109–112. doi:10.1016/j.scijus.2016.01.002 PMID:26976469
- Lenz, R. (2016). Peer-to-Peer Lending: Opportunities and Risks. *European Journal of Risk Regulation*, 7(4), 688–700. doi:10.1017/S1867299X00010126
- MacGregor, J., & Stuebs, M. (2014). The silent Samaritan syndrome: Why the whistle remains unblown. *Journal of Business Ethics*, 120(2), 149–164. doi:10.1007/10551-013-1639-9
- Manurung, D. T., & Hardika, A. L. (2015). *Analysis of factors that influence financial statement fraud in the perspective fraud diamond: Empirical study on banking companies listed on the Indonesia Stock Exchange year 2012 to 2014*. Paper presented at International Conference on Accounting Studies. Retrieved from <http://repo.uum.edu.my/17583/>
- Mawanza, W. (2014). An analysis of the main forces of workplace fraud in Zimbabwean organisations: The fraud triangle perspective. *International Journal of Management Sciences and Business Research*, 3(2), 86–94. doi:10.2139/ssrn.2463235
- Mishra, S., & Singh, G. (2017). Forensic accounting: An emerging approach to deal with corporate frauds in India. *Global Journal of Enterprise Information System*, 9(2), 104–109. doi:10.18311/gjeis/2017/15922
- Mock, T. J., Srivastava, R. P., & Wright, A. M. (2017). Fraud risk assessment using the fraud risk model as a decision aid. *Journal of Emerging Technologies in Accounting*, 14(1), 37–56. doi:10.2308/jeta-51724
- Morales, J., Gendron, Y., & Guénin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. *Accounting, Organizations and Society*, 39(3), 170–194. doi:10.1016/j.aos.2014.01.006
- Morgan, A. R., & Burnside, C. (2014). Olympus corporation financial statement fraud case study: The role that national culture plays on detecting and deterring fraud. *Journal of Business Case Studies*, 10(2), 175–184. doi:10.19030/jbcs.v10i2.8506
- Murdock, H. (2008). The three dimensions of fraud: Auditors should understand the needs, opportunities, and justifications that lead individuals to commit fraudulent acts. *The Internal Auditor*, 65(4), 81–83.
- Nia, E. H., & Said, J. (2015). Assessing fraud risk factors of assets misappropriation: Evidences from Iranian banks. *Procedia Economics and Finance*, 31, 919–924. doi:10.1016/S2212-5671(15)01194-6
- Olaniyi, T. A., Saad, T., Abiola, W. O., & Adebayo, S. A. (2013). Employee motivation and public sector fraud: Evidence from kwara state, Nigeria. *Journal of Humanities. Social Sciences and Creative Arts*, 8(1), 13–24.

- Petraşcu, D., & Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance*, 16, 489–497. doi:10.1016/S2212-5671(14)00829-6
- Prabowo, H. Y. (2014). To be corrupt or not to be corrupt. *Journal of Money Laundering Control*, 17(3), 306–326. doi:10.1108/JMLC-11-2013-0045
- PWC. (2014). *Economic crime: A threat to business globally*. Retrieved from <https://www.pwc.com/gx/en/economic-crime-survey/pdf/pwc-latin-america-economic-crime-survey.pdf>
- Rae, K., Subramaniam, N., & Sands, J. (2008). Risk management and ethical environment: Effects on internal audit and accounting control procedures. *Journal of Applied Management Accounting Research*, 6(1), 11–30.
- Schnader, A. L., Bedard, J. C., & Cannon, N. (2015). The principal-agent dilemma: Reframing the auditor's role using stakeholder theory. *Accounting and the Public Interest*, 15(1), 22–26. doi:10.2308/apin-51234
- Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. *Security Journal*, 29(2), 107–121. doi:10.1057j.2013.1
- Sidorov, J. (2015). Best practices for health outcomes public reporting. *Population Health Management*, 18(6), 399–401. doi:10.1089/pop.2015.0033 PMID:26091187
- Simha, A., & Stachowicz-Stanusch, A. (2015). The effects of ethical climates on trust in supervisor and trust in organization in a Polish context. *Management Decision*, 53(1), 24–39. doi:10.1108/MD-08-2013-0409
- Simser, J. (2014). Culpable insiders-the enemy within, the victim without. *Journal of Financial Crime*, 21(3), 310–320. doi:10.1108/JFC-11-2013-0068
- Smith, R. (2016). Of bad-seed, black-sheep and prodigal-sons. *International Journal of Entrepreneurial Behaviour & Research*, 22(1), 39–62. doi:10.1108/IJEBr-04-2014-0059
- Soltani, B. (2014). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals. *Journal of Business Ethics*, 120(2), 251–274. doi:10.1007/10551-013-1660-z
- Song, D. B., Lee, H. Y., & Cho, E. J. (2013). The association between earnings management and asset misappropriation. *Managerial Auditing Journal*, 28(6), 542–567. doi:10.1108/02686901311329919
- Sutherland, E. H. (1983). *White collar crime: The uncut version*. Yale University Press.
- Swain, S., & Pani, L. K. (2016). Frauds in Indian banking: Aspects, reasons, trend-analysis and suggestive measures. *International Journal of Business and Management Invention*, 5(7), 1–9.
- Timofeyev, Y. (2015). Analysis of predictors of organizational losses due to occupational corruption. *International Business Review*, 24(4), 630–641. doi:10.1016/j.ibusrev.2014.11.007
- Trompeter, G. M., Carpenter, T. D., Jones, K. L., & Riley, R. A. Jr. (2014). Insights for research and practice: What we learn about fraud from other disciplines. *Accounting Horizons*, 28(4), 769–804. doi:10.2308/acch-50816

- Van Gelder, J. L., & De Vries, R. E. (2016). Traits and states at work: Lure, risk and personality as predictors of occupational crime. *Psychology, Crime & Law*, 22(7), 701–720. doi:10.1080/1068316X.2016.1174863
- Victor, B., & Cullen, J. B. (1988). The organizational bases of ethical work climates. *Administrative Science Quarterly*, 33(1), 101–125. doi:10.2307/2392857
- Vinten, G. (2004). The future of UK internal audit education: Secularisation and submergence? *Managerial Auditing Journal*, 19(5), 580–596. doi:10.1108/02686900410537810
- Vrij, A., Hope, L., & Fisher, R. P. (2014). Eliciting reliable information in investigative interviews. *Policy Insights from the Behavioral and Brain Sciences*, 1(1), 129–136. doi:10.1177/2372732214548592
- Warren, J. D. Jr, Moffitt, K. C., & Byrnes, P. (2015). How Big Data Will Change Accounting. *Accounting Horizons*, 29(2), 397–407. doi:10.2308/acch-51069
- West, J., Bhattacharya, M., & Islam, R. (2014). Intelligent Financial Fraud Detection Practices: An Investigation. *Computers & Security*, 57, 47–66. doi:10.1016/j.cose.2015.09.005
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.
- Wright, J. P., Tibbetts, S. G., & Daigle, L. E. (2014). *Criminals in the making: Criminality across the life course*. Sage Publications.
- Zakaria, M. (2015). Antecedent factors of whistleblowing in organizations. *Procedia Economics and Finance*, 28, 230–234. doi:10.1016/S2212-5671(15)01104-1

## Chapter 3

# Powerlessness as the Basis for Financial Crimes: A Brief Overview

Tayo Oke

*Afe Babalola University, Nigeria*

### ABSTRACT

*Scholarly analysis of financial crime, its modus operandi, and the characters involved have almost exclusively been focused on the activities of the elite and the powerful for decades. Recommendations on how to minimise its debilitating impact have always, also, been focused on the elite, the powerful, and the state institutions they control. Corruption and financial crime are the pastime of people at the top only. This overview contends that perpetration of financial crime by the powerless can be just as corrosive and harmful as that perpetrated by the powerful. The quality of criminality and its pervasiveness is as relevant as its quantum and location. Exclusive focus on the higher echelons of financial crime subsumes its roots and significance within society, thereby leading to the lop-sidedness of proposed remedies. This chapter seeks to establish the nexus between low- and high-level financial crime as a way of providing a more holistic view of the depth of its effect, especially in less sophisticated economic environments.*

### INTRODUCTION

This chapter was inspired by two profound sayings from two different and diverse political environments, across the Atlantic, trying to unravel the Gordian knot. First, is noble Lord Acton, the 19<sup>th</sup> century historian, and British Parliamentarian, who opined: “*Power tends to corrupt, and absolute power corrupts absolutely*”. This was said about elite corruption and abuse of office, which has remained the fulcrum of analysis of corruption and financial crime ever since. The other is a Yoruba<sup>1</sup> saying: ‘*A mukun eru e wo..*’ (Seized by the tilted load on the head of the semi-crippled). To elaborate in plain English, and with a modicum of imagination, when you observe the rotten fruits on a tree in isolation of its decomposing roots, and start passing judgement, the tree then beckons you to focus your attention on the bottom first. Of course, but for the decomposing roots, the fruits would not have been so rotten. Similarly, but for the

DOI: 10.4018/978-1-7998-5567-5.ch003

semi-crippled legs, the load would not have become tilted. This is a wake-up call to those who often cannot see the forest for the trees; a jolt for the observer to smell the coffee, and an invitation for the assessor to separate the wheat from the chaff. In the area of finance, elite criminality may be bad and odious, but it is not the original sin. Financial crime cannot be dissected in isolation of its less visible, less prominent, but equally potent roots in society.

The concept put forward in this chapter is a radical departure from conventional wisdom, the characters under the microscope are not the usual suspects, but the premise upon which the analysis is based remains immutable<sup>2</sup>. It remains such because corruption is ‘found almost everywhere, but it is stubbornly entrenched in the countries of Sub-Saharan Africa, Latin American and Asian countries (Amundsen, 1999; Ibrahim, 2021). What is unravelled in this discussion is the assumption of the link between corruption, big cities and the state being the only show in town as it were. Rent seeking, no doubt, is a phenomenon that is present in developing economies. For the World Bank, corruption covers a broad range of human actions: bribery, theft, political and bureaucratic, isolated, and systemic, and private-sector corruption (Mundial, 1997). All these amount in some form to abuse of public office for private gain. Most definitions of corruption exclude ‘intra-societal corruption’, focussing instead, on state actors-society relations (Amundsen, 1999).

## **FRAGMENTATION OF STATE INSTITUTIONS**

The ‘fragmented’ nature of state institutions in developing countries is almost universally found to be the main culprit. This reasoning has a significance particularly in countries where there continues to be a question mark over the legitimacy of the state and its institutions. Powerful elites, no doubt, take advantage of the fragmentation to exert rent at all levels of interactions with citizens. It has sometimes been described as “*State capture*” (South Africa), “*Family Fiefdom*” (Angola and Guinea Equatorial) or the “*Oligarch*” (Russia and the former Soviet states). Others, still, have seen state fragmentation in terms of neo-patrimonialism as was the case in the Democratic Republic of Congo under the late strongman leader, Mobutu Sese-Seko. Neo-patrimonialism is made possible by non-compliance and non-conformity with formal rules. This too varies according to the size and structure of government, democracy and the political system, quality of institutions, economic freedom/openness of the economy, salaries of civil service, press freedom and the judiciary amongst others (Enste & Heldman, 2017). High-level corruption is a major problem in any event, but it does not tell the whole story.

For instance, when low-level officials collect bribes, which they share with superiors, it is called “bottom up” corruption (Rose-Ackerman & Palifka, 2016). Be it the police numerous checkpoints extorting pittance from motorists, or administrative officers demanding small amounts to process documents, it all adds up to the mounting trillions of dollars lost to bribery worldwide annually (Lawder, 2016). This amounts to at least 5% of the world’s gross domestic product (UN, 2018). A direct link between corruption and economic growth is a difficult one to quantify, but suffice it to say that corruption does have significant negative impacts on key economic structures, such as investment (especially foreign direct investment), competition, entrepreneurship, government efficiency, and human capital formation (OECD, 2020). If it is difficult to establish a direct link between corruption and economic growth, it is not so doing the same in respect of corruption and poverty. Poor people are more likely to be victims of corrupt behaviour by street-level government bureaucrats (Justesen & Bjørnskov, 2014).

The alternative explanation proposed later in this chapter does not take the ‘victim approach’ to low-level corruption in developing countries. It focuses on how cost of support for government action is imposed from the bottom up to counter grand-scale embezzlement. State is seen as illegitimate in the eyes of many at the bottom in many of the countries, either through lingering colonial arbitrary partition and ethnic schisms, or through decay in governmental structure over time. The cost passed on from below is then met through corrupt use of public office at the top. Corruption from below and corruption from above are intertwined; they are two opposite sides of the same coin. It is the existence of one which necessitates the existence of the other. A theory of high-level corruption is incomplete without a corresponding theory of low-level corruption. Corruption, by itself, does not produce poverty. Rather, corruption has direct consequences on economic and governance factors, intermediaries that in turn produce poverty (Chetwynd, Chetwynd & Spector, 2003; Alam *et al.* 2021). In other words, poverty is a relative term, not given to a single criterion.

## **MOTIVATION FOR CORRUPTION**

Human nature is a much complex phenomenon, it is difficult to measure what motives an individual to engage in a corrupt act. For a lot of people, corruption is an opportunity crime, for others, poverty is a powerful motivation. For others, still, it is sheer greed and abuse of office. Whichever model used in measuring it (rational choice, structural, cultural), corruption is debilitating, but it can also be a stabilizing factor in each policy (Løvseth, 2001). Based on this reasoning, corruption is principally a governance issue. A failure of institutions and a lack of capacity to manage society by means of a framework of social, judicial, political, and economic checks and balances. It is logically a demand and supply equilibrium. Among the factors affecting the demand are regulations and authorisations, tax systems, spending decisions, provision of goods and services at below market price. And on the supply side are bureaucratic traditions, level of public sector wages, penalty systems, institutional controls, transparency of rules, laws, and procedure, and finally, leadership (Tanzi, 1998). This ‘Washington’ perspective is generally correct in so far as it goes. The problem is that it is tilted towards measuring and devising solutions to metropolitan elite corruption rather than dissecting its roots in society. It avoids the analysis of the political-economic conditions that allows for ‘grand corruption’ to thrive (Jain, 2001).

Much of the focus by Western financial agencies on reducing corruption around the world is on making bribes more difficult to pay and accept, for instance, USA’s Foreign Corrupt Practices Act (1977), and the UK’s Bribery Act (2010). Nonetheless, corruption, defined more comprehensively, involves inappropriate use of political power and it reflects a failure of the political institutions within a society. The focus on power is relevant here, but it is the other side of the power configuration; powerlessness, that is at the discussion in this chapter. On that account, we find ourselves aligned with succinct issues posed by an influential research paper on this topic which asks: Under what political, social, and economic conditions is corruption likely to thrive? What are the costs of corruption to the poor and to the state? What anti-corruption interventions are effective and why? (DFID, 2015). The answers to these questions, according to the paper, lie in a further understanding of the difference between “administrative” and “political” corruption, as corruption is intricately linked with rent-seeking.

For this discussion, the questions are rather pertinent, but the tool of analysis is the dynamics of power and powerlessness as opposed to a narrow probe into ‘weak institutions’ and other similar indices. Given the enormous amount of money that is lost to bribery worldwide, it stands to reason that reducing

its quantum reduces the opportunity for illicit financial flows. The OECD report in 2014 canvassed for improvement in governance at the source, ‘through building a sound business environment and increasing opportunities for citizens, giving them incentives to engage in legal economic activities, pay their taxes and dues, and re-invest their profits and income (OECD, 2014). A good governance structure for taxes is mandatory to combat revenue leakages (Rafay & Ajmal, 2014). This ‘Eurocentric’ viewpoint is as valid as the ‘Washington’ stance highlighted earlier. They both attack the problem of corruption and illicit financial flows as a grand narrative of high-level crime in developing countries. The aim in this discussion is to expose its limitations and sketch a new analytical framework for understanding the financial crime in those countries.

Rational choice-inspired anti-corruption strategy of the West has largely failed because it explains corruption as the functioning of calculating, strategic, self-interested behaviour (Dupuy & Neset, 2018). Rational choice theories explain how one should reason, not how one actually reason. It is partly the failure of rational choice inspired diagnosis of financial crime in developing countries that serves as the impetus for radical alternative propositions of the kind we are engaged with in this chapter. A recent survey of 185 countries finds that corruption and shadow economy are poverty-driven and is highly prevalent in low-income countries. Higher levels of corruption and shadow economy are thought to correlate with low levels of economic and sustainable development (Hoinaru *et al.* 2020). There is a ‘broad consensus’ to demonstrate the link between corruption and poverty (U4, 2020).

To say that corruption is “poverty-driven” is only partially correct. Other crucial indices such as: alienation, perceived marginalisation, and powerlessness give us a wider and more penetrative perspective. In an Asia-Pacific study, far from being driven by poverty, corruption is often at its worst in justice systems (UNDP, 2008). in as much as illicit flow of money is often more rampant at the lower-level with a high degree of pervasiveness and tolerance than we are led to believe hitherto. Illicit financial flow is not only natural in some communities, but also actively nurtured.

## **NURTURING ILLICIT FINANCIAL FLOW**

This part of the chapter is modelled on Steven Lukes’s (1974) *Power: ‘A Radical View’*. It was a seminal work re-issued in 2005. It was originally a contribution to the debate about the dominance of a ruling elite in American politics, challenging the orthodoxy of a plural and egalitarian political system long held up as the shining example of progress and a beacon to the rest of the world (Lukes, 1974). Lukes attempted to provide answers to the burning questions of the day: How do the powerful secure the compliance of those they dominate and, more specifically, how do they secure their willing compliance?

These questions are compared in this analysis, to another burning issue of the day, the continued menace of financial crime. Conventional wisdom has a one-dimensional view of financial crime. It is seen as a supply-side problem emanating from officials in high places. In other words, it is a crime perpetrated in the corridors of power in urban metropolitan cities. The alternative view of financial crime here is that it is embedded in the fabric of society. More significantly, that it emanates from the bottom up far more frequently than it does from high places. Financial crime is prevalent in developing economies not necessarily because of ‘weak institutions’, but principally because there is a higher tolerance level for it owing to the value it generates. This analysis maps out a way of thinking about financial crime conceptually and how to study it empirically, unravelling how the powerless secure the willing compliance of the powerful in the commission and execution of financial crime (Shah, 2021).

## ***Powerlessness as the Basis for Financial Crimes***

To achieve this objective, there is a need to think about financial crimes more broadly and to pay attention to those aspects of illicit financial flows that are least accessible to observation; that are outside the formal sector; outside the metropolitan cities and large corporations, and outside large government bureaucracies. Financial crime is seen as social levy and the imposition of cultural dues and those subject to it acquire beliefs that result in a self-imposed obligation and adaption to informal structures of influence by non-coercive forms. Illicit financial flows are one of those concepts which is invariably value dependent. Both its definition and any given use of it, once defined are inextricably tied to a given set of value assumptions which pre-determine the range of its empirical applications.

Advanced show of gratitude for an official help about to be received, perfectly normal in one cultural setting, becomes “bribery of an official” under a universal application of financial crime legislation. A distortion of, and diversion of public investment funds for clannish interest is hailed as “son-of-the-soil” endeavour in one cultural setting, and a grand larceny in the context of universal assumptions of financial crime. Powerlessness is conceived here as an absence of capacity rather than the absence of influence. A person can lack capacity yet be able to exert influence. This departure from convention is empirically useful in the sense that it allows the framing of hypothesis that are in principle verifiable or falsifiable.

To corruptly divert common funds to support clannish demands is no longer seen as a crime, but as ‘just reward’. Financial crime is tolerated, indeed enhanced by the powerless if the perpetrator is at once accepted as a ‘local champion’ in a Robin Hood type of way. Criminal prosecution of financial crime is perceived as less as potent, as it is widely seen as point scoring, and score-settling by the metropolitan elite. Stealing from the commonwealth is absorbed by the powerless because of ‘cake sharing’ however meagre the crumbs. It is the capacity to channel demands without entering into confrontation with state agents and political elite by shaping perceptions, cognitions and preferences of the powerless in such a way as to ensure the acceptance of certain obligations towards them in the existing order.

There are many ways in which financial malfeasants are kept out of the criminal jurisdiction whether through individuals’ decisions or through the operation of social forces and institutional practices. Luke’s (1974) power analysis also stresses the importance of the concept of latent conflict. For this discussion, a latent conflict consists in a contradiction between the interest of the powerful and the real financial interests of the powerless which are excluded. The conflict is latent because those subject to power do not express or even remain unaware of their interest. Latent problem poses many problems to the scholar of sociology or political science, however, because the line between social determinism and the lack of awareness about a group’s interests is very thin (Lorenzi, 2006). As far as Luke is concerned though, the interests are empirically ascertainable if discovered and applied case by case.

There are references or ways to measure something. Power of the ballot could be ascertained by reference to the weight of the count. Choice of school could be verified by reference to the number of schools on offer, choice of healthcare could be verified by reference to the quality of hospitals available, choice of career path could be verified by reference to how many from poor background secured jobs without family contacts, self-sufficiency could be measured by reference to employment opportunities on offer across the board, choice of medication could be measured by reference to its affordability, protection from crime could be assessed by reference to the number of active police officer in the neighbourhood, choice of television channels could be measure by counting the number of household with access to cable television, etc. By so doing, purchasing power of the powerless could be verified by reference to their income.

A one-dimensional view of financial crime is the one which treats such crime as the pastime of the urban metropolitan elites in developing countries. Laws, regulations, and international conventions are



thus fashioned around those thoughts falling within the rubrics of Politically Exposed Persons (PEPs). Financial crime is not only reflected in direct bribery and grand larceny, however, individual or groups in communities can inverse the course of the flow of public funds to relatively non-controversial projects by influencing community values and political procedures and rituals. Informal influence from the bottom can also be in the willingness to create or reinforce barriers to the public airing of illicit financial flows. An empirical analysis would thus involve the examination of decisions on both criminal and non-criminal litigations. A non-criminal litigation is one designed to avoid the emergence of values and interests contrary to those of the community. Non-criminal litigation is a means by which demand for change in the allocation of benefits and privileges in the community can be suffocated, kept covert, or prevented from gaining access to the relevant criminal jurisdictions. It is often the outcome of socially structured and culturally patterned collective behaviour.

Informal influence by the powerless can also be exercised by preventing public outcries, by shaping perceptions, cognitions, and preferences in such a way as to secure the acceptance of the status quo since no alternative appears to exist, or because it is seen as natural and unchangeable, or indeed beneficial. This is where the informal structures of powers (via local chiefs, kings, religious leaders, family kinship etc.) are at the most relevant. This is how potential issues of illicit financial flows are kept out of public scrutiny through individual actions or through the operation of social forces and institutional practices. How these findings should be appraised?

## **REFLECTIONS ON FUTURE STRATEGIES**

Corruption often conjures up images of people getting rich, and others impoverished when in fact corruption's connections to poverty are far more numerous and pervasive (Johnston, 2009). Powerlessness permeates corruption, while corruption deepens illicit financial flow. Powerlessness both thrives upon weaknesses in key financial and political institutions, and it is also self-serving, advancing economic interests of the neglected and people in the shadow economy. As it happens, low level officials themselves may have trouble earning an honest living even with the best will in the world. And, in poor societies, they must also provide a stream of payments that go back up the chain of command. In such settings, bribery, extortion, and theft become matters of survival (Johnston, 2009).

Looking at things from the perspective of the poor, the World Development Report of 2000/2001 brought together the experiences of over 60,000 poor women and men from 60 countries around the world (Narayan, 2000). Using open-ended qualitative and participatory research techniques, the voices of the poor study aimed to understand poverty from the perspective of poor people and to illuminate the human experience behind the poverty statistics. The study finds that poverty is multidimensional with important non-economic dimensions. Across the board and all parameters, it also finds that poor people's lives are characterised by powerlessness and voicelessness, which limit their choices and define the quality of their interactions with employers, markets, the state and even non-governmental organisations (Narayan, 2000). When people feel powerful, they are more likely to express opposition to the status quo, but feelings of powerlessness can lead those same individuals to support systems that disadvantage them (Van der Toorn *et al.*, 2015). This is all too often the case in developing countries where there is a deep sense of alienation from the Leviathan state. In that situation powerlessness becomes 'corrosive, hemmed in by rules and treated as unimportant, people get even by exerting themselves on their im-

## ***Powerlessness as the Basis for Financial Crimes***

mediate environment, imposing cost on legitimate business and circumscribing government ability to execute public projects (Kanter, 2010).

The neo-liberal economic agenda of the 1980s foisted on countries across the developing world with its pro-market worldview, promoted economic growth, but accentuated the alienation of the people from the consumerism it engendered. The corruption-poor-people-poverty narrative appeals to the elite in those countries because they dominate the economic space and shape public opinion (Bello, 2010). Structural causes of poverty, powerlessness, and illicit financial flow are intertwined. It captures the contours of financial crime and its beneficial impact on the lower rungs of the economic ladder.

This is not a justification for corruption, but a succinct explanation. Where poverty is the disease, corruption becomes the cure (Careerride, 2015). Self-Sustainability is also an important issue (Rafay, Ajmal & Khalid, 2016). Corruption cannot, of course, ‘cure’ poverty outside economic empowerment and financial self-sustainability. What it does, however, is provide a breathing space for the powerless to maintain viability. Over time though, a permissive culture of tolerance to financial crime develops and blossoms at the lower level of society, which reinforces bureaucratic corruption and illicit flow of finance from the top. The symbiotic relationship between the two in developing countries is undeniable. It is what gives financial crime its complexity, at the same time its peculiarity in those societies.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in his personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## **REFERENCES**

U4. (2020). *Review of the literature on the link between corruption, poverty and conflict, and evidence on the impact of corruption on donor interventions*. Oslo: U4 Anti-Corruption Resource Centre. Retrieved from <https://www.u4.no/publications>

Alam, M. D., Tabash, M. I., Hassan, M. F., Hossain, N., & Javed, A. (2021). *Shariah Governance Systems of Islamic Banks in Bangladesh: A Comparison with Global Governance Practices*. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Amundsen, I. (1999). *Political Corruption: An Introduction to the Issues* (WP 1999: 7). Bergen: Chr. Michelsen Institute. Retrieved from <https://open.cmi.no/cmi-xmlui/handle/11250/2435773>

Atuobi, S. M. (2007). *Corruption and State Instability in West Africa: An Examination of Policy Options* (KAIPTC Occasional Paper, December 2007). Accra: Kofi Annan International Peacekeeping Training Centre. Retrieved from <https://reliefweb.int/report/world/corruption-and-state-instability-west-africa-examination-policy-options>

Bello, W. (2010). *Is Corruption the Cause? The Poverty Trap*. TNI.org. Retrieved from <https://www.tni.org/es/node/10907>

Careerride. (2015). *Poverty causes corruption*. Retrieved from <https://www.careerride.com/view/poverty-causes-corruption-26204.aspx>

Chetwynd, E., Chetwynd, F., & Spector, B. (2003). Corruption and poverty: A review of recent literature. *Management Systems International*, 600, 5–16.

DFID. (2015). *Why Corruption Matters: Understanding Causes Effects and How to Address Them* (DFID Evidence Paper on Corruption). London: Department for International Development. Retrieved from <https://www.gov.uk/government/publications/why-corruption-matters-understanding-causes-effects-and-how-to-address-them>

Dupuy, K., & Neset, S. (2018). *The cognitive psychology of corruption. Micro-level explanations for unethical behavior* (U4 Issue2018:2). Bergen: Chr. Michelsen Institute. Retrieved from <https://www.cmi.no/publications/6576-the-cognitive-psychology-of-corruption>

Enste, D., & Heldman, C. (2017). *Causes and Consequences of Corruption: An Overview of Empirical Results* (IW-Report No. 2/2017). Cologne: Institut der deutschen Wirtschaft. Retrieved from <https://www.econstor.eu/handle/10419/157204>

Hoinaru, R., Buda, D., Borlea, S. N., Văidean, V. L., & Achim, M. V. (2020). The Impact of Corruption and Shadow Economy on the Economic and Sustainable Development. Do They “Sand the Wheels” or “Grease the Wheels”? *Sustainability*, 12(2), 481. doi:10.3390u12020481

Ibrahim, A. R. (2021). Religio-Spiritual Implications of Corruption and Money Laundering: The Case of Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Jain, A. K. (2001). *The Political Economy of Corruption*. Routledge. doi:10.4324/9780203468388

Johnston, M. (2009). *Poverty and Corruption*. Forbes. Retrieved from [https://www.forbes.com/2009/01/22/corruption-poverty-development-biz-corruption09-cx\\_mj\\_0122johnston.html?sh=3f24c2111a56](https://www.forbes.com/2009/01/22/corruption-poverty-development-biz-corruption09-cx_mj_0122johnston.html?sh=3f24c2111a56)

Justesen, M. K., & Bjørnskov, C. (2014). Exploiting the poor: Bureaucratic corruption and poverty in Africa. *World Development*, 58, 106–115. doi:10.1016/j.worlddev.2014.01.002

## **Powerlessness as the Basis for Financial Crimes**

- Kanter, R. M. (2010). Powerlessness Corrupts. *Harvard Business Review*, 2010(July-August). <https://www.hbs.edu/faculty/Pages/item.aspx?num=38070> PMID:20607962
- Lawder, D. (2016). *IMF: Global corruption costs trillions in bribes, lost growth*. Reuters.com. Retrieved from <https://www.reuters.com/article/us-imf-corruption-idUSKCN0Y22B7>
- Løvseth, T. (2001). *Corruption and Alienation*. Paper presented at ECPR Joint Sessions April 2001, Grenoble, Panel 16: “Corruption, Scandal and the Contestation of Governance in Europe”. Retrieved from <https://ecpr.eu/Events/Event/PaperDetails/5494>
- Lukes, S. (1974). *Power: A Radical View*. Palgrave Macmillan. doi:10.1007/978-1-349-02248-9
- Mundial, B. (1997). *Helping countries combat corruption: the role of the World Bank. Poverty Reduction and Economic Management*. The World Bank Group.
- Narayan, D. (2000). Poverty is powerlessness and voicelessness. *Finance & Development*, 37(4), 18.
- OECD. (2014). *Illicit Financial Flows from Developing Countries: Measuring OECD Responses*. Paris: Organisation for Economic Cooperation and Development. Retrieved from <https://www.oecd.org/corruption-integrity/>
- OECD. (2020). *Anti-Corruption*. Paris: Organisation for Economic Cooperation and Development. Retrieved from <https://www.oecd.org/g20/topics/anti-corruption>
- Rafay, A., Ajmal, M., & Khalid, Z. (2016). Self-Sustainability of SME Banks - A Myth or Reality? Evidence from Selected Developing Economies across Asia. *SMEDA Research Journal*, 3(1), 64–74.
- Rafay, A., & Ajmal, M. M. (2014). Earnings Management through Deferred Taxes Recognized under IAS 12: Evidence from Pakistan. *Lahore Journal of Business*, 3(1), 1–19. doi:10.35536/ljb.2014.v3.i1.a1
- Rose-Ackerman, S., & Palifka, B. J. (2016). *Corruption and Government: Causes, Consequences, and Reform*. Cambridge University Press. doi:10.1017/CBO9781139962933
- Shah, S. (2021). Compliance Monitoring and Testing Seismometer to Detect Compliquake. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Tanzi, V. (1998). *Corruption Around the World: Causes, Consequences, Scope and Cures* (IMF WP/98/63). Washington, DC: International Monetary Fund.
- UN. (2018). *Global Cost of Corruption at Least 5 Per Cent of World Gross Domestic Product* (8346<sup>th</sup> meeting of Security Council). Retrieved from <https://www.un.org/press/en/2018/sc13493.doc.htm>
- UNDP. (2008). *Tackling Corruption, Transforming Lives – Accelerating Human Development in Asia and the Pacific* (Human Development Report, UNDP). Retrieved from <http://hdr.undp.org/en/content/tackling-corruption-transforming-lives>
- Van der Toorn, J., Feinberg, M., Jost, J. T., Kay, A. C., Tyler, T. R., Willer, R., & Wilmuth, C. (2015). A sense of powerlessness fosters system justification: Implications for the legitimization of authority, hierarchy, and government. *Political Psychology*, 36(1), 93–110. doi:10.1111/pops.12183

## ENDNOTES

- <sup>1</sup> Yoruba is one of Nigeria's most significant ethnic group, occupying the Lagos metropolis and South Western part of the country, with a growing population of over thirty million whose descendants spread across the neighbouring West Africa and Brazil in South America.
- <sup>2</sup> In the author's recollection, the first reference to the phrase 'powerlessness corrupts' was made in the early 1980s on a British television programme by the late Professor Ali Mazrui about the Israel-Palestine conflict. No doubt, Lord Acton's aphorism has stood the test of time. Nonetheless, if the Noble man were to be woken up for his reaction to the inversion of his centuries-old assertion today, he would be bemused, but would most certainly agree with the underlying premise that financial crime in whatever guise is a common mischief for which there is still no common remedy.

# Chapter 4

## The Power of Currency: Financial Coercion in the 21st Century

**Robert Beeres**

*Netherlands Defence Academy, The Netherlands*

**Jan van Lieshout**

 <https://orcid.org/0000-0002-3888-0168>

*Netherlands Defence Academy, The Netherlands*

**Myriame Bollen**

*Netherlands Defence Academy, The Netherlands*

### ABSTRACT

*This chapter explores the coercive power of currencies. The authors add to the existing literature on two strands. First, within the scope of the chapter, money encompasses all aspects of currency and financial relations – the processes and institutions of financial intermediation (mobilization of savings and allocation of credit) as well as the creation and management of money itself. The authors discuss as to what extent money can be deployed to prevent wars and conflicts, or, in other words, can money serve as a weapon of coercion? The chapter analyzes four scenarios of potential (fictional) financial wars between states. The authors find that, indeed, money yields coercive power. Based on proxies for the size of the economies of a deterring state and its adversary, the chapter shows how the potential impact of financial coercion may be estimated.*

### INTRODUCTION

On September 24, 2001, the President George W. Bush addressed the American nation.

*“Good Morning. At 12:01 this morning, a major thrust of our war on terrorism began with the stroke of a pen. Today, we have launched a strike on the financial foundation of the global terror network [...] I’ve signed an executive order that immediately freezes United States financial assets of and prohibits*

DOI: 10.4018/978-1-7998-5567-5.ch004

*United States transactions with 27 different entities [...] We have developed the international financial equivalent of law enforcements “Most Wanted” list. And it puts the financial world on notice. If you do business with terrorists, if you support or sponsor them, you will not do business with the United States of America” (Bush, 2001).*

The abovementioned “stroke of a pen” refers to the President of the United States (U.S.) signing Executive Order 13224, which “prohibited transactions with terrorists”, thus, enabling the U.S. government “to designate and block the assets of those involved with terrorist organizations, both at home and abroad, by compelling foreign banks to participate” (Gilbert, 2019). Upon issuing Executive Order 13224, the Bush administration started to force behavioral change throughout the financial world. From then on, money was to be used as a weapon of coercion. Not so much as by targeting the terrorist adversaries themselves directly, but, instead, aiming at those providing them with financial funds.

Deterring those who finance terror has been the main rationale underpinning national and international counter-terrorism policies. Following the attacks on September 11, 2001, the scope of measures to monitor and evaluate achievements in the field of counter-terrorism finance has increased drastically, including both preventive and repressive measures (Beeres *et al.*, 2017; Brzoska, 2016). Preventive measures aim to establish “a regulatory regime for financial institutions, intended to reduce the scope for using the financial systems to collect and transfer funds for terrorist purposes” (Raphaeli, 2003). Internationally, the Financial Action Task Force (FATF)’s recommendations are regarded as the most important anti-terrorist financing standards (Bogers and Beeres, 2011; Joosten *et al.* 2019). As per the repressive measures, they “originate from agreements between countries and aim to alter national laws to such extents, that certain acts become illegal. Examples are establishing blacklists of suspicious persons or organizations, freezing bank accounts, and excluding certain individuals or organizations from insurances and financial services” (Beeres and Bollen, 2011; Beeres *et al.* 2017). In order to properly evaluate counter-terrorism policies and measures, Brzoska (2016) distinguishes between output, outcome, and impact. The output refers to legal frameworks for shaping interventions in the field of counter-terrorism finance. The outcome addresses the question of whether the framework is implemented as intended, while the impact focuses on questions whether the financiers, in practice, have been deterred. Although the output and the outcome are usually seen as important preconditions for the impact, actually, they do not suffice to establish any impact. To the best of the authors’ knowledge, research findings on the impact of counter-terrorism policies are still lacking. Till now, and regardless of the FATF’s regulative, monitoring, and auditing efforts, it remains unclear whether financiers of terror are indeed being deterred. Thus far, the extent to which the implemented measures are functioning as weapons against terrorism remains unclear.

Despite this lack of clarity in literature, it is commonly acknowledged that money can serve as a weapon (Bracken, 2007; Fenaroli, 2016; Katz, 2017; Lin, 2015; Rhodes, 2012; Van Duren, 2010; Rab, 2020). In this respect, the common used terminology refers to *financial warfare* (Bracken, 2007), *currency warfare* (Crespo, 2018; Pringle, 2019; Rickards, 2012), or, regarding the War on Terror, *(counter) threat (or terrorist) finance* (Keatinge and Danner, 2018; Keene, 2014). Money is vital to making war (Mouré, 2020). However, the questions related to what extent money can be useful to prevent wars and conflicts, or, to put it more aptly, how it can be successfully deployed as a coercive weapon, remains unexplored. Whether money can be considered as a useful instrument for coercion is researched in the field of international political economy (Andrews, 2006; Cohen, 2018; Kirschner, 1995; 2006; Lawton *et al.*, 2018; Mathieu, 2020). The relation between power and currency, to date, still constitutes a very

small niche (Cohen, 2018; Kirschner, 1995). This chapter aims to shed light on the question to what extent money can act as an instrument of coercion in the 21<sup>st</sup>-century. From the analysis, it will appear that, if used in a credible way, money indeed provides for an excellent instrument of coercion.

The authors add to the existing literature on two strands. First, within the scope of the chapter, money encompasses “all aspects of currency and financial relations – the processes and institutions of financial intermediation (mobilization of savings and allocation of credit) as well as the creation and management of money itself” (Cohen, 2000). Thus, money refers not only to coins and notes, which, as a physical flow, in Western society, has been replaced almost completely by virtual and digital flows, but in using the term money, the authors refer to all financial instruments, such as, debts and equities, stocks, and bond deposits, options, as well as making money (Rafay & Farid, 2017; Gilbert, 2019; Taskinsoy, 2020). Second, the chapter’s analysis is geared towards the state level and the relations among states and state-sponsored organizations, e.g., the International Monetary Fund (IMF) and the World Trade Organization (WTO), including the (global) financial markets that these institutions use for trade purposes. Admittedly, due to globalization and technological developments, the 21<sup>st</sup>-century security environment has gained complexity. In this respect, Keene (2014) states that “historically, adversaries were well-defined, allowing a relatively clear course of action”. The author adds that “this is no longer the case, as non-state actors forming a global network of terrorist organizations, associated criminal groups, corrupt governments, and indifferent or uninformed individuals or corporations, increasingly take center stage”. However, to deploy currency as an instrument of deterrence, in a credible way, one has to be able to create money, which, at least until nowadays, remains a state’s prerogative (Kelton, 2020; Ahmad *et al.*, 2020). As long as states constitute the basic units of formal currency governance, Cohen (2000) argues that “inter-state relations will continue to be part of the story and well worth exploring on their own”.

The next section presents a 20<sup>th</sup>-century case study to serve as an example of financial coercion. Next, section 3 elaborates on the research design, and in section 4, four scenarios are put forward and analyzed. The final section contains a conclusion and discussion.

### **SETTING THE SCENE: CURRENCY AS AN INSTRUMENT OF DETERRENCE, A 20<sup>th</sup> CENTURY EXAMPLE**

This section presents a case study on international monetary power. This particular study is well-known and often used to introduce the concept of financial deterrence by means of currency manipulation in the field of international political economy (Andrews, 2006; Bracken, 2007; Fenaroli, 2016; Kirschner, 1995).

On October 31, 1956, the British and French military invaded Egypt determined to regain the Suez Canal, nationalized three months previously by the Egyptian President Gamal Abdel Nasser. The U.S. disagreed with this course of action and the President Dwight D. Eisenhower, abstaining from direct military force, successfully coerced the United Kingdom (U.K.) and France out of the Suez Canal by means of financial warfare. Eisenhower ordered the Treasury Department to dump British pound sterling into the international market to devalue it. On November 5<sup>th</sup>, about a week after the invasion, the pound sterling was under sustained pressure in the international markets. By November 6<sup>th</sup>, the U.K. officials requested support from their U.S. counterparts. They were informed no help would be forthcoming unless the U.K. complied with the U.S. sponsored United Nations resolution calling for immediate ceasefire and withdrawal from Egypt. Moreover, if London would withdraw its forces, the U.S. would not only cooperate with the U.K. at the IMF, but also, would provide additional resources in the form of an im-



mediate export-import credit. By that time, the depressed value of the pound sterling was already causing a shortage of reserves needed for imports' payments and, if this financial situation would continue, inflation would soar. Threats regarding inflation and the inability to pay for their imports sufficed to convince the U.K. to withdraw their troops from the Suez Canal. The French followed suit.

The above is an example of financial coercion, in accordance with De Wijk (2014)'s definition underlining that "the deliberate and targeted use -or threat thereof- of power instruments to manipulate and influence the politico-strategic choices of an actor, or player, defined as an entity that plays an identifiable role in international relations". The case study narrates how the U.S. President Dwight D. Eisenhower threatens to diminish and even destroy the pound sterling's value to force the U.K. to cease its behavior (i.e., the military invasion in Egypt to nationalize the Suez Canal). The U.K. then outweighs the costs to be incurred (i.e., devaluation of its currency and inability to pay for imports) against expected benefits (i.e., preservation of the Suez Canal) and decides to act accordingly.

De Wijk (2014) breaks down coercion into deterrence and compellence. According to De Wijk, deterrence involves attempts to prevent something from happening, whereas compellence refers to the use of force to revise an action that has occurred, meaning that, as the U.K. already had invaded Egypt, strictly speaking, the case study above is on compellence. However, the authors agree with Frey (2018) that deterrence will only remain credible when used occasionally, and, as such, deterrence may transgress into compellence.

The primary reason for the successful financial coercion was the economic dependence of the U.K. on the U.S. Secondly, the country was in a fragile economic position to begin with. Thirdly, by controlling the British's access to the lending capabilities of the IMF and the World Bank, the U.S. was able to exercise full control over the U.K. government, which could not avail of alternate sources of funding. A final reason worth mentioning was that the "insistence of British government on making the continued strength of the pound and the maintenance of the sterling area chief national priorities, presented the American government with the perfect weapon to use against Prime Minister Anthony Eden" (Kunz, 1991).

## RESEARCH DESIGN

To date, well into the 21<sup>st</sup> century, one common supranational currency still does not exist. If so, money would no longer be of use as an instrument of financial coercion between states. However, it is not expected that, in the foreseeable future, whether voluntarily or not, a common global currency will be achieved. Therefore, monetary rivalry and the possibility to deploy money as an instrument of deterrence will remain viable. Following Cohen (2018), the authors of this chapter agree that as yet, there is regrettably a little systematic theory to help understand monetary rivalry in the 21<sup>st</sup> century.

Kirshner (2006) argues that all research on the manipulation of currency values and monetary arrangements to advance political goals appears to stem from the 20<sup>th</sup> century, which he considers to be a knowledge gap. The author views both globalization and unipolarity as two major distinctions between the 20<sup>th</sup> and 21<sup>st</sup> centuries and asks whether financial globalization (i.e., the presence of very large integrated and influential currency markets) has changed the capabilities of states to practice financial coercion. Analyzing the case study *Plots against the Iraqi Dinar*, Kirshner (2006) concludes that "as long as there are states and money, states will attempt to manipulate monetary relations to advance their political objectives", and then he proceeds to point out two changes due to globalization. First, financial markets are more crisis-prone, and second, failing to provide help to a country in distress or extorting

concessions in exchange for help will proliferate in such contexts. The U.S. in particular, according to Kirshner (2006), “is well placed to use its resources or to wield its enormous influence in international institutions either to help out – or fail to help out – those in distress”.

As empirical data are not yet available to underpin this research, and, as the chapter aims for insights on the question to what extent money can act as an instrument of coercion in the 21<sup>st</sup>-century, the authors have, inspired by Rickards’ (2012) *Currency Wars*, decided on scenario analysis as their research method (Cairns and Wright, 2018). Indeed, a scenario analysis can raise awareness of possible or probable future developments (Warren, 2012). As a method, it enables an exploration of what might happen, based on creative thinking and a consideration of various possibilities in a complex and ambiguous world, even when fictional.

The next section introduces four fictional scenarios, each encompassing a conflict between two states, in which one state (the adversary) threatens another state (the actor) with an intended highly problematic course of action. Next, the actor attempts to financially coerce the adversary. Third, the authors proceed to offer, for each scenario, potential outcomes of the attempted coercion, thereby exploring how such outcomes may put an end to the conflict. Last, it is assessed whether and to what extent financial coercion can contribute to preserving peaceful stability.

*Table 1. Financial coercion, four scenarios*

Actor/Adversary	Large		Small	
<b>Large</b>	China versus U.S.		China versus Netherlands	
AREA	9,388.2	9,147.4	9,388.2	33.7
POP	1,392.7	327.2	1,392.7	17.2
GDP	13,608.2	20,544.3	13,608.2	913.7
<b>Small</b>	Ireland versus E.U.		Jordan versus Syria	
AREA	68.9	4,238.7	88.8	183.6
POP	4.8	513.2	10.0	16.9
GDP	382.5	18,768.1	42.2	40.4

**Note:** All figures are from 2018, except the GDP of Syria (2007); AREA: Land area (square km<sup>3</sup>); POP: population (millions); GDP: Gross Domestic Product (billions current US\$) (Source: Worldbank 2020a; b; c)

The fictional scenarios vary regarding the relative size of a state (large or small) in relation to other states (see Table 1). A combination of wealth, population, and area serves as a proxy for size (Beeres and Bollen, 2015; Kollias, 2008; Sandler and Forbes 1980). Moreover, the authors have selected more or less plausible backgrounds for fictional conflicts. The first scenario, against the background of the recent *U.S.-China Trade War*, 2018-2020 elaborated on a fictional conflict between China (large) and the U.S. (large). In the second scenario, against the background of the *Affair of the Submarine*, 1980-1984, the authors have decided on a fictional conflict between China (large) and the Netherlands (small). The third scenario, against the background of the *European Debt crisis*, 2010-2014 elaborates on a fictional conflict between Ireland (small) versus the European Union - EU (large). Finally, in the fourth scenario, the fictional conflict (situated in contemporary times) takes place between Jordan (small) versus Syria (small). Last, for the sake of readability, the authors have decided to present their scenarios as four nar-

ratives (Buchanan and Badham, 2020). In the next section, these four narratives are presented, offering potential outcomes of the what-if analyses.

## **NARRATIVES AND OUTCOMES**

### **Scenario 1: Deterrence Doomsday**

The President Donald J. Trump is fed up. As opposed to what everybody is telling him, and, despite the ongoing Chinese currency account surplus, the Yuan's exchange rate remains low, defying thereby all economic laws. In the case where a country's exports exceed its imports, the currency's value is expected to increase, whilst the exchange rates should drop. Reversely, it should lead to a decrease in the currency's value, whereas the exchange rate would increase. Therefore, the country with the trade surplus (i.e., China), is supposed to have become wealthier and its industries less competitive, while the country suffering from a trade deficit, the U.S., is expected to have become poorer, whereas its industries supposedly would be more competitive.

As the Yuan's exchange rates keep falling, Trump twitters, "Not happening, can't trust those fancy economists". Neither is the U.S. President enamored by the Chinese tit-for-tat strategy. Whenever he increases the import tariffs on Chinese goods, the Chinese President Xi Jinping acts likewise on behalf of American goods. "Unfair and not going anywhere", the President Trump twitters furiously. "But America will win this trade war, we always do".

To this effect, the President Trump's newest plan, *The Chinese back to China* involves a law enabling the deportation of all Chinese people in the U.S. to China. This plan is launched on Saturday morning, January 25, 2020.

Upon receiving this news, the President Xi Jinping telephones President Trump to inform him this is no way to behave to the honorable and industrious Chinese people in the U.S. nor to the People's Republic of China. The Chinese President continues his call by threatening to destroy the U.S. economy if this plan is not revoked immediately. "How?", the President Trump asks. "Dumping dollars", the President Xi Jinping explains, as succinctly. This threat, however, does not appear to impress the U.S. President. "Incredible. In the first place, you own a lot yourself. Where do you suppose your trade surplus stems from? Besides, as the U.S. dollar is the reserve currency of almost every other nation, you will take down everyone with you. You will not dump dollars". Triumphantly, the President Trump disconnects the President Xi.

Xi proceeds to dump dollars. By Monday morning, January 27<sup>th</sup>, 2020, at the opening of the stock exchanges all over Asia, the dollar's exchange rate has already risen significantly, compared to the last official ratings. In Singapore, the dollars are dumped into the market, as in Tokyo and Hong Kong. The dollar's value keeps dropping, whereas its exchange rate keeps rising. Across Asia, the stock markets are in an uproar, and panic spreads to Europe. Meanwhile, the U.S. dollar has gone into free fall, and, as by now, it has become impossible to decide on trustworthy buying and selling rates, the U.S. currency cannot be traded anymore in money and exchange offices.

Next, on Monday afternoon, the U.S. financial markets open up and, as elsewhere in the world, the dollar is at a dramatic low. The President Trump requests the EU leaders and banks for their support, "Buy dollars". Then, the President Xi twitters, "If you do business with the U.S., you will not do business with the People's Republic of China". The EU leaders renounce tradability between the dollar and euro,

## ***The Power of Currency***

and, outraged by such betrayal, the President Trump renounces all trade relations between the U.S. and the EU. The Europe's political leaders blame the American President for the ensuing financial crisis, in which Western welfare society, as known until then, is severely disrupted. Within the course of one day, the world has become a much poorer place.

In this first scenario, the adversary does not take the actor's threat seriously, which is not remarkable in itself. After all, economically speaking, why would any head of state want to render both themselves and the rest of mankind that much poorer? In this narrative, national pride and honor provide the main drivers. Although this scenario, based on currency manipulation, may seem unlikely, in practice, the method described is not impossible to apply. Foremost, the scenario intends to show that, if and when the dollar is severely attacked in today's global economy, due to the fact this coin also doubles as the prime international reserve currency, mutually assured destruction may -perhaps rather too easily- turn into global assured destruction.

### **Scenario 2: Don't You Dare Dream of a Yellow Submarine**

Finally, it has been decided. It is all over the news which shipyard has been contracted to build the Royal Navy's new submarines to replace four Walruses. According to the Dutch Prime Minister Mark Rutte, "national and security interests as well as the interests of Dutch industries have been balanced and, moreover, construction costs can be controlled at all times". When interviewed, Rutte, in a festive mood, observes that "as to the costs, also, everything seems to turn out for the best". Only recently, the Taiwanese government has ordered ten submarines to be built by the same Dutch shipyard. "Taiwan prefers exactly the same submarines, except they want theirs to be painted yellow. That shouldn't be an issue". The Prime Minister continues exuberantly, "this way, we will spread the indirect costs over a bigger number of submarines, which will result in lower costs for each. Of course, the Dutch government has immediately consented with the Taiwanese order".

As soon as the President Xi Jinping is informed on the cause of Rutte's excellent mood, he telephones the Dutch Prime Minister. "Are you intending to deliver submarines to Taiwan once more?". "What do you mean by once more", Rutte asks. "Besides, we have carefully deliberated our decision. All is just fine, not to say, super!". The President Xi, reminiscing a recent experience of his with the U.S., smiles serenely into his phone, "If you continue your course of action, I will destroy the Euro". The Chinese President's telephone message goes viral on social media, and, after calls from all European leaders, the Dutch government decides, within one day, to revoke its decision on the lucrative Taiwanese order.

In this second scenario, the threat posed by the actor China is highly credible. Indeed, based on the first scenario, this actor already has proved that his threats do hold consequences and, therefore, is to be trusted. The method of monetary warfare used in this scenario is (predatory) currency manipulation.

### **Scenario 3: The Power of the Poor Leprechaun**

In a hurry, Michael D. Higgins, the President of Ireland, leaves the office of his Prime Minister Varadkar on his way to take the next flight to Frankfurt, Germany, to visit Mrs. Christine Lagarde and inform her that Ireland will quit paying back billions of Euros, received as loans.

Only one hour earlier, the Irish Prime Minister Varadkar updated Higgins on Ireland's financial and economic situation. From 2009, the Irish economy has been suffering due to the financial crisis, forcing the government to pump billions of Euros into national system banks to prevent those banks from fall-

ing. Fortunately, the Irish received 85 billion Euros in the form of a support package from the EU and the IMF. Now, the loans are being reimbursed, but, according to Varadkar, although the Irish economy is recovering step by step, with a small yearly increase in GDP, paying back the full 85 billion Euro will bring Ireland more financial harm than salvation.

“So, what’s next?”, the President asks. Varadkar, who has posed this exact same question to the Minister of Finance, suggests for Ireland to unilaterally step out of the program that was supposed to help them survive the financial crisis. “Since we are only a minor EU economy, we propose you go to Frankfurt and tell Mrs. Lagarde that we are about to stop our reimbursements”. Varadkar continues, “There is not much the European Central Bank (ECB), or the EU can do if we threaten to stop paying back. Ireland will go down if we are compelled to refund each and every Euro we have borrowed and that will lead to even bigger problems for the EU than if they are not being repaid. Our threat is supposed to result in a 100% quittance of debt. If Mrs. Lagarde decides we should repay, you may inform her that Ireland will have no option but to exit the EU”.

The President Higgins is shocked, not as much because he is to be the bringer of bad news, but because of the sheer power of the financial coercion that he has been asked to pass. Just imagine what Greece may do when Ireland will leave the EU because of its inability to reimburse!

On March 17<sup>th</sup>, 2019, after four hours of discussion with Mrs. Lagarde and her co-workers, the President Higgins leaves the ECB premises, on his way back to Dublin. Upon recovering from the initial shock, caused by the Irish message, potential options have been deliberated and it has been concluded that the EU and ECB will suspend all repayments until the national debt of Ireland has recovered at a lower level than 60% of its GDP.

In this third scenario, the Irish threat not to repay their debts or, else, to exit the EU can be regarded both as coercive as probable. After all, Ireland cannot avail of many alternatives, and the Irish economy indeed can be expected to suffer seriously if the government complies with the EU expectations. On the other hand, the Irish stance poses a serious problem for the EU and ECB too, since this threat leaves them empty-handed as far as coercive options go.

## **Scenario 4: Pay Me My Money Down**

From 2011, when the civil war started in Syria, many civilians have sought refuge in Jordan and the King Abdullah II had no other option than to welcome his suffering neighbors. The King realized also that sheltering over 1.5 million refugees (population growth of 15%) would have major effects on the society and local economy. Jordan had to accommodate and take care of the Syrian refugees, but this would come at a cost. Such costs were to be understood quite literally, including additional financial costs for housing, healthcare, and education. This bothered the King, as the Jordanian economy was vulnerable to begin with and such compounding expenses might be devastating. Accordingly, the King commissioned the Prime Minister Omar Razzaz to work out a detailed plan to cope with additional costs, aiming for Syria, the refugees’ birth land, to refund all extras. Razzaz, a Harvard-educated economist and former student in engineering, reverted back to the King Abdullah II with a cunning plan. “In practice, my strategy would be to threaten to attack Syria using so-called debt and equity engineering. We hold Syria accountable for the extra costs we have to make on account of vast numbers of Syrian refugees. We do not want to destroy Syria financially, because in that case, we will never be reimbursed, we just want to be compensated. So, we use this strategy to deter the Syrian government”, Razzaz advised. Briefly, a strategy of debt and equity engineering will affect total or partial Jordanian ownership of

## ***The Power of Currency***

Syrian enterprises and industries. Such ownership can be obtained in the forms: debt and/or equity. The Jordanian Prime Minister did not believe, it would be effective to merely ask the President Assad to pay the extra costs. Instead, the Jordanian government and their King decided to threaten to attack Syria by using monetary power. Based on various financial weapons they could avail of; this seemed the most effective and efficient approach. "Although we are not a rich country ourselves, we can use state funds to obtain ownership in Syrian enterprises that are financially better off. Jordanian companies, and specially assigned middlemen, will buy either shares or debts, and will become the owners of these enterprises. Subsequently, the earnings will flow our way, ending up making more money, while Syrian economy will lose income." The Jordanian Prime Minister continued his advice to his King, adding that threatening alone would probably convince the President Assad that his economic loss would be devastating, should he decide not to repay Jordan's costs related to Syrian refugees.

The King Abdullah II was utterly delighted and telephoned the President Assad immediately to inform him of his intended course of action. The Syrian President got back to him within days. Although deeply regretting this particular threat and Jordanian hostility towards his country, enterprises and civilians in general, Assad realized that the deterrence due to the Jordanian monetary coercion posed too big a risk. He proposed a reimbursement scheme if the King Abdullah II would give up his plans for hostile takeovers.

In this fourth scenario, the probability of Jordan to execute their deterrent plan is high, so Syria cannot neglect this threat. Syria will be less bad off when it pays for the accommodation of the civilians in Jordan. Losing income from local enterprises and industries will hurt the Syrian economy more. Therefore, Jordan wins a battle that will not have been fought. Moreover, Jordan will not suffer from negative economic effects of the support to Syrian refugees.

## **ANALYSIS**

All four scenarios show that money, and particularly, the battles money, allows to embark on, yields a fair extent of coercive power. Mainly, the four scenarios differ as to the extent of total damage they may cause. The first scenario of China against the U.S. will end in serious collateral damage, as the collapse of the dollar will hurt the entire world. In scenario 4, if the Jordanians would execute their threat, Syria will suffer seriously, whereas Jordan will suffer less, for a shorter period, after which, the Jordanian strategy will result in recovery. The degrees of damage following the monetary attacks presented in the second and third scenarios are in between the effects of the first and fourth scenario, therefore, it appears that size does matter. This finding stems from the interaction between the sizes of the economies per scenario: two major economies involved in a monetary war will cause the greatest damage, whereas a financial war between two small economies will primarily cause havoc within each involved state.

Table 2 summarizes the results of the four what-if analyses and, notably, it appears that the objective of the actors can be achieved in full, partially, or not at all. Based on these results, the authors hold that expected outcomes impact the success ratio. China demands to stop the eviction of their people from the U.S., but the outcome of global destruction, following their coercive threat to destroy the U.S. dollar is an outcome that will be too damaging for the Chinese themselves.

Each threat potentially hurts the adversary's economy, and each fictional scenario is possible in real-life; there is no distinction between the narratives presented. However, the narratives do differ from each other with regard to the probability of a specific scenario manifesting itself in reality, and these differences are based on insecure and uncertain factors. Since the state under attack cannot judge nor assess

*Table 2. Overview of scenarios, conflicts, methods, outcomes and preservation of peace*

Scenario	China (Actor) vs US (Adversary)	China (Actor) vs Netherlands (Adversary)	Ireland (Actor) vs EU (Adversary)	Jordan (Actor) vs Syria (Adversary)
Conflict in scenario	Eviction of Chinese people from US	Sale of submarines to Taiwan	Refusal to repay debt	Extra costs of Syrian refugees
Method of coercion	Currency manipulation	Currency manipulation	Currency manipulation	Equity & debt engineering
Outcome	Global destruction	No sale	Delay of execution	Repayment of extra costs
Contribution in preservation of peace	Absent	In full	Partially	In full
Probability	Low	Moderate	High	Very high

to what extent the aggressor will pursue his plans, the probability of execution of the threat depends on chance and risk. The adversary can only estimate the chance for the actor to continue, based on known financial strengths and risks, and based on the expected damages.

This method teaches us that the first scenario (China versus the U.S.) will be less probable than the fourth scenario (Jordan versus Syria). Based on the financial strength of China and the expected damage, this strategy will cause that the U.S. will take into account that China, also, faces severe risks, as the ensuing damage will be global. In the case of Jordan threatening Syria, the adversary will estimate the probability that Jordan executes its plan as high, since Jordan is capable of doing so while the risk for damage on the Jordanian side is low. Thus, the probability of scenario 4 is higher than of the first scenario.

In sum, threatening to deploy financial weapons, in a credible way, can be used to force hostile states to change their behavior and strive for peaceful stability.

## CONCLUSION

This chapter aims to clarify the extent to which currencies can be deployed for coercion. Based on four scenario analyses, the authors find that money is a potentially strong weapon. Based on proxies, used for the size of the economy of a deterring state and its adversary, the potential impact (and probability) of a coercive strategy can be estimated.

All scenario analyses are based on fictional narratives. The next step is to apply simulation techniques, based on scenarios such as presented in this chapter. Currently, simulation game programming offers possibilities to enact each scenario, based on various sets of potential actions of both the actor and adversary. The authors will follow this pathway to further explore and elaborate on this research programme.

## DISCLAIMER

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

- Ahmed, J., Collins, P., & Meera, A. K. M. (2020). Conditional Currency Convertibility Based on Primary Commodities: The Shari'ah-Compliant Grondona System. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 61–84). IGI Global. doi:10.4018/978-1-7998-0218-1.ch004
- Andrews, D. M. (2006). Monetary Power and Monetary Statecraft. In D. M. Andrews (Ed.), *International Monetary Power* (pp. 7–28). Cornell University Press.
- Andrews, D. M. (Ed.). (2006). *International monetary power*. Cornell University Press.
- Beeres, R., Bertrand, R., & Bollen, M. (2017). Profiling Terrorists—Using Statistics to Fight Terrorism. In P. A. Ducheine & F. P. Osinga (Eds.), *Netherlands Annual Review of Military Studies 2017: Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises* (pp. 221–235). TMC Asser Press. doi:10.1007/978-94-6265-189-0\_12
- Beeres, R., & Bollen, M. (2011). The global financial War on Terror: Analyses en cijfers. In F. P. Osinga, J. M. L. M. Soeters, & W. vanRossum (Eds.), *Nine eleven: Tien jaar later* (pp. 92–106). Boom.
- Beeres, R., & Bollen, M. (2015). Exciting Dilemma: A Defence Economics View on a US Exit from NATO. In J. Noll, D. van den Wollenberg, F. Osinga, G. Frerks, & I. van Kemenade (Eds.), *Netherlands Annual Review of Military Studies 2015: The Dilemma of Leaving: Political and Military Exit Strategies* (pp. 271–297). TMC Asser Press. doi:10.1007/978-94-6265-078-7\_11
- Bogers, M., & Beeres, R. (2011). Burden sharing in combating terrorist financing. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, 7(12), 2992–2998.
- Bracken, P. (2007). Financial warfare. *Orbis*, 51(4), 685–696. doi:10.1016/j.orbis.2007.08.010
- Brzoska, M. (2016). Consequences of assessments of effectiveness for counterterrorist financing policy. *Administration & Society*, 48(8), 911–930. doi:10.1177/0095399714532272
- Buchanan, D., & Badham, R. (2020). *Power, Politics, and Organizational Change*. SAGE.



- Bush, G. W. (2001, September 24). *President Freezes Terrorists' Assets*. The White House. Retrieved from <https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010924-4.html>
- Cairns, G., & Wright, G. (2018). Advanced methods in scenario development: Uncovering causality and using the Delphi method. In *Scenario thinking* (pp. 141–154). Springer. doi:10.1007/978-3-319-49067-0\_7
- Cohen, B. J. (2000). Money and power in world politics. In *Strange Power: Shaping the Parameters of International Relations and International Political Economy* (pp. 91-113). London: Routledge.
- Cohen, B. J. (2018). *Currency power: Understanding monetary rivalry*. Princeton University Press.
- Crespo, R. A. (2018). Currency warfare and cyber warfare: The emerging currency battlefield of the 21st century. *Comparative Strategy*, 37(3), 235–250. doi:10.1080/01495933.2018.1486090
- De Wijk, R. (2014). *The Art of Military Coercion: Why the West's Military Superiority Scarcely Matters*. Amsterdam University Press.
- Fenaroli, G. C. (2016). *Financial Warfare: Money as an Instrument of Conflict and Tension in the International Arena* (Senior Projects). Bard College. Retrieved from [https://digitalcommons.bard.edu/senproj\\_s2016/136/](https://digitalcommons.bard.edu/senproj_s2016/136/)
- Frey, B. S. (2018). Countering Terrorism: Deterrence vs More Effective Alternatives. *Open Economics*, 1(1), 30–35. doi:10.1515/openec-2017-0002
- Gilbert, E. (2019). Military geoeconomics: money, finance and war. In R. Woodward (Ed.), *A Research Agenda for Military Geographies* (pp. 100–114). Edward Edgar Publishing. doi:10.4337/9781786438874.00014
- Joosten, E., Bogers, M., Beeres, R., & Bertrand, R. (2019). Predictors for compliance with anti-terrorist financing standards. *Journal of Money Laundering Control*, 22(2), 257–269. doi:10.1108/JMLC-02-2018-0011
- Katz, D. J. (2017). Waging Financial Warfare: Why and How. *Parameters*, 47(2), 41–49.
- Keatinge, T., & Danner, K. (2018). Assessing Innovation in Terrorist Financing. *Studies in Conflict and Terrorism*, 1–18. doi:10.1080/1057610X.2018.1559516
- Keene, S. D. (2014). *Operationalizing Counter Threat Finance Strategies*. The Letort papers. Strategic Studies Institute. Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a612777.pdf>
- Kelton, S. (2020). *The deficit myth. Modern monetary theory and how to build a better economy*. John Murray.
- Kirschner, J. (1995). *Currency and coercion: the political economy of international monetary power*. Princeton University Press.
- Kirschner, J. (2006). Currency and coercion in the Twenty-First Century. In D. A. Andrews (Ed.), *International monetary power* (pp. 139–161). Cornell University Press.
- Kollias, C. (2008). A preliminary investigation of the burden sharing aspects of a European Union common defence policy. *Defence and Peace Economics*, 19(4), 253–263. doi:10.1080/10242690802164777
- Kunz, D. B. (1991). *The economic diplomacy of the Suez crisis*. University of North Carolina Press.

## ***The Power of Currency***

Lawton, T. C., Rosenau, J. N., & Verdun, A. C. (Eds.). (2018). *Strange Power: Shaping the Parameters of International Relations and International Political Economy*. Routledge.

Lin, T. C. W. (2015). Financial Weapons of War. *Minnesota Law Review*, 100, 1377–1440.

Mathieu, A. (2020). Power and Currency: Did the Euro Improve the French State's Monetary Power? *International Journal of Political Economy*, 49(1), 62–82. doi:10.1080/08911916.2019.1693163

Mouré, K. (2020). Money in wars. In S. Battilossi, Y. Cassis, & K. Yago (Eds.), *Handbook of the History of Money and Currency* (pp. 995–1020). Springer., doi:10.1007/978-981-13-0596-2\_39

Pringle, R. (2019). Money as a Tool of the State. In *The Power of Money* (pp. 151–156). Palgrave Macmillan. doi:10.1007/978-3-030-25894-8\_14

Rab, H. (2020). Money and Monetary Issues in Islamic Finance. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 38–60). IGI Global. doi:10.4018/978-1-7998-0218-1.ch003

Rafay, A., & Farid, S. (2017). Financial Integration in Money Markets: Evidence from SAARC Region. *DLSU Business and Economics Review*, 26(2), 87–114.

Raphaeli, N. (2003). Financing of terrorism: Sources, methods, and channels. *Terrorism and Political Violence*, 15(4), 59–82. doi:10.1080/09546550390449881

Rhodes, K. (2012). The counterfeiting weapons. *Region Focus*, 16(1), 34–37.

Rickards, J. (2012). *Currency Wars*. Penguin.

Sandler, T., & Forbes, J. F. (1980). Burden sharing, strategy, and the design of NATO. *Economic Inquiry*, 18(3), 425–444. doi:10.1111/j.1465-7295.1980.tb00588.x

TaskinsoyJ. (2020). From Primitive Barter to Inflationary Dollar: A Warless Economic Weapon of Mass Destruction. doi:10.2139/ssrn.3542145

Van Duren, E. C. G. J. (2010). Money is ammunition; don't put it in the wrong hands. A view on COIN contracting from Regional Command South. *Militaire Spectator*, 179(11), 564–578.

Warren, L. (2012). Scenario analysis for S&OP. *The Journal of Business Forecasting*, 31(1), 32–35.

Worldbank. (2020a). *GDP (current US\$)*. Retrieved from <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=chart>

Worldbank. (2020b). *Land area (sq. km)*. Retrieved from <https://data.worldbank.org/indicator/AG.LND.TOTL.K2?view=chart>

Worldbank. (2020c) *Population, total*. Retrieved from <https://data.worldbank.org/indicator/SP.POP.TOTL?view=chart>

## Chapter 5

# Adam's Garden or Eve's?

## A Gender-Centric Analysis of Corruption Perceptions

**Ayesha Afzal**

*Lahore School of Economics, Pakistan*

**Aiman Asif**

*Lahore School of Economics, Pakistan*

### ABSTRACT

*Corruption, or the misuse of public office, has become a major concern for governments in recent years. The purpose of this study is to identify how women, in an economic capacity, influence perception of corruption in a country, and how the relationship changes over time. Female empowerment movements have grown in the past decades, resulting in increased labour force participation of women. This chapter considers 167 countries from 1995 to 2018 to study the relationship. The results suggest that working women in an economy have a significant impact on reducing the perceived level of corruption, from 2007 to 2018, whereas this effect is not as strong in the earlier decade. These findings have implications for policies surrounding female employment. It is suggested that encouraging women to get higher education and become professionals can help curb the levels of corruption, especially in developing countries where corruption is widely prevalent.*

### INTRODUCTION

Corruption has prevailed in various institutions, governments, and social settings, over thousands of years, with the earliest records dating back to 2<sup>nd</sup> and 3<sup>rd</sup> century B.C. This wide nexus of corruption has led organizations, such as the World Bank and Transparency International, to consider corruption to be a hindrance to economic growth and development, and to recognize that it leads to an inefficient allocation of resources, distortions in policies, and hurts the lower income groups (Gouda and Park, 2015).

DOI: 10.4018/978-1-7998-5567-5.ch005

Allegations and affirmations of corruption in recent years have had a significant impact on the political and justice systems worldwide. Political accountability movements, such as those stipulated after Panama Papers materialized in 2016, have become a focal area of electoral campaigns. The outrageous prevalence of corruption has shaken up many governments and led to the deposing of various heads of state. In these circumstances, the role women has become a center of attention, given the perception that women are less corrupt.

The study aspires to elucidate what determines corruption levels, and to bring forth the role that female labour force participation may play in regulating the prevalence of corruption. In doing so, the research aims to provide governments and institutions the tools to identify, in particular, the role of gender and corruption, in a country. Private businesses, government institutions, and policy makers will be able to benefit from this study, to evaluate whether female employment can lead to higher efficiency, improve productivity and transparency within institutions.

## **ROLE OF WOMEN IN CORRUPTION**

The role that women can play *vis-a-vis* corruption is a widely understudied subject. Women are stereotypically believed to be more honest and risk averse, compared to their male counterparts. Several empirical studies, especially under an experimental setting, such as Esarey and Schwindt-Bayer (2019) and Barnes *et al.* (2018), find that women may mitigate corruption within public institutions, including legislation, bureaucracy, and law enforcement. Largely, such studies only concentrate on the public sector, and the employment of women in the government, or law enforcement institutions, such as the police. Private organizations are often unwilling to provide such information, and allow researchers to implement an experiment, or study the practices within the organization.

A substantial level of risk and moral aversion is expected in females as an outcome of cultural or institutional restraints. The aftermath of which is women being reluctant to indulge in bribery and corruption (Esarey and Schwindt-Bayer, 2019). Assuming that women have a lower tolerance for risk, it is often suggested that women are less likely to make decisions with a higher degree of risk involved or be employed in a sector which is high-risk. Thereby, women may dissociate themselves from corrupt activities and may be less likely, compared to their male colleagues, to accept a bribe. This idea is based on utility maximization where individuals may commit crimes or indulge in illegal activities when they are more risk loving. However, this is all circumstantial and contingent on the stereotype being factual.

Proponents of female empowerment highlight that there is little evidence of female involvement in corruption. The correlation between female politicians and lower corruption has been established in recent years, which is often naively associated with the cliché that women are more honest. Survey experiments have hinted that some degree of causation is plausible; the evidence still is lacking. One rational explanation suggests that women are considered “political outsiders”. This is reinforced by the fact that women are unable to emulate the social capital of men in elite circles where this corruption may be taking place (Wachs *et al.*, 2019). Social networks facilitate the development of dense communities, where individuals are homogenous. Such tightly knit communities may often be based on factors such as ethnic backgrounds or class. These networks promote exclusivity and prevent the inclusion of “outsiders”, as a mechanism for building trusts and bonds, and developing social capital within the network. Women may therefore be excluded from such networks, as they do not match the social capital, in terms of ethnicity, religion, economic status, or even gender.

Therefore, when it comes to positions of power and influence, be it public office or a private organization, women are far fewer in number, and therefore, may not have the necessary access to these male-dominated corruption networks. Men within these networks will be inclined to exclude women from these exclusive “boy’s clubs”. Even if women have some restricted access to these networks, such networks promote favoritism within the group, and create an environment for nepotism and corruption. Thus, even with access to networks, women may still be at a disadvantage. When choosing to assign a contract between members of the particular corrupt network, men with greater social capital, and higher standing would always be preferred to women (Wachs *et al.*, 2019). This fact is reiterated by Fazekas and Wachs (2020), who highlight the prevalent corruption in procurement markets and support the fact that non-favoured entities are excluded from obtaining government contracts.

It is also highlighted that women in the government may be unaware of the corrupt networks prevalent within the male-dominated institutions, and therefore, an increase in representation of women at the government or parliament level may create a disruption in this system. In this case, women are unaware of the network of corruption, thereby creating an information asymmetry across gender, and thus resulting in a negative association between female participation and corruption (Esarey and Schwindt-Bayer, 2019).

In reality, women may pursue corruption of a different nature and scale compared to men, which may lead to the stereotype of women being less corrupt. Women are anticipated to be involved in smaller scandals where illicit means are adopted to attain public services they would otherwise be deprived of. Contrarily, men undertake such activities at a larger scale, with a motive of obtaining unwarranted power or wealth. Bauhr and Charron (2020) defined this as greed corruption, where individuals indulge in corruption to create inequitable circumstances, through some illicit advantage or unfair wealth and power. Therefore, when it comes to prominent corruption cases of a magnanimous proportion regarding political imbalance and exploitation, the front runners are mostly male. However, this does not make women any less corrupt, as they too are involved in corruption of a different nature.

Some literature supports the idea that women have a negative impact on the level of corruption within an economy, in a non-experimental setting. Studies find that female participation in the labour force and politics tends to reduce the level of corruption prevalent in a country (Debski *et al.*, 2018). This relationship holds true for the representation of women in the parliament and also corruption within the government (Esarey and Schwindt-Bayer, 2019). Similarly, as female entrepreneurship has grown over the past decade, findings suggest that such firms are less likely to indulge in corrupt activities (Breen *et al.*, 2017). However, there is little concrete evidence establishing whether an increasing proportion of female workforce is necessarily a good sign for the economy in terms of corruption and the perception of corruption. Moreover, evidence is lacking as to how women reduce corrupt.

## **CORRUPTION VS. PERCEPTION OF CORRUPTION**

It is essential to discern between corruption and its perception, in order to differentiate between the two most commonly used proxies for measuring corruption. Corruption is the misuse of public office and authority. This is an objective measure, where individuals are expected to conduct themselves in *modus operandi*, avoiding immoral or corrupt behavior as identified by the requisite law. Due to the nature of activities that comprise corruption, it is difficult to quantify the degree of corruption in a country, especially for comparison across countries.

The perception of corruption, in contrast to corruption, is more subjective in nature and is often determined through opinion-based questions and surveys. Often, a person's perception of corruption may be determined through their inclination towards bribery, tax evasion or payments for a public good. Using data from such surveys, a Corruption Perceptions Index has also been constructed by Transparency International. This index uses 12 different surveys, and scores countries based on how corrupt the country is perceived to be, given the information in these surveys. The index scores countries such that a country having high levels of corruption scores closer to zero. This index also ranks countries out of 180, making the comparison across countries easier. The surveys come from different sources, and therefore prove to be an unbiased source of information, making the index score reliable.

The results conclude that there is a statistically significant inverse relationship between the level of corruption and women's participation in the labour force, such that higher participation of women leads to lower levels of corruption in the country. This effect is particularly seen in the past decade, from 2007 to 2018, where female participation in the formal workforce has become more widespread, compared to the earlier decade.

The chapter has been structured as follows: section II discusses some possible causes of corruption and its ramifications for an economy, section III presents the framework for the study, section IV discusses the methodology, and section V contains the empirical findings. Finally, Section VI presents the conclusion, along with policy recommendations to use the findings effectively.

## **SIGNIFICANCE OF CORRUPTION**

### **What Leads to the Phenomenon of Corruption?**

Corruption is a complex phenomenon which needs to be understood in all its facets to address this problem. Researchers have examined factors within a country that can affect its ranking in various corruption indices. There is evidence that governance indicators, such as the democratic process and the quality of law enforcement, as well as the level of economic development, are extremely important in determining the level of corruption in a country.

The incidence of corruption may vary across different segments of the society, based on their religious inclination, gender, social status and moral values. The involvement of an individual in bribery may depend on their self-condemnation as a result and peer pressure, suggesting that willingness to be corrupt was influenced through social interactions (Dong, Dulleck and Torgler, 2012). Similarly, individuals that are more inclined towards religious values are less likely to indulge in corrupt behavior (Gouda and Park, 2015). The association between gender and involvement in corruption is considered to be inverse, based on individual level data, implying that women are less likely to recognize corrupt behavior as appropriate, and therefore less likely to justify it (Torgler and Valev, 2010). One explanation already offered for this relationship suggests that women are less likely to be included in the male dominated corruption networks, while others suggest that gender discrimination may prevent women from being able to benefit from corruption, while being a part of these networks.

Corruption within a system can be greatly influenced by the current political scenario in a country. Even in a well-institutionalized political system, private interests of the politicians or bureaucracy can lead to officials making policies or decisions where private benefit exceeds public welfare. This is especially prevalent in systems where the autonomy of the elite is beyond the system of accountability (Sun

and Johnston, 2009). However, people are expected to be more aware of their rights, and their freedom in a democratic political system. Within a liberal democracy, citizens anticipate having the freedom to scrutinize and criticize the government for their corrupt activities, and have access to accountability of the bureaucracy and political elite, whereas such civic engagement may not be possible under other political regimes. Thus, a more democratic system is expected to have lower levels of corruption for high income countries whereas democratization increases corruption levels in developing countries (Jetter *et al*, 2015). This is particularly true if democracy within a country is durable, as measured by the Polity IV indicator for governance.

The age of a democracy can be critical for determining the level of corruption. Regulation and accountability within a democracy develop as the democracy matures. As a result of the long-term presence of a democratic regime, democratic institutions are developed, which can be instrumental in the reduction of corruption. It is estimated that democracy should be prevalent for at least 40 years before having an impact on corruption levels in a country (Kalenborn and Lessman, 2013; Nightingale, 2015).

In a similar manner, a more educated population will be less likely to accept the corrupt behaviour of bureaucrats and institutions, as education allows people to learn about their rights and increases their awareness in general. Thus, education may also have a negative impact on the levels of corruption in a country. Despite all these possible determinants, it is imperative to understand the causes and consequences of corruption to enable the governments to address the issue.

## **Impact of Corruption**

Corruption causes disruptions in the functioning of public and private institutions. Foremost, governments are unable to achieve their objectives when the elites within it choose to maximize private benefit and utility by indulging in corrupt activities. Moreover, the reduction of corruption comes with a price tag where the institutions have to incur a higher price. This is because institutions will be required to ensure that its members think beyond their personal gain; they will also have to ensure that law enforcement agencies are not bribed and are working efficiently.

As far as the economic effects are concerned, corruption results in an inefficient allocation of resources as government contracts may be handed over to the party offering the highest bribe, rather than on the basis of productive or allocative efficiency, thereby reducing the efficiency of the government (Elbahnasawy and Revier, 2012). Decisions are often based on vested interests of the influential political elite and they influence society in a detrimental manner. This is witnessed especially when funds are seen to be allocated inefficiently to a development project with greater kickbacks and political returns instead of being allocated to projects with a higher social welfare, such as the improvement of government schools, or the provision of free healthcare.

Similarly, corruption scandals of the elite may lead to encouraging bribery and corruption at lower levels within the government. Such scandals reduce the reliability of public institutions, affect the sentiments of the public as well as become an obstacle for the democratic process of a country (Treisman, 2000). This was witnessed when the Panama papers were released in 2016. The general public loses trust in the individuals that comprise the bureaucracy, resulting in people being less willing to pay for public goods or to pay taxes. The society as a whole will therefore decline, as people can no longer trust institutions, especially law enforcement, and will not be willing to contribute to its development. However, governments have made attempts to reinstate this trust through various legislations. It was after the release of Panama papers that 16 countries collected over \$500 million in unpaid taxes and penalties.

In India, the National Rural Employment Guarantee Act (2005) has been a source of controversy in recent years. The Act was introduced to improve income security for poorer households in the country, promising them 100 days of unskilled manual labour at the market wage. However, in 2015, only 28% of the workers were paid on time, as compared to 2018, when 32% payments were made on time. Moreover, in 2018, around 600 cases of violations of the act were reported, and workers complained about middlemen pocketing their payments (Kapoor, 2018).

In the US, the Racketeer Influenced and Corrupt Organizations (RICO) Act has helped curb infiltration of criminal organizations and corrupt officials within government ranks, as well as enterprises that may affect foreign or interstate trade. In May 2015, several FIFA officials were arrested under this Act, on 47 counts of money laundering and wire fraud, and suspicions of \$150 million in bribes (Gibson and Gayle, 2015). The RICO act is being used to root out corruption from within government institutions as it gives the Attorney General the right to indict public officials who have a direct or indirect interest in an enterprise or be a stakeholder in foreign or interstate commerce with higher penalties.

Another journalistic expose, called the “Paradise Papers” consisting of almost 13 million documents, from 2017 resulted in widespread action across the globe. The Papers highlighted the extent of exploitation of individuals, where even universities like Stanford, were exposed of their offshore “investments”. As a result, the European Union has made attempts to reduce these “tax havens” (Fitzgibbon and Starkman, 2017). These papers featured hundreds of scandals regarding prominent individuals, including the Queen of England whose private estate was involved with offshore investments in the Cayman Islands and Bermuda, also with Prince Charles. Similarly, three Canadian prime ministers were named in the paper’s offshore maneuvers. Stephen Bronfman, a close associate, and adviser of Prime Minister Trudeau has also been revealed in these papers for avoiding taxes, and moving multimillion-dollar cash flows to Leo Kolber, a former senator.

The level of corruption in a country affects its external affairs as much as internal matters and can have spill-over effects. One example of this is the Red Mafia in Chongqing, China, which was a group of corrupt government officials providing protection to organized crime groups. This mafia helped in creating monopolies, and thus reduced investment in the province, as a result harming the economic activity in the area (Wang, 2013).

Mexico was one of the most corrupt countries in the world in 2018, according to Transparency International. A recent example of the rampant corruption in the country is oil theft, where almost 20 percent of the daily production is stolen by the employees of Pemex, a state-owned oil company (Garcia and Parraga, 2019). Moreover, the Energy Regulation Commission has found the law enforcement profiting from this racket alongside the employees, making it difficult for the government to reduce this theft (Dey and Rodriguez-Espindola, 2019). As a result, Mexico is unable to export more oil, despite increases in production, making investment futile for the economy.

Corruption, especially at such a large scale, has a direct effect on the major components of aggregate expenditure, such as net exports, investments, and consumption. This also has an indirect effect on the economy through flows of foreign currency and exchange rates. Investment declines where corruption is prevalent, because where businesses are expected to pay higher bribes as a way to reduce bureaucratic delays, fewer businesses will enter the market. A waning of economic activity is inevitable in such countries, as entry into industries is restricted, and equipment investment declines. Consequently, in the long term, production is lower and consumption declines within the economy, as needs of the public are ignored, and public officials try to maximize their personal gains (Sriyalatha, 2019).



Where corruption is widely prevalent, the inefficient allocation of resources to projects that have greater kickbacks, rather than to projects which will have greatest social benefit, together with the interrupted market mechanisms, create what may be considered a dead weight loss of corruption in terms of slowed growth and hindered development in the long run. Thus, it is essential that for an economy to grow sustainably, corruption within an economy is curbed and its dead weight loss is minimized (De Groot *et al.*, 2003).

## THEORETICAL FRAMEWORK

Treisman (2000) and La Porta *et al.* (1999) are two of the most important pieces of literature pertaining to determining the causes of corruption. Initially, the researchers focusing on the determinants looked at country level characteristics, or just individual level characteristics. Later expositions use their techniques, and similar variables, and try to identify which variable is the most important to explain the incidence, or “justifiability” of corruption. This variable is frequently used in studies, including Lee and Guven (2013), which focuses on micro-level data, and pertains to an individual’s likelihood of accepting a bribe, or claiming a benefit.

Previously, studies have focused on micro-level dataset, identifying the characteristics of an individual (such as gender) and the household, in order to determine what makes them more susceptible to corrupt activities. In most cases, studies analyzing the determinants of corruption recognize that various characteristics, broadly identified as household characteristics and community level characteristics need to be accounted for, or controlled, because they may have an impact on the results. However, the effect of macroeconomic variables on corruption, specifically with respect to female participation in the economy, remains largely unexplored. This study, therefore, focuses on exploring the impact of macro-level variables and female participation on corruption.

## DATA

To estimate the relation between corruption and female participation, 137 countries have been included in the analysis over 23 years, from 1995 to 2018. This particular time frame has been selected as female participation in the formal economy has seen an immense increase over these decades. This increase has been encouraged due to the female empowerment movements all across the world, along with the demands for gender equality.

The data for this study has been sourced from World Bank’s World Development Indicators (WDI), Transparency International, International Labour Organization, Integrated Network for Societal Conflict Research (INSCR) and the United Nations Development Program’s Human Development Data. These sources have been largely referred to in existing literature, by studies including Gouda and Park (2015) and Debski *et al.* (2018) and are more reliable and exhaustive sources of information. A detail of the variables, their definitions and their sources is given in the table 1.

The dependent variable, which is essentially the level of corruption, will be measured using the Corruption Perceptions Index, published annually by Transparency International. The organization defines corruption as the abuse of power and authority for any sort of gains, specifically in the government sector. This index scores 180 economies out of 100 points, where a larger score indicates a lower degree of

*Table 1. Variable Details*

Variable Name	Definition	Source
z-scores	The Corruption Perception Index value converted to a normal distribution. A higher z-score indicates lower corruption.	Transparency International, Author's Estimates
Female participation (ages: 15-64)	Females who are economically active as a proportion of female population between the ages of 15 and 64.	International Labour Organization
Female Labour force (% of working population)	Females who are economically active as a proportion of total working population.	International Labour Organization
Log of GDP per capita (lnGDP)	Natural logarithm transformation of GDP per capita	World Development Indicators, Author's Estimates
Foreign Direct Investment (FDI)	Net investment flows from abroad to acquire a long-term management interest as a proportion of GDP	World Development Indicators
Polity IV	A quantitative index coding qualitative characteristic of a country, making institutional quality comparable across countries.	Integrated Network for Societal Conflict Research
Education (average years)	Average years of schooling received by the population in a country.	Human Development Data, United Nations

corruption. This index is comprehensive, in that it considers 13 different sources of data, ensuring that the index value is completely unbiased.

The index is converted to z-score values by the authors of this study to improve comparability across years. This transformation is required because the scoring of the index changes in 2012. The index scores countries on a scale of 0 to 10 from 1995 to 2011. However, 2012 onwards, the methodology changed to have a constant average and standard deviation each year, to make it comparable across years. Conversion of annual index into z-scores is helpful because it creates a normal distribution for each year, based on their index value. It is important to highlight that the z-scores are constructed in accordance with the original index, and therefore, a higher z-score indicates lower corruption. Similarly, any variable with a positive coefficient would suggest a negative relationship with corruption.

Within the independent variables, female labour participation in the workforce is the variable of interest. Female labour force participation rate for women between 15 and 64 years, as the primary measure for female employment. The secondary measure is female labour force as a proportion of the total workforce. Both these measures are reported by the International Labour Organization (ILO), and are used in research. The main difference in these variables is that while one compares the female labour force to the female population the second measure considers male employment as well.

## METHODOLOGY

To empirically analyze the relationship between gender and corruption, and whether more women joining the workforce improves efficiency, or leads to corruption, the basic model for estimation is given as follows. A simple, linear regression model and a panel regression model with random effects is adopted.

$$CORRUPT_{it} = \beta_0 + \beta_1 FLFP_{it} + \beta_2 \ln GDP_{it} + \beta_3 FDI_{it} + \beta_5 POLITY_{it} + \beta_6 EDU_{it} + \varepsilon_{it}$$

It is important to consider that the women empowerment movement and female participation in the labour force was increasing in the 1990s and early 2000s. This began in 1992, which was declared the “Year of the Woman,” in the United States (US) where over 20 women were elected to the Congress, making it a new record. The UN Security Council Resolution 1325, passed in 2000, became the first framework that called for women’s participation at the global level for conflict resolution. Moreover, the Millennium Development Goals set by the UN greatly emphasized that women should be provided relevant healthcare, better education, and greater employment opportunities to make development in a country sustainable.

Local movements also helped women realize their role in society, such as the movement for peace in 2003 in Liberia, where women helped end a 14 year civil war; or the Gulabi Gang movement against domestic violence, in India, in 2006. Moreover, the World March for Women, which was founded in 2000, became an important turning point for these local movements. This feminist movement has worked for women empowerment and gender equality, raising a voice to highlight the discrimination against women all over the world. The March that began in Canada is so popular today that women all across the globe, even in countries like Pakistan, march out on the streets and demand equality every year on 8<sup>th</sup> March, which is now commemorated as the International Women’s Day.

In the early 2000s, this was all relatively new, and since women were new entrants in the formal workforce, and were highly discriminated, they may not have been able to affect the system as much. However, it was only a few years after the rise in movements for gender equality, where women began demanding equal pay and benefits, that they were competent and equal to their male colleagues. In order to cater for these social movements, a time split is considered in the data almost halfway. From 1995 to 2006, it is expected that women may not have had much of an impact on the level of corruption as they may have been discriminated against and excluded from any private networks. However, from 2007 to 2018, their male colleagues began treating them as equals as their number grew significantly with the rising awareness created by women’s movements. A difference in means test is conducted to test whether this difference in female participation was significant.

In the model above,  $CORRUPT_{it}$  represents the z-score of the index value of corruption for all countries and is the dependent variable. Based on the models presented by Branisa and Zielger (2010) and Ghaniy and Hastiadi (2017), this study uses a model that includes a relevant set of explanatory variables which try to explain the level of corruption within a country.

The explanatory regressor of interest in this model is the female labour force participation. This may affect corruption in various ways and may increase or reduce the level of corruption in a country.

So far, the available literature is unable to conclude whether the increasing number of working women in a country is necessarily good for decreasing the level of corruption. While Esarey and Schwindt-Bayer (2019) and Barnes *et al.* (2018) find that women reduce the level of corruption based on their higher level of risk aversion, these results are based on experiments and may not necessarily reflect the true situation across all occupations. In fact, Eckel and Grossman (2008) find that the risk preferences for men and women are often misrepresented, and so, while women are perceived to be risk averse and thus, less likely to indulge in risky behaviours such as corruption, it is possible that they are actually involved in such activities to a greater extent.

Other determinants of corruption included in our model are the level of economic activity, the average level of education, quality of governance, and foreign investment flows. The level of economic activity is measured by the log of GDP per capita, which helps control the economic growth and development in a country. This is included because more developed, or “richer”, countries can devote more resources

### ***Adam's Garden or Eve's?***

to the detection of corruption. However, countries with a lower level of development may have other priorities, such as reducing poverty levels, and providing basic necessities to the poorer population (Swamy *et al.*, 2001).

The average level of education in a country, as obtained from the United Nations, is an important indicator that is seldom used in the literature to explain corruption. A country where, on average, individuals are more educated will have lower levels of corruption. This may be because people with higher levels of education are more aware of their surroundings, and understand the law better, and thus will understand the consequences of getting caught better than the less educated. Moreover, more educated people will be more likely to report any such activity.

The quality of governance and political stability in a country play a very important role in the control of corruption. Countries with greater stability and better governance are also associated with better quality institutions and more transparency, allowing for more democratic processes. Citizens in such a country are more likely to trust the system, and thus, less likely to get involved in corrupt activity. The Polity IV score is constructed on six different dimensions of governance, including government integrity, protection of property rights and judicial effectiveness, making it a wholesome measure for governance.

Foreign Direct Investment (FDI) is also included in the model, as a measure for foreign investment flows. A higher level of FDI is associated with freedom to move funds, and thus is indicative of a lower level of corruption. Countries with higher levels of FDI will also have better terms with their trade partners and would have little margin for corrupt officials to create artificial barriers in investment in the economy, in order to get some kickbacks.

## **EMPIRICAL RESULTS**

To estimate the model, it is imperative to determine whether there is a significant difference in the average female participation over time. Over 23 years, the social scenario changed globally, allowing for a greater proportion of women to join the labour force. Therefore, the empirical results include full panel regressions, for all 23 years, as well as splitting the sample into two halves, in order to understand whether the effect of female participation in the labour force was constant over time, or if it changed as the proportion of women in the labour force increased.

The sample is split through the time variable, from 1995 to 2006, and from 2007 to 2018. A difference in means test is conducted to ensure that there is statistical difference in the female participation over time. Table 2 presents the results for this test.

*Table 2. Difference in means test*

Variable	Mean (1995-2006)	Mean (2007-2018)	t-Value	t-Critical (5%)
Female participation (ages: 15-64)	56.51	57.60	1.7501	1.65
Female Labour force (% of working population)	25.70	26.21	1.68	1.65

The difference in means tests concludes that both measures of female participation in the labour force are significantly different in the selected time range. Therefore, the regression analysis may present different results for these time panels.

The results for the basic model that is the Pooled OLS Regression Model are given in Table 3.

*Table 3. Pooled OLS Regression Results*

	(1)	(2)	(3)
<b>Dependent Variable:</b>	<b>1995-2018</b>	<b>1995-2006</b>	<b>2007-2018</b>
<b>Corruption Perception Index (z-Scores)</b>	<b>OLS</b>	<b>OLS</b>	<b>OLS</b>
Female participation rate (age: 15-64)	0.0101**** (0.00212)	0.0103**** (0.00285)	0.0102**** (0.00201)
lnGDP	0.351**** (0.0384)	0.411**** (0.0439)	0.343**** (0.0430)
FDI	0.000741 (0.000636)	0.000476 (0.000683)	0.000934 (0.000896)
Polity IV	0.0424**** (0.00404)	0.0323**** (0.00516)	0.0454**** (0.00434)
Education (average years)	-0.0201 (0.0153)	-0.00196 (0.0188)	-0.0325 (0.0180)
Constant	-5.937**** (0.258)	-5.831**** (0.310)	-6.038**** (0.264)
Observations	2,898	1,063	1,835
R-squared	0.767	0.775	0.786

Robust standard errors in parentheses

\*p<.05, \*\*p<.01, \*\*\*p<.001, \*\*\*\*p<.0001

The pooled regression results indicate that female participation in the female labour force has a strong impact on corruption, such that an increase in female participation in a country will reduce the perceived level of corruption in the economy. It must be kept in mind that the Corruption Perceptions Index, and consequently its z-scores, are constructed such that a higher score indicates lower levels of perceived corruption in the economy. The second measure for female participation, which measures female employment as a proportion of the working population, for the same model also reiterates these findings. (These results are presented in Table 4.) This prevents the results from being biased towards a particular measure of female employment.

The results of the pooled regression indicate that the relationship does not change for the different time periods, with respect to female participation. However, there is a change in the relationship for education. Average education in a country, according to these results, has an insignificant effect or a positive effect on corruption. The result is only significant for the 2007 to 2018 panel, showing that an increase in average years of schooling leads to an increase in corruption.

*Table 4. Pooled OLS: Regression Results*

	(1)	(2)	(3)
Dependent Variable:	Full Panel	1995-2006	2007-2018
Corruption Perception Index (z-Scores)	OLS	OLS	OLS
Female participation rate (% working population)	0.0174**** (0.00408)	0.0188*** (0.00562)	0.0178**** (0.00397)
lnGDP	0.368**** (0.0400)	0.428**** (0.0466)	0.364**** (0.0445)
FDI	0.000802 (0.000627)	0.000417 (0.000633)	0.00106 (0.000964)
Polity IV	0.0434**** (0.00415)	0.0323**** (0.00544)	0.0467**** (0.00449)
Education (average year)	-0.0159 (0.0151)	0.00439 (0.0183)	-0.0305 (0.0180)
Constant	-6.046**** (0.281)	-5.924**** (0.342)	-6.190**** (0.284)
Observations	2,877	1,054	1,823
R-squared	0.756	0.766	0.775

Robust standard errors in parentheses

\*p<.05, \*\*p<.01, \*\*\*p<.001, \*\*\*\*p<.0001

The Polity Index score, which measures governance, has a consistently significant effect on the level of corruption, which suggests that a higher quality of governance and better institutions will help curb the level of corruption in a country. The economic development of a country, measured using the log of GDP per capita, suggests a similar relationship, where countries with a higher level of economic development, or richer countries, have a better corruption score, and thus lower corruption.

However, pooled regression estimates are not enough to conclude the relationship between corruption and its determinants. This is because, when observing the same entities across time, pooled regression analysis ignores the correlation between the observations, making these results unreliable (Wooldridge, 2010). Therefore, a fixed or random effects model is more suitable for panel data. The Breusch-Pagan Lagrangian Multiplier test is conducted to test any variance across countries and to identify whether random effects are suitable (Table 5). The null hypothesis for the test states that there is no significant difference across entities, or countries in this case, and therefore the variance is zero (Breusch and Pagan, 1980). The p-value for this test is less than 0.05, therefore we cannot reject the null hypothesis. This suggests that the random effects model is a suitable fit for the data because variance across countries is zero.

*Table 5. Breusch-Pagan Lagrangian Multiplier test*

$\chi^2$	p-Value
13746.67	0.00

Based on the Breusch-Pagan Lagrangian Multiplier test, therefore the random effects model for the panel regression is used as it is more suitable.

The results for the panel regression with random effects are given in Table 6 and 7, for the two measures of female participation.

*Table 6. Panel regression with Random Effects*

	(1)	(2)	(3)
<b>Dependent Variable:</b>	<b>Full Panel</b>	<b>1995-2006</b>	<b>2007-2018</b>
<b>Corruption Perception Index (z-Scores)</b>	<b>Panel OLS</b>	<b>Panel OLS</b>	<b>Panel OLS</b>
Female participation rate (age: 15-64)	0.00151 (0.00240)	0.00106 (0.00333)	0.00875**** (0.00205)
lnGDP	0.133**** (0.0269)	0.169**** (0.0395)	0.215**** (0.0298)
FDI	0.000735**** (0.000210)	-0.000357 (0.000447)	0.000850**** (0.000225)
Polity IV	0.0167**** (0.00277)	0.0142**** (0.00320)	0.0188**** (0.00379)
Education (average years)	0.0123 (0.0143)	0.0294 (0.0162)	0.0605**** (0.0144)
Constant	-2.330**** (0.277)	-2.522**** (0.373)	-3.996**** (0.298)
Observations	2,898	1,063	1,835
Number of countries	167	141	166

Robust standard errors in parentheses

\*p<.05, \*\*p<.01, \*\*\*p<.001, \*\*\*\*p<.0001

The results from Table 6 suggest that female participation does change in its effect on the perceptions of corruption in a country over time. While there is no significant relationship between female labour force participation and the corruption perceptions z-scores until 2006, the relationship is significant after 2007. These results suggest that increasing female labour force participation increases the z-scores, and their corruption perceptions score, suggesting that the country has a lower level of corruption. Similarly, average years of education and FDI also increase in their significant effect on corruption over time, even though this effect is not obvious in the full panel regressions from 1995 to 2018.

The results from Table 7 narrate a similar story. The results from 1995 to 2018 suggest that the increasing female participation has led to an increase in the level of corruption, by reducing the corruption perceptions score. However, columns (2) and (3) suggest that while the negative effect of female participation from 1995 to 2006 is insignificant, the impact on corruption levels changes direction and becomes statistically significant after 2007. From 2007 to 2018, the relationship changed and increases in female participation led to a decrease in the level of corruption.

*Table 7. Panel Regression with Random Effects*

	(1)	(2)	(3)
Dependent Variable:	Full Panel	1995-2006	2007-2018
Corruption Perception Index (z-Scores)	Panel OLS	Panel OLS	Panel OLS
Female participation rate (% working population)	-0.00805 (0.00472)	-0.00703 (0.00650)	0.00961* (0.00394)
lnGDP	0.128**** (0.0271)	0.154**** (0.0417)	0.210**** (0.0307)
FDI	0.000623** (0.000200)	-0.000331 (0.000432)	0.000724*** (0.000234)
Polity IV	0.0166**** (0.00276)	0.0141**** (0.00316)	0.0192**** (0.00383)
Education (average years)	0.0184 (0.0141)	0.0316 (0.0161)	0.0713**** (0.0147)
Constant	-2.048**** (0.290)	-2.183**** (0.396)	-3.813**** (0.327)
Observations	2,877	1,054	1,823
Number of countries	166	140	165

Robust standard errors in parentheses

\*p&lt;.05, \*\*p&lt;.01, \*\*\*p&lt;.001, \*\*\*\*p&lt;.0001

With respect to other control variables, the findings are supported by literature and economic theory. Countries with higher levels of development have significantly lower levels of corruption. Similarly, better quality of governance, indicated by a higher Polity score, will reduce the level of corruption within the economy, and countries with a more educated population on average will have lower corruption. An inflow of foreign direct investment makes the country less corrupt, as increases in the investment make it more susceptible to scrutiny from the legal and political system.

Average years of education and foreign investment are both significant for 2007 to 2018 dataset. However, their effect in the full panel regression, or earlier decades, is less significant. This indicates that over the years, certain changes in the society and economy have occurred, which explain this trend, along with the change in the effect of female participation. Therefore, in recent years, the determinants of corruption may have changed.

## CONCLUSION

This study examines the relationship between the level of corruption in a country and the participation of women in the labour force, controlling for various other causes of corruption in the model. The study uses panel data over a panel of 167 countries, for 23 years, from 1995 to 2018. The dataset is split into two, from 1995 to 2006 and from 2007 to 2018, for further investigation into how the determinants change over time.



These results are highly aggregated and are not restricted to a certain group of countries. The results of this research identify that there is a statistically significant relationship between the level of corruption and the involvement of women in the labour force, such that increased participation of women in the workforce leads to a lower level of corruption in the country. This is perhaps because women are less likely to be involved in corrupt activities, compared to men.

The relationship between gender and corruption on a macroeconomic level can be justified by the idea that women in a working environment are more risk averse, and honest, and may be working due to financial constraints. These factors make them less likely to risk their social standing or their job. This argument strengthens the notion that women are more honest and less likely to indulge in risky endeavours.

While one possible explanation could also be that women in a professional environment are unaware of the corruption that takes place around them, the changing trend over time indicates that the effect takes place sometime after the female empowerment movements allowed for women to be treated equally. This suggests that the reduction in corruption levels only takes place after women are considered a permanent part of the workplace, dismissing the explanation that women may be unaware of the corruption.

Considering these findings, governments and institutions should be able to identify the importance of women in the labor force, and to identify their role in corruption reduction in a country. Firms, private and government institutions, and policy makers will be able to benefit from this study, to evaluate whether or not female employment can lead to lower dead weight losses and improved productivity. Similarly, women in higher managerial positions are more likely to create an environment of transparency, and thus reduce malpractice in the business environment at a higher level.

Keeping these findings in mind, the government should encourage women empowerment programs, and create an environment that encourages women as entrepreneurs and senior management. This further implies that the government should incentivize the education of women at all levels, to ensure that these women contribute to the labor force in a more productive way.

Educated women will, in the long run, have better opportunities for work. The government can also reduce the prevalent corruption, particularly in the government institutions, through setting a quota for women; such as a higher quota for females selected in the Civil Services through the competency exams as well as encouraging political parties to promote female representation in a country's legislature. Similarly, to improve the quality of institutions and to improve the system of governance in a country, more women should be encouraged to be a part of the national and provincial assemblies, and more women should be involved in the decision making processes. It must be kept in mind that this process of female literacy, employment and education is a long-term process and will need consistent policies over at least a decade, in order to reap the benefits in terms of corruption reduction.

Future research in this area should identify what causes women to be less likely to indulge in corrupt behaviour. Finding the cause behind this difference across genders can be particularly helpful in identifying why people indulge in corrupt activities, and therefore help reduce the levels of corruption at the government and administrative levels as well as improve the business environment of a country. Moreover, as the findings suggest, the determinants of corruption are changing over time. Therefore, these new determinants need to be highlighted for better policies to be developed to reduce the level of corruption in a country, and to improve the quality of institutions.

## DISCLAIMER

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

- Barnes, T. D., Beaulieu, E., & Saxton, G. W. (2018). Restoring trust in the police: Why female officers reduce suspicions of corruption. *Governance: An International Journal of Policy, Administration and Institutions*, 31(1), 143–161. doi:10.1111/gove.12281
- Bauhr, M., & Charron, N. (2020). Do men and women perceive corruption differently? Gender differences in perception of need and greed corruption. *Politics and Governance*, 8(2), 92–102. doi:10.17645/pag.v8i2.2701
- Branisa, B., & Ziegler, M. (2010). *Reexamining the link between gender and corruption: The role of social institutions* (No. 24). Courant Research Centre: Poverty, Equity and Growth-Discussion Papers.
- Breen, R. E. H., Tasker, S. L., & Hiebert, B. (2017). How self-employed women with children manage multiple life roles. *Canadian Journal of Counselling and Psychotherapy*, 51(3), 187–206.
- Breusch, T. S., & Pagan, A. R. (1980). The Lagrange multiplier test and its applications to model specification in econometrics. *The Review of Economic Studies*, 47(1), 239–253. doi:10.2307/2297111
- De Groot, H. L., Linders, G. J., & Rietveld, P. (2003). *Why do OECD-countries trade more?* (No. 03-092/3). Tinbergen Institute Discussion Paper.
- Debski, J., Jetter, M., Möhle, S., & Stadelmann, D. (2018). Gender and corruption: The neglected role of culture. *European Journal of Political Economy*, 55, 526–537. doi:10.1016/j.ejpoleco.2018.05.002


- Dey, P. K., & Rodriguez-Espindola, O. (2019, February 27). *Mexico is being held to ransom by oil thieves and systemic corruption*. Retrieved from <https://theconversation.com/mexico-is-being-held-to-ransom-by-oil-thieves-and-systemic-corruption-111118>
- Dong, B., Dulleck, U., & Torgler, B. (2012). Conditional corruption. *Journal of Economic Psychology*, 33(3), 609–627. doi:10.1016/j.joep.2011.12.001
- Eckel, C. C., & Grossman, P. J. (2008). Men, women and risk aversion: Experimental evidence. *Handbook of Experimental Economics Results*, 1, 1061–1073.
- Elbahnasawy, N. G., & Revier, C. F. (2012). The determinants of corruption: Cross-country-panel-data analysis. *The Developing Economies*, 50(4), 311–333. doi:10.1111/j.1746-1049.2012.00177.x
- Esarey, J., & Schwindt-Bayer, L. A. (2019). Estimating causal relationships between women's representation in government and corruption. *Comparative Political Studies*, 52(11), 1713–1741. doi:10.1177/0010414019830744
- Fazekas, M., & Wachs, J. (2020). Corruption and the network structure of public contracting markets across government change. *Politics and Governance*, 8(2), 153–166. doi:10.17645/pag.v8i2.2707
- Fitzgibbon, W., & Starkman, D. (2017). *The 'Paradise Papers' and the Long Twilight Struggle Against Offshore Secrecy*. Retrieved from <https://www.icij.org/investigations/paradise-papers/paradise-papers-long-twilight-struggle-offshore-secrecy>
- Garcia, D. A., & Parraga, M. (2019, January 12). *Explainer: Mexico's fuel woes rooted in chronic theft, troubled refineries*. Retrieved from <https://www.reuters.com/article/us-mexico-fuel-explainer-idUSKCN1P52BC>
- Ghaniy, N., & Hastiadi, F. F. (2017). Political, social and economic determinants of corruption. *International Journal of Economics and Financial Issues*, 7(4), 144–149.
- Gibson, O., & Gayle, D. (2015, May 27). *Fifa officials arrested on corruption charges as World Cup inquiry launched*. Retrieved from <https://www.theguardian.com/football/2015/may/27/several-top-fifa-officials-arrested>
- Gouda, M., & Park, S. M. (2015). Religious Loyalty and Acceptance of Corruption. *Journal of Economics and Statistics*, 235(2), 184–206.
- Jetter, M., Agudelo, A. M., & Hassan, A. R. (2015). The Effect of Democracy on Corruption: Income is Key. *World Development*, 74, 286–304. doi:10.1016/j.worlddev.2015.05.016
- Kalenborn, C., & Lessmann, C. (2013). The impact of democracy and press freedom on corruption: Conditionality matters. *Journal of Policy Modeling*, 35(6), 857–886. doi:10.1016/j.jpolmod.2013.02.009
- Kapoor, M. (2018, September 26). *4 reasons why MGNREGA is not benefitting workers*. Retrieved from <https://www.businesstoday.in/top-story/4-reasons-why-mgnrega-is-not-benefitting-workers/story/282891.html>
- La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. (1999). The quality of government. *Journal of Law Economics and Organization*, 15(1), 222–279. doi:10.1093/jleo/15.1.222

- Lee, W. S., & Guven, C. (2013). Engaging in corruption: The influence of cultural values and contagion effects at the micro level. *Journal of Economic Psychology*, 39, 287–300. doi:10.1016/j.joep.2013.09.006
- Nightingale, E. (2015). *A critical analysis of the relationship between democracy and corruption*. University of Sussex.
- Sriyalatha, M. A. K. (2019). The Impact of Corruption on Economic Growth: A Case Study of South Asian Countries. *Economic Research Journal*, 3(10), 35–47. doi:10.29226/TR1001.2020.161
- Sun, Y., & Johnston, M. (2009). Does democracy check corruption? Insights from China and India. *Comparative Politics*, 42(1), 1–19. doi:10.5129/001041509X12911362972719
- Swamy, A., Knack, S., Lee, Y., & Azfar, O. (2001). Gender and corruption. *Journal of Development Economics*, 64(1), 25–55. doi:10.1016/S0304-3878(00)00123-1
- Torgler, B., & Valev, N. T. (2010). Gender and public attitudes toward corruption and tax evasion. *Contemporary Economic Policy*, 28(4), 554–568. doi:10.1111/j.1465-7287.2009.00188.x
- Treisman, D. (2000). The causes of corruption: A cross-national study. *Journal of Public Economics*, 76(3), 399–457. doi:10.1016/S0047-2727(99)00092-4
- Wachs, J., Yasseri, T., Lengyel, B., & Kertész, J. (2019). Social capital predicts corruption risk in towns. *Royal Society Open Science*, 6(4), 182103. doi:10.1098/rsos.182103 PMID:31183137
- Wang, P. (2013). The rise of the Red Mafia in China: A case study of organised crime and corruption in Chongqing. *Trends in Organized Crime*, 16(1), 49–73. doi:10.1007/12117-012-9179-8
- Wooldridge, J. M. (2010). *Econometric analysis of cross section and panel data*. MIT Press.

## Chapter 6

# Innovation and Corruption in Turkey: “Grease the Wheels” or “Sand the Wheels”

Hülya Ünlü

 <https://orcid.org/0000-0002-6429-7582>  
Cankiri Karatekin University, Turkey

Merve Karacaer Ulusoy

Ankara Yildirim Beyazıt University, Turkey

### ABSTRACT

*In this chapter, one of the important financial crimes and its effect on the innovation success of firms has been investigated for Turkey. The business environment and enterprise performance survey is used to examine how the business perceives informal payments for the period between 2013-2014. The main concern of the chapter is that when corruption is the case, either “sand the wheels” or “grease the wheels” is the result of being unproductive or (even worse) destructive entrepreneurs. Moreover, different corruption levels are estimated and tested by using a PROBIT model. It is suggested that while the “sand the wheels” effect is strong, financial resources should be transferred to the innovation investments rather than corrupt activities. Even though corruption does not show a hindering effect on innovation, the time spent by the managers is the “grease the wheels” effect for innovation.*

### INTRODUCTION

From the start of life till today, the world has been arguing the same specific question “*How can we survive?*”. Many scientists are trying to investigate this specific question from different points of view. After millions of years passed, our challenge to survive has not been changed whereas it should be focused on not only to survive but also to live in better conditions. The new goal is to improve our lifestyles as well as surviving. From the invention of fire to electricity, life still depends on important inventions. These inventions are needed in all sectors, from health to education, from finance to security. Adam

DOI: 10.4018/978-1-7998-5567-5.ch006

Smith explains why we are working so hard. According to his well-known book “Wealth of Nations,” the self-interest of people is the motivation of working more and being curious about creating new. He summarizes his thought as “*Give me that which I want, and you shall have this which you want, is the meaning of every such offer...*” (Smith, 1776). This makes sense and can be centralized and generalized for the intention of every behavior of people, enterprises, governments, international unions, and organizations around us. What we do not know is how self-interest can be limited by ethical issues. We may say that self-interest is the main idea behind the motivation of being creative, this idea creates the following question “What if we cross the line?”. Depends on which side of the line (using creativity to solve a problem in an ethical way or an unethical way) we are staying, the result of this solution may vary both for the microeconomy and macroeconomy.

If we stay on the right side of the line, self-interest is the source of motivation for being creative, which ends with creating value for the economy in the long term. On the other hand, if we stay on the wrong side of the economy may lead to the losing ability to grow sustainably. Understandings of creating value may change too. This time the questions might be “Is it possible that our self-benefit turns into someone else’s harm? Are we going to use our talent for creating good/services or are we going to use this talent for lobbying to get things done easily at our business for seeking more rent?”. In this study, we focus on finding answers to those questions.

*Figure 1. Innovation cycle*

*Source: Authors’ creation*



Baumol (1990) also took the attention of his readers to the above questions. In his study he mentions that productive entrepreneurs' directly or indirectly create value in the economy, namely, they choose to innovate. On the other side unproductive, or even worse destructive entrepreneurs broke this chain by joining rent-seeking or illegal activities, bribing, and various forms of other corrupt activities (Baumol, 1990, 1993; Sauka, 2008).

Especially in the 1990s, the phenomenon called corruption starts to get extremely remarkable. Although it started to become popular in the 1990s, traces of corruption can be found in history. One of the pieces of evidence of corruption was found two thousand years ago in India (Tanzi, 1998). Arthashastra is written by the Prime Minister of the Indian Emperor, Kautilya (350-275 BCE) (he is also known as a philosopher). *"Just as it is impossible knowing when a fish moving in water is drinking it, so it is impossible to find out when government servants in charge of undertakings misappropriate money."* (Rangarajan, 1987). In his saying he refers to the appearance of corruption. There is also evidence from the Arthashastra that how corruption may distract the creation of value in the economy *"He who causes loss of revenue eats the king's wealth, (but) he who produces double the (anticipated) revenue eats up the country and he who spends all the revenue (without bringing any profit) eats up the labor of workmen."* (Rangarajan, 1987). After all those years one can easily say that corruption takes more attention than any other time in history (Tanzi, 1998; Ibrahim, 2021).

Both innovation and corruption have been one of the most important issues mentioned with globalization, especially since the early 1990s. With the collapse of the Union of Soviet Socialist Republics (USSR) in 1991, there has been a transition from a planned economy to a market economy. This process brings an increase in many macro and socio-economic indicators such as inflation, unemployment, crime, poverty, and corruption. Regarding this, after Transparency International published the Corruption Perceptions Index in 1995, the interest in the concept of corruption has increased even more by the academicians and politicians (Carraro *et al.*, 2016; Khan, 1999; Schmidt, 2007; Smith & Thomas, 2015).

In this context, the two important factors "Innovation and Corruption" for economies are our concerns in this chapter. One step further than the work of Baumol (1990), we are interested in that when corruption is the case, which of the following situation is the result of being unproductive or (even worse) destructive entrepreneurs; "sand the wheel" or "grease the wheel".

Differently from previous years, international non-governmental organizations sound up, and become more and more active, such as IMF (International Monetary Fund), OECD (Organization for Economic Co-operation and Development), and TI (Transparency International). In addition to them, Panama Papers (ICIJ, 2017) and Wikileaks are also important sources fighting against corrupt activities. The information they released about corruption has an incredible effect. Today, there are Prime Ministers, CEOs, and politicians, who had to resign because of involving in corrupt activities (Prime Minister of Pakistan (Masood, 2017), Iceland (Fontaine, 2016), and Ukraine (BBC, 2016)). As a result, it does not make any sense whether the country has a high-income level and has a good average on Human Development Index or it has a low-income level, and it is at the bottom of the list.

This chapter focuses on the impact of an important kind of financial crime, which is corruption. Different types of corruption and different types of innovation have been used. It is tried to identify which corruption types have greased the wheel effect and which has the sand the wheel effects. It is implemented the empirical analysis by using firm-level data from the World Bank Enterprise Surveys for Turkey. Business Environment and Enterprise Performance Survey (BEEPS) has 1344 firms' respondents from Turkey in 2013. We measure corruption in different forms following its purposes and find that the regulatory burden has a positive impact on the product, process, market, and organizational innovations.

Taxes play a vital role in revenue collection for the betterment of an economy (Rafay & Ajmal, 2014). According to Rose-Ackerman (2007), the concept of administrative corruption specifically includes bribery and favoritism for avoiding taxes, evading regulations, and winning low-level supply contracts (Zolkafllil, Nazri & Omar, 2021). Our work examines in more detail administrative corruption, such as administrative corruption, kickbacks tax, and bribe tax. The results of this chapter confirm the expectations that administrative corruption and bribe tax sand the wheel of having successful product innovation. Mahagaonkar (2008) suggests that it is important for companies to launch new products and that it is possible to encounter many bureaucratic obstacles in this process.

Our results suggest that the bribe tax is found statistically significant and negative only with product innovation. The kickbacks tax suggests a different theory, if a firm pays an informal gift to secure a contract with the government to rescue its product and process innovation, the effect is seen as greasing the wheel. On the other hand, it affects organizational innovation negatively and sands the wheel. State capture index also sands the wheel of product innovation. According to literature, it is expected that the relationship between time tax and innovations should be positive. Our findings support the view of literature. We find that the correlation between time tax and innovation is positive and statistically significant, moreover, probit models show that spending time on dealing with requirements imposed by government regulations increases the probability of making product, market, and organizational innovations and greases the wheels.

This chapter makes several contributions to the literature on discussions about corruption and innovation. This is one of the first studies which investigates different types of corruption on different types of innovations, to the best knowledge of the time being. In the literature, many studies focus on the country-level data whereas only a few of them investigate the effect of corruption at the firm level. The remainder of the chapter proceeds as follows. Section 2 reviews the literature. Section 3 describes both the data used and presents the empirical methodology. Section 4 discusses the results and finally, the last section concludes.

## **BACKGROUND**

Many earlier studies have intense in the effect of corruption on investments and economic growth (Asiedu & Freeman, 2009; Batra, Kaufmann, & Stone, 2003; Gaviria, 2002; Mauro, 1995; Tanzi & Davoodi, 1998; Wei, 2000;). The existing literature shows interesting findings. According to Méon and Sekkat (2005), corruption is an obstacle to the development and growth of the economy. A precursor work of Mauro (1995) shows a relationship between corruption and investment that will negatively affect growth. Brunetti and Weder (1998), Mo (2001), and Hodge *et al.* (2011) provide similar results. Their findings are called the “sand the wheel hypothesis”.

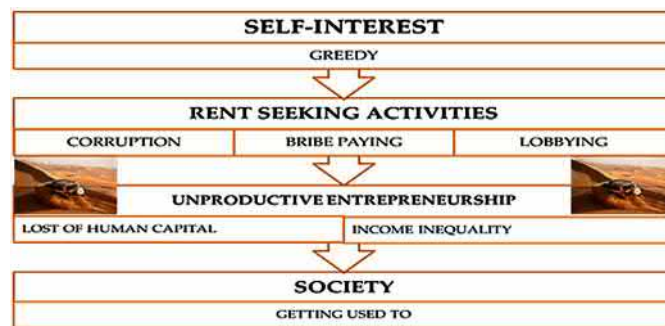
According to Mo (2001), corruption harms economic growth for a group of countries from 1960 to 1985. Likewise, Hodge *et al.* (2011) work with a cross-section of 81 countries between 1984 and 2005. Differently from others, the study investigates the link between corruption and economic growth through different transmission channels. Their findings support the Sand the Wheel hypothesis by the physical capital investment and the political instability channels. Huang and Yuan (2019) study corruption in the United States and they found that corruption has a sanding wheel effect on innovation. Ellis, Smith, and White (2020) suggest similar findings with Huang and Yuan (2019) for United States firms. They find that corruption is a hindering factor in the performance of innovation. One of the new and compre-



hensive studies belongs to Lee, Wang, and Ho (2020). While their results support the Sand the Wheel hypothesis for both emerging and developing countries, they also indicate that the country governance has a crucial role in the innovation of firms that engage in corruption (Alam *et al.*, 2021). For African countries, Hussen and Çokgezen (2020) find that corruption is sanding the wheel of innovation. They suggest that reducing regional corruption to make regional institutions better and more systematic will have a major impact on increasing the effectiveness of innovation in Africa.

*Figure 2. Sand the Wheel Hypothesis*

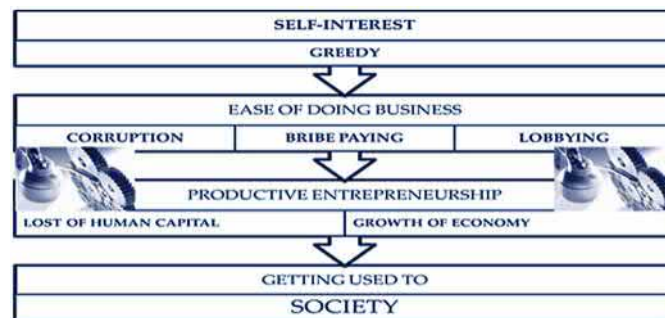
*Source: Authors' creation*



Opposite to the sanding wheel hypothesis, some researchers support the positive relationship between corruption and growth. De Maria *et al.* (2015) define the “greasing wheel hypothesis” as a way of overcoming institutional barriers to government administration. The “Greasing Wheel” hypothesis pioneered by Leff (1964), Huntington (1968), and Leys (1965), this hypothesis suggests that corruption may be beneficial to overcome an existing obstacle, which occurs because of an inefficient bureaucracy during investment processes. The “Greasing Wheel” hypothesis is found as a trouble-saving device.

*Figure 3. Grease the Wheel Hypothesis*

*Source: Authors' creation*



One of the most important drivers of the growth of a country is its innovation rate, for this reason, an inherent curiosity about the interrelationships between corruption and innovation rises among researchers (Nosheen *et al.*, 2016). However, only a few studies have been investigated the link between corruption and innovation (Anokhin & Schulze, 2009; Avnimelech, Zelekha, & Sharabi, 2014; Ayyagari, Demirgüç-Kunt, & Maksimovic, 2010; Ayyagari, Demirgüç-Kunt, & Maksimovic, 2014; Avnimelech & Zelekha, 2015; Botrić & Božić, 2016; Paunov, 2016).

Mahagaonkar (2008), De Waldemar (2012), Krammer (2013), and De Maria *et al.* (2015) examined the relationship between corruption and innovation. Mahagaonkar (2008) works with firm-level data of African countries and does an empirical analysis. He finds that corruption hinders product and organizational innovation, and also that corruption has no effect on process innovation but has a positive effect on marketing innovation. De Waldemar (2012) analyzes the example of India and states that corruption negatively affects new product innovation. Krammer (2013) works with transition economies. Their study examines the impact of bribes on firm innovation while supporting a positive relationship between corruption and innovation. De Maria *et al.* (2015) denote the important role of trade in the relationship between corruption and innovation. They suggest that “if the firm will face higher corruption at home, then it will go abroad to innovate if and only if the rate of corruption in the host country is extremely lower. When the rate of corruption is high in both countries, the outcome is likely to be an overall reduction of the innovation rate”. Moreover, Wen, Zheng, Feng, Chen, and Chang (2020), analyze OECD countries and state that corruption plays an important and fundamental role in determining innovation activities in OECD countries. Heo, Hou, and Park (2021) investigate the greasing wheel hypothesis for investment and innovation for advanced and emerging economies. According to their findings, corruption greases the wheel of the corporate investment in emerging economies and on innovation in advanced economies. On the other hand, their findings suggest that there is no significant effect on investment in advanced economies or on innovation in emerging economies.

## **DATA AND RESEARCH METHODS**

In this chapter, we have used The Business Environment and Enterprise Performance Survey (BEEPS), which is a joint initiative of the World Bank, the European Bank for Reconstruction and Development (EBRD), and the European Investment Bank (EIB). The first advantage of the survey is that both innovation and corruption have been asked with details. This survey provides firm-level data in transition economies of Eastern Europe, Central, and Western Asia. Data allow us to investigate the relationship between different types of innovation and different types of corruption. The selected period includes question-related to corruption, which is the main concern of this chapter, the selected data is the period of 2013-2014. According to the group classification of ISIC Revision 3.1, the sample comprises manufacturing industries (1081 firms), retail (122 firms), and (141 firms) for other services. This special wave of the BEEPS includes an Innovation Module, which covers a range of innovation such as product, process, organizational, and marketing innovation. In previous waves of the BEEPS questions related to state capture corruption have not been asked. We used a probit model in our analyses. Our dependent variables are structured as a binary variable. If the enterprise answers “yes” to the innovation questions, for example, “During the last three years, has this establishment introduced new or significantly improved products or services? “, then the firm is doing production innovation. Additionally, the data has been cleaned from non-responses and responses such as “Do Not Know” and “Does Not Apply”. The same

approaches are done for process innovation, market innovation, and organizational innovation. The corruption variables are produced by using principal component analysis.

In the case of binary variables, there are two possible outcomes of dependent variables. These outcomes are known as “0” and “1” where these numbers refer to results of an action or a situation etc. Most of the time binary variables indicate whether an individual is a participant or a non-participant. Examples of binary variables could be whether being a large firm or not, whether the firm is belonging to a precise sector or not. The binary outcome  $y$  depends on the several independent explanatory variables and independent variables could be both consisted of binary variables or continuous variables.

When  $y$  takes the value of “0” or “1”, the conditional expectation of  $y$  is.

$$E(y|X) = P(y = 1|X) = F(X'\beta)$$

Where  $X'\beta$  is an index function and, where  $X$  is a  $K \times 1$  regressor vector and  $\beta$  is a vector of unknown parameters. The Logit and Probit Models are used for the estimation of the Binary Models. The distribution of binary outcome is ‘S’ shaped where both Logit and probit models more or less share the same ‘S’ shape. The difference between the two of the Model is that the Logit model gives more weight to the tails of the distribution. The bounds of the two distributions are at the bottom “0” and the top “1”. In both models, the specification of the dependent  $y$  is done as a continuous latent variable. The latent variable determines the participation of the individuals on the binary outcomes. One can imagine that  $y^*$  (latent variable) is an individual’s propensity to participate. As there is a two outcome “0” and “1”, the latent variable should offer two outcomes as well; non-participation and participation if  $y^*$  takes negative values then the observed outcome is “0” if  $y^*$  takes positive values then the observed outcome is “1” (Wooldridge, 2010). The dependent variable and latent variable relation can be expressed

$$\begin{aligned} y &= 1 && \text{if } y^* > 0 \\ &= 0 && \text{otherwise} \end{aligned}$$

Where

$$y^* = X'\beta + \varepsilon$$

Then

$$P(y = 1 | X) = P(y^* > 0 | X) = P(\varepsilon > -X'\beta) = F(X'\beta)$$

If the standard error terms of the linear regression model give a standard normal distribution, then it gives a Probit Model. If the standard error terms of the linear regression model give a standard logistic distribution, then it gives a Logit Model. Both models are typically estimated by the method of maximum likelihood estimation. Nevertheless, the results of the two models do not show any significant differences in applications. The log-likelihood function will be

$$LogL = \sum_i \left\{ (1 - y) \log(1 - F(X'\beta)) + y \log(F(X'\beta)) \right\}$$

The Maximum likelihood estimator of  $\beta$  maximizes this log-likelihood function (Wooldridge, 2010). Here the X vector composes the following control variables. In addition to our control variables, we added corruption variables one by one into the models. To be able to count the effect of possible heteroscedasticity heteroskedastic probit model is also used for testing all models given in the chapter. Also, the LM test has been used to test the normality after the probit model.

In this chapter, we also present the variables' descriptions and summary statistics. Table 1 shows the summary statistics of innovation variables. Around 12% -15% of firms in our sample are innovators who introduced or developed new products or services. Turkish companies are more likely to make market innovation rather than other types of innovations. Table 1 also shows the firm characteristics of Turkish companies. Firms, whose ages are above 10 years, constitute 75% of the overall sample. A top manager of a firm's average experience, which is above 10 years, is 83% of the whole sample. On the other hand, on average, 11.28% of permanent full-time employees have a university degree. A large part of the sample is comprised of small-sized firms. Small-sized firms make up 40% of the whole sample, medium and large-sized firms constitute 35% and 23% of the sample. In terms of the foreign relations of firms, two variables are concerned, such as ownership status and exporters' status. 19% of the sample is composed of foreign firms, and 37% of the sample is direct exporters. The percentage of secured or attempted to secure a government contract for all firms responding is 16 points. Access to Finance is perceived least often as an obstacle to operations of establishments in Turkey. The percentage of firms that have an internationally recognized quality certification is 46 points. Additionally, Table 1 reports corruption variables and their summary statistics. Turkish Companies find corruption as a minor obstacle to operating a business. Its mean on a 1-5 scale (with 1 indicating no obstacle, and 5 indicating "very severe" obstacle) is only 0.88. In a typical week, senior managers' time spent on dealing with regulation (the "time tax") is an average of about 22%. The average annual sales spent on bribe payments (the "bribe tax") is almost near zero with a percentage of 0.49. When we look at kickbacks tax, it is seen that firms are paying %1.88 of the contract value to secure a government contract.

In this study, we follow the definition of corruption which is done by Knack and Kisunko (2011) that corruption in the public sector refers to illegal or unauthorized actions by public officials who abuse their positions of authority to gain personal gain. According to them, corruption is a symptom of bad governance.

We are going to investigate corruption under three groups: Administrative Burden, Administrative Corruption, and State Capture.

***"Administrative (regulatory) Burden** refers to the administrative costs incurred by firms in dealing with government regulation of business. Use of the term "burden" should not be taken to imply that the optimal number of regulations is zero but reflects instead that fact that costs of complying with regulations (in senior managers' time, fees, and bribes) remain unnecessarily high for transitional countries overall, for example in comparison with OECD countries." p.3. (Knack & Kisunko, 2011).*

*Table 1. Variables' Description and Summary Statistics*

Type	Variable	Description	Mean	Std. Dev.	Min.	Max.	N
Dependent Variables	Product Innovation	=1 if the firm has introduced new or significantly improved products or Services=0 otherwise	0.13	0.33	0	1	1302
	Process Innovation	=1 if the firm has introduced any new or significantly improved methods for the production or supply of products or services, =0 otherwise	0.12	0.32	0	1	1302
	Marketing Innovation	=1 if the firm has introduced new or significantly improved marketing methods, =0 otherwise	0.15	0.36	0	1	1301
	Organizational Innovation	=1 if the firm has introduced any new or significantly improved organizational or management practices or structures, =0 otherwise	0.14	0.35	0	1	1299
Explanatory Variables for all equations	Financial Obstacle	=1 if the firm perceives Financial Barrier as a "Major obstacle" or "Very severe obstacle", =0 otherwise	0.73	1.10	0	4	1302
	Firm Age	=1 if the age of the firm is more than 10 years, =0 otherwise	0.74	0.44	0	1	1253
	Size	Small: =1 if 5- 19 employees, =0 otherwise	0.40	0.49	0	1	1326
		Medium: =1 if 20-99 employees, =0 otherwise	0.35	0.48	0	1	1326
		Large: =1 if 100 and over employees, =0 otherwise	0.23	0.42	0	1	1326
	Research	=1 if the firm has spent on R&D, =0 otherwise	0.15	0.36	0	1	1291
	Managerial Experience	=1 if the manager's experience for more than 10 years, =0 otherwise	0.93	0.37	0	1	1278
	Educated Workforce	=percent of the establishment's permanent full-time employees employed had a university degree	11.28	15.85	0	100	1246
	Government Contract	=1 if the firm has attempted to secure or secured a government contract, =0 otherwise	0.16	0.37	0	1	1300
	Export	=1 if the share of direct exports is positive, =0 otherwise	0.37	0.48	0	1	1303
	Certification	=1 if the firm has an internationally-recognized quality certification =0 otherwise	0.46	0.50	0	1	1275

*continues on following page*

*Table 1. Continued*

Type	Variable	Description	Mean	Std. Dev.	Min.	Max.	N
Corruption Variables	Time Tax	% of senior management's time spent on dealing with regulation	21.71	28.10	0	100	1207
	Kick Backs Tax	% of contract value typically paid to secure a government contract	1.24	7.87	0	100	185
	Bribe Tax	% of total annual sales paid as informal payment/gift	2.49	4.52	0	100	1278
	Administrative Obstacle	Factor Variable	-0.15	1.47	-1.53	5.27	1326
	Administrative Corruption Index	Factor Variable	-0.30	1.08	-1.04	2.94	1326
	State Capture Index	Factor Variable	-0.48	0.91	-1.35	2.35	1326
	Corruption Obstacle	(0, 1, 2, 3, 4) No obstacle, Minor obstacle, Moderate obstacle, Major obstacle, Very severe obstacle	0.88	1.26	0	4	1297

Source: Authors' creation

To measure the effect of Administrative Burden we use Time tax; the percentage of total senior management's time was spent on dealing with requirements imposed by government regulations. We also investigate the perception of corruption by the firms. Whether they find administrative activities as a hindrance factor for their innovation activities or not. A factor variable created for this purpose, which includes taxes, courts, labor regulations, business licensing and permits, tax administrations, and land access.

Our hypothesis can be written as

**Hypothesis One:** Corruption increases a firm's innovativeness in the presence of administrative burdens.

*Table 2. Polychoric Correlation Matrix for Administrative Obstacle Index*

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
(1) Customs and trade regulations - an obstacle to current operations	1						
(2) Access to land - obstacle to current operations	0.29	1					
(3) Tax administration - obstacle to current operations	0.33	0.26	1				
(4) Business licensing and permits - obstacle to current operations	0.29	0.32	0.33	1			
(5) Corruption - obstacle to current operations	0.31	0.32	0.41	0.41	1		
(6) Courts - obstacle to current operations	0.33	0.37	0.45	0.41	0.48	1	
(7) Labor regulations - obstacle to current operations	0.30	0.33	0.39	0.37	0.38	0.45	1

Source: Authors' creation

*Table 3. Principal Component Analysis on Administrative Obstacle Index*

PC	Eigenvalue	Variance Explained	Source	Cronbach's Alpha	Factor Loadings
1	3.19	0.45	Customs and trade regulations - obstacle to current operations	0.68	0.59
2	0.75	0.56	Access to land - obstacle to current operations	0.68	0.59
3	0.73	0.67	Tax administration - obstacle to current operations	0.65	0.68
4	0.65	0.76	Business licensing and permits - obstacle to current operations	0.67	0.66
5	0.60	0.85	Corruption - obstacle to current operations	0.64	0.71
6	0.55	0.92	Courts - obstacle to current operations	0.65	0.76
7	0.49	1.00	Labor regulations - obstacle to current operations	0.66	0.69

Source: Authors' creation

*“Administrative corruption refers to the intentional imposition of distortions in the prescribed implementation of existing laws, rules, and regulations to provide advantages to either state or non-state actors as a result of the illicit and non-transparent provision of private gains to public officials” p.3. (Pradhan, 2000).*

According to this definition, the Administrative Corruption Index, Bribe Tax, and Kickbacks Tax are used for estimations. Bribe tax is the percentage of total annual sales used for buying gifts or making informal payments to public officials to “get things done” concerning customs, taxes, licenses, regulations, services, etc. Kickbacks Tax is the percentage of the contract value, which establishments do informal payments or giving gifts to secure the contract when they do business with the government. We also investigate the Administrative Corruption Index. A factor variable created for this purpose, which measures How often does a business have to pay some irregular “additional payments or gifts” to get things done concerning customs, taxes, licenses, regulations and to deal with customs/imports, to deal with courts and to deal with taxes and tax collection.

Our hypothesis can be written as.

**Hypothesis Two:** Corruption increases a firm’s innovativeness in the presence of administrative corruption.

*Table 4. Polychoric Correlation Matrix for Administrative Corruption*

	(1)	(2)	(3)	(4)
(1) Frequency of informal payments/gifts to get things done	1			
(2) Frequency of unofficial payments/gifts to deal with customs/imports	0.62	1		
(3) Frequency of unofficial payments/gifts to deal with courts	0.63	0.85	1	
(4) Frequency of unofficial payments/gifts to deal with taxes and tax collect	0.70	0.80	0.86	1

Source: Authors' creation

*Table 5. Principal Component Analysis on Administrative Corruption Index*

PC	Eigenvalue	Variance Explained	Source	Cronbach's Alpha	Factor Loadings
1	3.25	0.81	Frequency of informal payments/gifts to get things done	0.87	0.81
2	0.44	0.92	Frequency of unofficial payments/gifts to deal with customs/imports	0.79	0.91
3	0.18	0.97	Frequency of unofficial payments/gifts to deal with courts	0.76	0.93
4	0.11	1.00	Frequency of unofficial payments/gifts to deal with taxes and tax collect	0.75	0.93

Source: Authors' creation

***“State Capture refers to the actions of individuals, groups, or firms both in the public and private sectors to influence the formation of laws, regulations, decrees, and other government policies to their advantage as a result of the illicit and non-transparent provision of private benefits to public officials” p.3. (Pradhan, 2000).***

A factor variable created for measuring the state capture, which includes unofficial payments/gifts, private payments, or other benefits to public officials to gain advantages in the drafting of laws, decrees, regulations, and other binding government decisions.

Our hypothesis can be written as;

**Hypothesis Three:** Corruption increases a firm's innovativeness in the presence of state capture corruption.

*Table 6. Polychoric Correlation Matrix for State Capture Corruption*

	(1)	(2)	(3)
(1) Private payments/gifts/other benefits to Parliamentarians	1		
(2) Private payments/gifts/other benefits to Government officials	0.94	1	
(3) Private payments/gifts/other benefits to local/regional officials	0.91	0.93	1

Source: Authors' creation

*Table 7. Principal Component Analysis on State Capture Corruption Index*

PC	Eigenvalue	Variance Explained	Source	Cronbach's Alpha	Factor Loadings
1	2.86	0.95	Private payments/gifts/other benefits to Parliamentarians	0.92	0.97
2	0.08	0.98	Private payments/gifts/other benefits to Government officials	0.91	0.98
3	0.05	1.00	Private payments/gifts/other benefits to local/regional officials	0.93	0.97

Source: Authors' creation



Table 8 represents the pairwise correlation matrix of the main variables. The observed associations between different types of innovation are statistically significant and high, which can be seen from Panel A of Table 8. We prefer to run four different regressions using four different dependent variables. Due to the high and statistically significant correlation between the various measures of corruption indexes, we include them in regressions one at a time as seen from Table 8 Panel C.

*Table 8. Correlation Tables*

A. Pairwise Tetrachoric Correlation Matrix of Innovation							
	Product Innovation	Process Innovation	Organizational Innovation	Market Innovation			
Product Innovation	1						
Process Innovation	0.7707*	1					
Organizational Innovation	0.6345*	0.7992*	1				
Market Innovation	0.6593*	0.7677*	0.8209*	1			
B. Pairwise Biserial Correlation Matrix Between the Main Variables of Interest.							
	Product Innovation	Process Innovation	Organizational Innovation	Market Innovation			
Time Tax	0.0539*	0.0226	0.0656*	0.0531*			
Kickbacks Tax	0.115	0.1357*	-0.0864	0.0695			
Bribe Tax	-0.0358	-0.0205	-0.0295	-0.0122			
Administrative Obstacle	0.1047*	0.0935*	0.1491*	0.1671*			
Administrative Corruption	-0.0451	-0.0534	-0.0367	-0.0491			
State Capture Index	-0.0324	0.0236	0.0071	0.017			
Corruption Obstacle	0.0870*	0.0724*	0.1298*	0.1226*			
C. Pairwise Correlation Matrix of Corruption Variables							
	ACI	SCI	TT	BT	KBT	AOI	COROBS
Administrative Corruption	1						
State Capture Index	0.5449*	1					
Time Tax	-0.1654*	-0.0458	1				
Bribe Tax	0.1222*	0.1062*	0.1177*	1			
Kickbacks Tax	0.1486*	0.0917	0.0315	0.2086*	1		
Administrative Obstacle	0.2575*	0.2052*	-0.1071*	-0.1071*	-0.1490*	1	
Corruption Obstacle	0.1694*	0.1557*	0.0897*	-0.0531	-0.1235	0.7595*	1

Source: Authors' creation

## **SOLUTIONS AND RECOMMENDATIONS**

Tables 9,10, and 11 present the average marginal effects after probit models. Besides the probit model, the heteroskedastic probit model is used for all models. At the end of each table, we present the Likelihood ratio test of ln sigma square to test the heteroscedasticity. Our results suggest that there is no

heteroscedasticity. Only one model gives a different result and the hetprob results are significant, but the overall significance has been tested by the Wald test and results suggest that the heteroscedastic model should be given which is seen from column 8 of Table 10. Table 9 shows the results of the administrative burden of the regulations. We used three variables to explain the administrative burden of regulations. The first two variables are administrative and corruption obstacles, which represent the firm's perception of corruption. The perception of corruption as an obstacle increases the likelihood of successful market and organizational innovation by 1.4 and 1.5 percentages. It is also evidenced that correlation between the perception of corruption as an obstacle and innovation variables are statistically significant and positive. There is an interesting result, which supports the grease the wheel hypothesis that the more firms perceived corruption as an obstacle the more they innovate. Besides perceiving corruption as an obstacle, we also investigate the perception of administrative obstacles. We found that the perception of the administrative obstacle increases the probability of market and organizational innovation on average by 1.7 percentage points. Another important variable to investigate the effect of administrative burden is defined as Senior management's time spent on dealing with regulations (time tax). According to the literature it is expected that the relationship between Time Tax and innovations is positive. Our findings support this view, it is found that the correlation between Time Tax and innovation is positive and statistically significant, in addition to correlations, probit models show that spending time on dealing with requirements imposed by government regulations increases the probability of making a product, market, and organizational innovations. Again, it is seen that the effect of the administrative burden supports the grease the wheel hypothesis. Control variables are also checked in the models. Contract with the government is seen as statistically significant for all types of innovation. Having an internationally recognized certification is also an important control variable for the performance of the innovation. These performances depend on research and development investments.

Table 10 shows the effect of Administrative corruption variables on innovation. Our work examines in more detail administrative corruption, such as administrative corruption, kickbacks tax, and bribe tax. These results confirm the expectations that administrative corruption sands the wheel of having successful product innovation. Bribe tax was not found statistically significant for innovation types. The kickbacks tax suggests a different theory, if a firm pays an informal gift to secure a contract with the government, the expectation changes from sand to grease the wheel hypothesis. Our results support our expectations that paying Kickbacks tax increases the likelihood of successful product and process innovations, whereas it decreases the probability of successful organizational innovation. Administrative Corruption Index includes the following types of corruption as referred to earlier in the chapter; Frequency of informal payments/gifts to get things done, Frequency of unofficial payments/gifts to deal with customs/imports, Frequency of unofficial payments/gifts to deal with courts, Frequency of unofficial payments/gifts to deal with taxes and tax collections. Results show that these corruption types are sands the wheel of the innovation performance of the firms which means that there is no meaning to spend money to get things done for a firm, instead, this money can be used for research and development.

Lastly, State Capture Index includes Private payments/gifts/other benefits to Parliamentarians, Private payments/gifts/other benefits to Government officials, Private payments/gifts/other benefits to local/regional officials. In Table 11, it is seen that state capture corruption affects the likelihood of product innovation. State capture index sands the wheel of product innovation.

Table 9. The Effect of Administrative Burden on Innovation

	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation
VARIABLES	COROB5	COROB5	COROB5	COROB5	AOI	AOI	AOI	AOI	TT	TT	TT	TT
AGE	1 -0.022 (0.021)	2 -0.003 (0.023)	3 -0.010 (0.024)	4 0.000 (0.024)	5 -0.017 (0.022)	6 -0.002 (0.023)	7 -0.010 (0.024)	8 -0.003 (0.024)	9 -0.009 (0.023)	10 -0.001 (0.024)	11 -0.010 (0.025)	12 -0.006 (0.025)
RDA	0.158*** (0.019)	0.164*** (0.020)	0.151*** (0.021)	0.180*** (0.021)	0.157*** (0.019)	0.163*** (0.020)	0.150*** (0.021)	0.180*** (0.020)	0.147*** (0.020)	0.159*** (0.020)	0.141*** (0.021)	0.172*** (0.020)
EXPORT	0.007 (0.020)	0.029 (0.021)	0.003 (0.021)	0.009 (0.021)	0.003 (0.020)	0.030 (0.021)	0.003 (0.022)	0.008 (0.021)	0.005 (0.020)	0.028 (0.022)	0.005 (0.022)	0.016 (0.021)
EDWF	0.001 (0.001)	0.001 (0.001)	0.001* (0.001)	0.001** (0.001)	0.001 (0.001)	0.001 (0.001)	0.001* (0.001)	0.001** (0.001)	0.001 (0.000)	0.001 (0.001)	0.001 (0.001)	0.001** (0.001)
MANEXP	0.004 (0.027)	0.024 (0.027)	0.000 (0.029)	-0.014 (0.029)	-0.004 (0.027)	0.025 (0.027)	0.003 (0.029)	-0.015 (0.029)	-0.000 (0.028)	0.014 (0.028)	-0.003 (0.030)	-0.022 (0.030)
CGOV	0.044* (0.023)	0.048** (0.024)	0.055** (0.024)	0.076*** (0.024)	0.050** (0.023)	0.048** (0.024)	0.057** (0.023)	0.075*** (0.023)	0.045* (0.023)	0.051** (0.024)	0.069*** (0.023)	0.077*** (0.023)
PFIN	0.022*** (0.008)	0.014 (0.009)	0.015 (0.009)	0.012 (0.009)	0.022** (0.010)	0.012 (0.011)	0.010 (0.011)	0.004 (0.010)	0.021*** (0.008)	0.018** (0.009)	0.020** (0.009)	0.017* (0.009)
PLARG	0.009 (0.022)	0.023 (0.023)	0.036 (0.022)	0.047** (0.023)	0.010 (0.022)	0.023 (0.023)	0.031 (0.023)	0.043* (0.023)	0.009 (0.022)	0.030 (0.022)	0.045** (0.022)	0.060*** (0.022)
CERT	0.032 (0.020)	0.040* (0.022)	0.089*** (0.021)	0.066*** (0.022)	0.035* (0.020)	0.043** (0.022)	0.083*** (0.021)	0.063*** (0.022)	0.035* (0.020)	0.048** (0.022)	0.095*** (0.021)	0.069*** (0.022)
COROB5	0.006 (0.008)	0.010 (0.008)	0.014* (0.008)	0.015* (0.008)								
AOII					0.002 (0.008)	0.007 (0.008)	0.017** (0.009)	0.017** (0.008)				
TT									0.000 (0.000)	0.001* (0.000)	0.001** (0.000)	0.001** (0.000)
OBSERVATIONS	1.055	1.054	1.057	1.056	1.067	1.066	1.068	1.068	1.007	1.007	1.008	1.009
Pseudo R2	0.1617	0.1553	0.1719	0.1952	0.1571	0.1425	0.1849	0.1911	0.1505	0.1640	0.1826	0.2078
LR chi2	121.36***	124.87**	147.58***	174.10	106.36***	104.72***	140.22***	151.60***	105.26***	125.67***	146.25***	172.16***

continues on following page

Table 1. Continued

	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation
Heteroscedasticity (hetprobit)	0.69	0.95	2.57	2.54	0.93	0.40	2.06	4.11	0.96	5.33	4.05	3.56
Likelihood-ratio test of Insignia2=0												
LM test for normality	1.22 [0.54]	6.56 [0.03]	1.14 [0.56]	3.04 [0.21]	3.80 [0.14]	8.85 [0.01]	0.54 [0.76]	1.23 [0.53]	0.18 [0.90]	2.56 [0.27]	0.91 [0.63]	0.88 [0.64]

Standard Errors in Parentheses \*\*\* P<0.01, \*\* P<0.05, \* P<0.1

Basic Categories are educated workforce and managerial experience.

LR test of Insignia2 tests the whole model with heteroscedasticity against the whole model without heteroscedasticity.

Source: Authors' creation

Table 10. The Effect of Administrative Corruption on Innovation

	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation	Process Innovation	Product Innovation	Organizational Innovation	Market + Innovation	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation
VARIABLES	1	2	3	4	5	6	7	8	9	10	11	12
AGE	ACI	ACI	ACI	ACI	KBT	KBT	KBT	KBT	BT	BT	BT	BT
	-0.017	-0.000	-0.008	0.000	0.041	0.005	0.019	0.020	-0.019	-0.004	-0.009	-0.006
	(0.022)	(0.023)	(0.024)	(0.024)	(0.090)	(0.087)	(0.098)	(0.088)	(0.022)	(0.023)	(0.024)	(0.024)
RDA	0.157***	0.163***	0.151***	0.181***	0.245***	0.279***	0.017	0.185*	0.159***	0.167***	0.162***	0.182***
	(0.019)	(0.020)	(0.021)	(0.020)	(0.058)	(0.061)	(0.079)	(0.082)	(0.020)	(0.020)	(0.022)	(0.021)
EXPORT	0.004	0.032	0.009	0.014	-0.013	0.102	-0.046	0.162*	0.001	0.025	-0.000	0.013
	(0.020)	(0.021)	(0.021)	(0.021)	(0.058)	(0.068)	(0.068)	(0.063)	(0.020)	(0.021)	(0.021)	(0.021)
EDWF	0.001	0.001	0.001	0.001**	-0.000	0.002	0.002	-0.013***	0.001	0.000	0.001	0.001**
	(0.000)	(0.001)	(0.001)	(0.001)	(0.002)	(0.002)	(0.002)	(0.006)	(0.001)	(0.001)	(0.001)	(0.001)
MANEXP	-0.006	0.021	-0.002	-0.022	0.126	0.029	0.158	0.000	-0.006	0.033	0.001	-0.015
	(0.027)	(0.027)	(0.029)	(0.029)	(0.097)	(0.086)	(0.118)	(0.002)	(0.027)	(0.027)	(0.030)	(0.029)
CGOV	0.051**	0.051**	0.066***	0.083***					0.055**	0.057**	0.069***	0.085***
	(0.023)	(0.024)	(0.023)	(0.023)					(0.023)	(0.024)	(0.024)	(0.023)
PFIN	0.025***	0.018**	0.023***	0.019**	0.041*	-0.019	0.044*	0.056***	0.024***	0.014	0.020**	0.012
	(0.007)	(0.009)	(0.008)	(0.008)	(0.022)	(0.028)	(0.026)	(0.021)	(0.008)	(0.009)	(0.008)	(0.008)

continues on following page

Table 1. Continued

	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation	Process Innovation	Product Innovation	Organisational Innovation	Market + Innovation	Process Innovation	Product Innovation	Organisational Innovation	Market Innovation
PLARG	0.013 (0.021)	0.031 (0.022)	0.047** (0.022)	0.058*** (0.022)	-0.064 (0.065)	0.043 (0.071)	0.035 (0.069)	0.102 (0.065)	0.006 (0.022)	0.033 (0.022)	0.048*** (0.022)	0.059*** (0.022)
CERT	0.037* (0.020)	0.045** (0.021)	0.088*** (0.021)	0.067*** (0.021)	0.033 (0.072)	-0.028 (0.080)	0.314*** (0.089)	0.033 (0.067)	0.037* (0.020)	0.055** (0.022)	0.092*** (0.021)	0.069*** (0.022)
AC11	-0.018** (0.008)	-0.012 (0.009)	-0.014* (0.008)	-0.020*** (0.009)								
KBT					0.005** (0.002)	0.005* (0.002)	-0.061*** (0.021)	0.003 (0.003)				
BT									-0.005 (0.005)	-0.022*** (0.007)	-0.010 (0.007)	-0.001 (0.002)
OBSERVATIONS	1.067	1.066	1.068	1.068	155	155	154	155	1.035	1.035	1.036	1.036
Pseudo R2	0.1688	0.1578	0.1698	0.2139	0.1623	0.1764	0.1185	0.1125	0.1621	0.1717	0.1788	0.1969
LR chi2	116.00***	117.31***	134.04***	172.87***	26.28***	30.90***	22.28***	22.70***	118.07***	134.32***	150.93***	170.02***
Heteroscedasticity (hetprobit) Likelihood-ratio test of Insigma2=0	2.64	1.59	4.19	3.97	5.30	2.16	1.21	7.45**	1.71	0.64	3.67	1.93
LM test for normality	3.58 [0.16]	0.75 [0.68]	0.69 [0.70]	1.71 [0.42]	0.01 [0.99]	1.98 [0.37]	1.53 [0.46]	1.78 [0.40]	0.63 [0.72]	7.33 [0.02]	0.28 [0.86]	1.47 [0.47]

Standard Errors in Parentheses \*\*\* P<0.01, \*\* P<0.05, \* P<0.1. Basic Categories are educated workforce and managerial experience. LR test of Insigma2 tests the whole model with heteroscedasticity against the whole model without heteroscedasticity. Results are estimated for the Heteroskedastic Probit model.

Source: Authors' creation

*Table 11. The Effect of State Capture on Innovation*

	Process Innovation	Product Innovation	Organizational Innovation	Market Innovation
VARIABLES	SCI	SCI	SCI	SCI
AGE	-0.017 (0.022)	0.000 (0.023)	-0.008 (0.024)	-0.000 (0.024)
RDA	0.157*** (0.019)	0.165*** (0.020)	0.151*** (0.021)	0.183*** (0.021)
EXPORT	0.004 (0.020)	0.029 (0.021)	0.009 (0.021)	0.013 (0.021)
EDWF	0.001 (0.001)	0.001 (0.001)	0.001* (0.001)	0.001** (0.001)
MANEXP	-0.004 (0.027)	0.021 (0.027)	-0.001 (0.029)	-0.020 (0.029)
CGOV	0.051** (0.023)	0.050** (0.024)	0.065*** (0.023)	0.081*** (0.023)
PFIN	0.023*** (0.007)	0.020** (0.009)	0.022** (0.008)	0.017** (0.008)
PLARG	0.011 (0.021)	0.032 (0.022)	0.045** (0.022)	0.057*** (0.022)
CERT	0.035* (0.020)	0.045** (0.022)	0.086*** (0.021)	0.066*** (0.022)
SCI1	0.004 (0.009)	-0.018* (0.011)	0.000 (0.010)	-0.005 (0.010)
OBSERVATIONS	1,067	1,066	1,068	1,068
Pseudo R2	0.1746	0.1721	0.1870	0.2052
LR chi2	106.21***	116.90***	128.58***	151.37***
Heteroscedasticity (hetprobit) Likelihood-ratio test of Insigma2=0	0.06 [0.97]	4.47 [0.10]	1.97 [0.37]	1.05 [0.59]
LM test for normality	2.68 [0.26]	2.75 [0.25]	1.05 [0.58]	0.73 [0.69]

Standard Errors in Parentheses \*\*\* P<0.01, \*\* P<0.05, \* P<0.1

Basic Categories are educated workforce and managerial experience.

LR test of Insigma2 tests the whole model with heteroscedasticity against the whole model without heteroscedasticity.

Source: Authors' creation

## FUTURE RESEARCH DIRECTIONS

As noted by many researchers in this chapter, two important issues are Innovation and Corruption, which are still fairly new research areas. With the COVID-19 outbreak, the challenges faced by businesses have increased more than ever today. As a result, it is possible to observe a significant increase in companies' demand for state support. It should therefore be considered that there may be an increased intention to

engage in corrupt activities in this process. Some companies that want to get a chance to gain priority for government support may participate in illegal activities such as bribery or other corrupt activities.

On the other hand, with the current pandemic, it is clear that the need for technology and innovation is increasing, so some firms are probably facing many developments across all innovation channels, such as marketing, organization, product and process. Therefore, companies should divert both financial and time resources to innovation rather than to illegal activities or financial crimes. This will be more effective for firms in the long run. In this context, it will be useful to examine the relationship between innovation and corruption during the COVID-19 outbreak as further research.

## **CONCLUSION**

A developing system of markets and sustainable growth is important for surviving in global markets. Enterprises are changed their direction for innovation so sharply. There are lots of steps to climb to end up with successful innovation. Regardless of the types of innovation, an entrepreneur may face a decision to pay bribe voluntarily to get things done or may have to pay bribe because of a bad business environment, which may result in losing time and money for nothing beneficial. The chapter reviews work which draws a link between different kind of innovation activities and different types of corruption. There exists a vast literature about the relationship between corruption and growth. On the other hand, there is a very least interest in the relationship between innovation and corruption. Some of the authors are examined the micro-level effect of corruption. They especially work on firm growth and the effect of corruption on firm growth. The existing literature shows interesting findings. Corruption is an obstacle to development and growth, which refers to the “sand the wheel hypothesis”. Opposite to the sand hypothesis, some of the researchers found a positive relationship between corruption and growth, which is defined as the “grease the wheel hypothesis” as a way to overcome institutional hurdles of the government administration. The “Grease the wheels” hypothesis pioneered by some authors. This hypothesis suggests that corruption may be beneficial to overcome an existing obstacle, which occurs because of an inefficient bureaucracy during investment processes. The “grease the wheels” hypothesis is found as a trouble-saving device.

This chapter differs from the above literature because it introduces different levels of corruption types, such as state capture and administrative corruption. And it is also very important to mention that determinants of innovation have not been determined for Turkish enterprises before by using econometric methods and the relationship of innovation types never analyzed in previous works. Corruption has vast literature but when the literature combined with innovation only a few studies can be found. The Business Environment and Enterprise Performance Survey (BEEPS), which is conducted by the World Bank, are used to examine how the business perceives informal payments. BEEPS have 1344 respondent from Turkey in 2013-2014. This chapter uses a probit model to identify whether there is sand the wheel or grease the wheel relationship. In general, it is found that corruption Sands the Wheel of Innovation in Turkey. This chapter documents that corruption has effects on firms’ innovative activities. The state capture index supports the evidence of sands the wheel hypothesis on product innovation. These results raise important issues around the corruption and innovation relationship. Our findings provide strong pieces of evidence that state capture corruption lowers the efforts of the enterprises to innovate more. While this is a form of political corruption policymakers especially the leaders of the political parties’ as well as ministers should fight strongly against corruption. Corruption’s effects damage product in-

novation, whether it is petty corruption or grand corruption. For this reason, not only policymakers but also enterprises have to show efforts to fight. Corruption has two corners bribe payers and bribe-takers. It is important to control both sides carefully. It is suggested according to the result of the chapter that any financial resources should be transferred to the innovation investments rather than corrupt activities.

An interesting result is that if the firm has a contract with the government “the more the company pays informal payments or gifts, the more the company innovates” when there is no contract this “advantage” (for some thoughts) disappears. The more the company pays informal payments or gifts to get things done the less they innovate. The “grease the wheels” hypothesis is found as a trouble-saving device when enterprises are ready to give their time to save their business. It seems that the most problematic regulations are making productive people using their time for less productive activities. This is a great obstacle to the development of the country.

We believe that any firms that are willing to enter the market in Turkey can benefit from the result of this chapter. They also can see what they should expect in terms of corrupt activities. Whether Turkey’s current situation is not on the red list but for the future targets of the country it is one more time seen that the fight against financial crime especially, corruption is important. And this should be done especially on each level of government from top to bottom. It is suggested that if the government officials are educated well and the regulations are made easy, simple, and basic for enterprises there will be a good start to fight with any kind of corruption. Transparency also especially important and must be supported with Freedom of thought and expression and Free Journalism to fight against corrupt people. This is particularly important to support innovative firms to enter markets for the sustainable growth of Turkey. The business environment must be protected from corrupt businesses and government officials.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.



## REFERENCES

- Alam, M. D., Tabash, M. I., Hassan, M. F., Hossain, N., & Javed, A. (2021). *Shariah Governance Systems of Islamic Banks in Bangladesh: A Comparison with Global Governance Practices*. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Anokhin, S., & Schulze, W. S. (2009). Entrepreneurship, innovation, and corruption. *Journal of Business Venturing*, 24(5), 465–476. doi:10.1016/j.jbusvent.2008.06.001
- Asiedu, E., & Freeman, J. (2009). The Effect of Corruption on Investment Growth: Evidence from Firms in Latin America, Sub-Saharan Africa, and Transition Countries. *Review of Development Economics*, 13(2), 200–214. doi:10.1111/j.1467-9361.2009.00507.x
- Avnimelech, G., & Zelekha, Y. (2015). The Impact of Corruption on Entrepreneurship. In R. Wolf & T. Issa (Eds.), *International Business Ethics and Growth Opportunities* (pp. 981–993). IGI Global. doi:10.4018/978-1-4666-7419-6.ch013
- Avnimelech, G., Zelekha, Y., & Sharabi, E. (2014). The effect of corruption on entrepreneurship in developed vs non-developed countries. *International Journal of Entrepreneurial Behaviour & Research*, 20(3), 237–262. doi:10.1108/IJEBR-10-2012-0121
- Ayyagari, M., Demirgüç-Kunt, A., & Maksimovic, V. (2010). *Are innovating firms victims or perpetrators? Tax evasion, bribe payments, and the role of external finance in developing countries* (World Bank Policy Research Working Paper No 5389). The World Bank.
- Ayyagari, M., Demirgüç-Kunt, A., & Maksimovic, V. (2014). Bribe payments and innovation in developing countries: Are innovating firms disproportionately affected? *Journal of Financial and Quantitative Analysis*, 49(1), 51–75. doi:10.1017/S002210901400026X
- Batra, G., Kaufmann, D., & Stone, A. H. (2003). *Investment climate around the world: Voices of the firms from the World Business Environment Survey*. The World Bank. doi:10.1596/0-8213-5390-X
- Baumol, W. J. (1990). Entrepreneurship: Productive, Unproductive, and Destructive. *Journal of Political Economy*, 98(5, Part 1), 893–921. doi:10.1086/261712
- Baumol, W. J. (1993). *Entrepreneurship, Management, and the Structure of Payoffs*. MIT Press.
- BBC. (2016). *Ukraine Prime Minister Arseniy Yatsenyuk to resign*. BBC News. Retrieved from <https://www.bbc.com/news/world-europe-36010511>
- Botrić, V., & Božić, L. (2016). Innovators' vs Non-innovators' perceptions of corruption in European post-transition economies. *International Journal of Business and Economic Sciences Applied Research*, 8(3), 47–58.
- Brunetti, A., & Weder, B. (1998). Investment and Institutional Uncertainty: A Comparative Study of Different Uncertainty Measures. *Weltwirtschaftliches Archiv*, 134(3), 513–533. doi:10.1007/BF02707928
- Carraro, A., Ribeiro, F. G., Costa, G. W., Menezes, G. R., Canevar, M. D., & Fernandez, R. N. (2016). Does governmental corruption affect entrepreneurship in Brazil? *Ensaaios FEE*, 37(3), 615–642.

- De Maria, F., Franco, C., & Solferino, N. (2015). *Corruption and innovation: the mediating role of trade* (Working Paper No. 139-2015). Associazione Italiana per la Cultura della Cooperazione e del Non-Profit.
- De Waldemar, F. S. (2012). New Products and Corruption: Evidence from Indian Firms: New Products and Corruption. *The Developing Economies*, 50(3), 268–284. doi:10.1111/j.1746-1049.2012.00171.x
- Ellis, J., Smith, J., & White, R. (2020). Corruption and Corporate Innovation. *Journal of Financial and Quantitative Analysis*, 55(7), 2124–2149. doi:10.1017/S0022109019000735
- Fontaine, A. S. (2016). Prime Minister Resigns. *The Reykjavik Grapevine*. Retrieved from <https://grapevine.is/news/2016/04/05/prime-minister-resigns/>
- Gaviria, A. (2002). Assessing the effects of corruption and crime on firm performance: Evidence from Latin America. *Emerging Markets Review*, 3(3), 245–268. doi:10.1016/S1566-0141(02)00024-9
- Heo, Y., Hou, F., & Park, S. G. (2021). Does corruption grease or sand the wheels of investment or innovation? Different effects in advanced and emerging economies. *Applied Economics*, 53(1), 35–60. doi:10.1080/00036846.2020.1791313
- Hodge, A., Shankar, S., Rao, D. S. P., & Duhs, A. (2011). Exploring the Links Between Corruption and Growth: Corruption and Growth. *Review of Development Economics*, 15(3), 474–490. doi:10.1111/j.1467-9361.2011.00621.x
- Huang, Q., & Yuan, T. (2019). Does Political Corruption Impede Firm Innovation? Evidence from the United States. *Journal of Financial and Quantitative Analysis*, 1–36. doi:10.1017/S0022109019000966
- Huntington, S. P. (1968). *Political order in changing societies*. Yale University Press.
- Hussen, M. S., & Çokgezen, M. (2020). The impact of regional institutional quality on firm innovation: evidence from Africa. *Innovation and Development*, 1–22. doi:10.1080/2157930X.2020.1750143
- Ibrahim, A. R. (2021). Religio-Spiritual Implications of Corruption and Money Laundering: The Case of Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- ICIJ. (2017). *The Panama Papers*. The International Consortium of Investigative Journalists. Retrieved from <https://panamapapers.icij.org/>
- Khan, M. M. (1999). Political and administrative corruption: Concepts, comparative experiences, and Bangladesh case. A Paper Prepared for Transparency International: Bangladesh Chapter, Dhaka.
- Knack, S., & Kisunko, G. (2011). *Trends in corruption and regulatory burden in Eastern Europe and Central Asia* (Working Paper No. 59465). The World Bank.
- Krammer, S. M. S. (2013). Greasing the wheels of change: the impact of corruption on firms' innovation in transition economies (Working Paper). *35th DRUID Celebration Conference*, 17-19.
- Lee, C., Wang, C., & Ho, S. (2020). Country governance, corruption, and the likelihood of firms' innovation. *Economic Modelling*, 92, 326–338. doi:10.1016/j.econmod.2020.01.013

- Leff, N. H. (1964). Economic Development Through Bureaucratic Corruption. *The American Behavioral Scientist*, 8(3), 8–14. doi:10.1177/000276426400800303
- Leys, C. (1965). What is The Problem About Corruption? *The Journal of Modern African Studies*, 3(2), 215–230. doi:10.1017/S0022278X00023636
- Mahagaonkar, P. (2008). *Corruption and innovation: a grease or sand relationship?* (Working No. 017). Jena economic research papers.
- Masood, S. (2017). *Nawaz Sharif, Pakistan's Prime Minister, Is Toppled by Corruption Case*. *New York Times*. Retrieved from <https://www.nytimes.com/2017/07/28/world/asia/pakistan-prime-minister-nawaz-sharif-removed.html>
- Mauro, P. (1995). Corruption and Growth. *The Quarterly Journal of Economics*, 110(3), 681–712. doi:10.2307/2946696
- Méon, P., & Sekkat, K. (2005). Does corruption grease or sand the wheels of growth? *Public Choice*, 122(1-2), 69–97. doi:10.1007/11127-005-3988-0
- Mo, P. H. (2001). Corruption and Economic Growth. *Journal of Comparative Economics*, 29(1), 66–79. doi:10.1006/jcec.2000.1703
- Nosheen, S., Sadiq, R., & Rafay, A. (2016, September). The primacy of innovation in strategic financial management-understanding the impact of innovation and performance on capital structure. In *2016 IEEE International Conference on Management of Innovation and Technology (ICMIT)* (pp. 280-285). IEEE. 10.1109/ICMIT.2016.7605048
- Paunov, C. (2016). Corruption's asymmetric impacts on firm innovation. *Journal of Development Economics*, 118, 216–231. doi:10.1016/j.jdevco.2015.07.006
- Pradhan, S. (2000). *Anticorruption in transition: A contribution to the policy debate*. The World Bank.
- Rafay, A., & Ajmal, M. M. (2014). Earnings Management through Deferred Taxes Recognized under IAS 12: Evidence from Pakistan. *Lahore Journal of Business*, 3(1), 1–19. doi:10.35536/ljb.2014.v3.i1.a1
- Rangarajan, L. N. (Ed.). (1987). *Kautilya: The Arthashastra*. Penguin Classics.
- Rose-Ackerman, S. (2007). Measuring private sector corruption (U4 Brief, 2007(5)). Bergen: Michelsen Institute.
- Sauka, A. (2008). Productive, Unproductive and Destructive Entrepreneurship: A Theoretical and Empirical Exploration. *SSRN Electronic Journal*. doi:10.2139/ssrn.1147811
- Schmidt, D. (2007). Anti-Corruption: What Do We Know? Research on Preventing Corruption in the Post-Communist World. *Political Studies Review*, 5(2), 202–232. doi:10.1111/j.1478-9299.2007.00129.x
- Smith, A. (1776). An Inquiry into the Nature and Causes of the Wealth of Nations. The Glasgow Edition of the Works and Correspondence of Adam Smith: Vol. 2. *An Inquiry into the Nature and Causes of the Wealth of Nations*. Oxford University Press. doi:10.1093/oseo/instance.00043218
- Smith, N., & Thomas, E. (2015). The Role of Foreign Direct Investment and State Capture in Shaping Innovation Outcome in Russia. *Europe-Asia Studies*, 67(5), 777–808. doi:10.1080/09668136.2015.1042430

Tanzi, V. (1998). *Corruption Around the World: Causes, Consequences, Scope, and Cures* (IMF Working Papers, 98(63)). International Monetary Fund.

Tanzi, V., & Davoodi, H. (1998). *Corruption, Public Investment, and Growth. The Welfare State, Public Investment, and Growth*. Springer. doi:10.1007/978-4-431-67939-4\_4

Wei, S. (2000). How Taxing is Corruption on International Investors? *The Review of Economics and Statistics*, 82(1), 1–11. doi:10.1162/003465300558533

Wen, J., Zheng, M., Feng, G. F., Chen, S. W., & Chang, C. P. (2020). Corruption and innovation: Linear and nonlinear investigations of OECD countries. *The Singapore Economic Review*, 65(01), 103–129. doi:10.1142/S0217590818500273

Wooldridge, J. M. (2010). *Econometric Analysis of Cross Section and Panel Data*. MIT Press.

Zolkaflil, S., Nazri, S. N. F. S. M., & Omar, N. (2021). Factors Influencing the Outcome of Money Laundering Investigations. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

## KEY TERMS AND DEFINITIONS

**Administrative Burden:** An administrative cost, which could be a senior manager's time, fees, and bribes, incurred by firms in dealing with government regulation of business.

**Administrative Corruption:** An illegal and non-transparent provision of private earnings to public officials. As a result, an advantage is given to state or non-state actors by deliberately falsifying the prescribed implementation of existing laws, rules, and regulations.

**Corruption:** The abuse of power entrusted to private gain that breaks trust, undermines democracy, hinders economic development, and worsens inequality, poverty, social division, and the environmental crisis.

**Financial Crime:** All activities (corruption, money laundering, fraud, market abuse, etc.) that generate wealth through illegal or dishonest means, or transactions to withhold the proceeds of crime from the access of the law.

**Grease the Wheel:** A way to facilitate some public processes by using corruption to increase the innovation output of innovative businesses.

**Innovation:** Producing a new or significantly improved product (good or service) or improving the process, introducing a new marketing method, or creating a new organizational structure.

**Obstacle:** Factors that interfere with or prevent the performance of the firms.

**Sand the Wheel:** An undesirable result of corruption, which increases transaction costs, feeds job uncertainty, causes misallocation of resources, and damages trust in official institutions.

**State Capture:** The actions of individuals, groups, or firms in both the public and private sectors to influence the formation of laws, regulations, decrees, and other government policies to the public authorities in their interests as a result of the illegal and non-transparent provision of private interests.

## Section 2

# Legislation for Financial Crimes

# Chapter 7

## Conflict of Interest for Corruption and Abuse of Public Power: The Case of European Legislation

**Nikolay Ivanov Nikolov**

*Central Election Commission, Bulgaria*

### **ABSTRACT**

*The chapter presents a conflict of interest as a new pioneering measure for combating corruption and abuse of public power. The study is based on an analysis of the conflict of interest legislations of about 15 European countries. European legislators' legislative decisions on several key criteria relating to conflict of interest have been analyzed. These criteria include the presence or absence of a special law, conflict of interest as a criminal or administrative offense, accountable persons, legal definition, prohibitions, competent authorities and procedures for ascertaining conflict of interest, sanctions, etc. A scientific definition of conflict of interest has also been proposed based on the characteristics of the phenomenon derived from the analysis of the national legislation in force on the European continent. The chapter also outlines the direction in which the phenomenon may develop in national legislations and includes examples of interesting cases of conflict of interest which have arisen in different European countries.*

### **1. INTRODUCTION**

Conflict of interest is a complex social phenomenon which arises both in the public and private sectors. In the former case, conflict of interest constitutes a form of abuse of power and corrupt practice. Conflict of interest undermines the very foundations of modern democratic states as it interferes with the basic principles of state operation such as legal equality, separation of powers and rule of law. The occurrence of conflict of interest in the public service has resulted in its regulation and prohibition in national laws. Various methods have been used at different times and under different political regimes to curb the abuse of public power and corruption.<sup>1</sup>

DOI: 10.4018/978-1-7998-5567-5.ch007

According to national legal regulations adopted in Europe, conflict of interest is always seen as an offence. In some countries it is considered a financial crime, but in most cases, it constitutes an administrative offence. Conflict of interest regulations are part of the so-called administrative measures aimed at combating corruption, which also include incompatibility, declaration of assets and interests, inspections to check the accuracy of the declaration of assets of individuals suspected of corrupt practices, restrictions after dismissal from a public position, etc.

There are two key points in conflict of interest regulations in Europe – definition of the general concept and the different types of conflict of interest, and their prohibition and implementation of methods and mechanisms for preventing and curbing conflict of interest, declaration of assets and interests, incompatibility, removal, withdrawal, etc.

In Europe there is a greater variety of processes and procedures for managing conflict of interest than on other continents. These differences can, however, be classified. Groups of identical or similar legislative decisions can be identified for the different elements of the phenomenon.

At national level European conflict of interest regulations are characterized by:

- relatively similar legislative decisions in relation to the main elements of the phenomenon, albeit with quite different details in the respective countries.
- a strong focus on the right of defence of the individual suspected of conflict of interest.
- significantly more fully developed conflict of interest regulations for the public sector compared to the private sector.

National regulations are also influenced by a supranational factor, which is unique for this continent. The legislative decisions relating to conflict of interest contained in the legislation of the European Union, being a community consisting of 27 countries, have an inevitable effect on the regulation of the phenomenon in the legislations of these member states and other countries.

This chapter provides a brief description of the conflict of interest phenomenon. In the broadest sense, conflict of interest is corruption.<sup>2</sup> The existing conflict of interest regulations mainly aim at preventing private interests from influencing the objective and impartial performance of the official duties of civil servants. Only legislative decisions aimed at managing conflict of interest in the public sector are going to be discussed. Moreover, this chapter also examines and draws conclusions on different aspects of the conflict of interest regulations in European countries – special legislation, the concept and legal definitions of conflict of interest, scientific definition, groups of accountable persons, declarations of assets and interests, restrictions whose violations result in conflict of interest, sanctions, competent authority, incompatibility, etc.

## **2. REGULATORY FRAMEWORK FOR SPECIAL LEGISLATION**

Conflict of interest is regulated in two main ways – through provisions under the general law or through special laws, where the former approach prevails. The general laws that contain provisions on conflict of interest are most often public service regulations (e.g. in France, the Netherlands, Hungary, Russia, etc.) or the Criminal code (e.g. in Germany, Austria). The countries that have special conflict of interest laws tend to be in Eastern Europe.<sup>3</sup> These countries include the Czech Republic, Slovakia, Latvia, Croatia, Bulgaria, Serbia, Montenegro, the Republic of North Macedonia, etc. The presence of special

legislation in these countries is related to the requirements for their accession to the EU and their status as current candidates.

As mentioned above, regardless of whether there is one or several general or special conflict of interest laws, the elements of conflict of interest under the different national legislations are identical or similar. This allows for the information and analysis that follow to be organized according to the main elements of conflict of interest. Due to the variety of rules existing in the different legal systems, it is possible to talk about sets of conflict of interest rules that regulate similar social relationships. These rules fall under the constitutional, administrative and in some cases criminal law of the respective countries.

## **Administrative or Criminal Offence**

In most European countries conflict of interest is seen as an administrative offence. In Germany, Austria and Hungary conflict of interest constitutes a criminal offence and is regulated in the Criminal Code.

The decision which of the two approaches to choose is left to the discretion of the national legislature. If conflict of interest is considered a criminal offence, then the legislator has concluded that it has a significant impact on social relationships. If it is seen as an administrative offence, this means that according to the legislator the rules and procedures of state operations have been violated, albeit to a lesser extent compared to the criminal offence.

## **Accountable Persons**

An important element of each national law is the provision which defines the persons obliged to comply with the conflict of interest regulation and make the disclosures stipulated in it. This group of persons is usually defined by the term “public office holders”. According to each examined national law, the accountable persons include the President and the Vice-president, the members of one or both chambers of Parliament, the Prime Minister and the ministers, deputy ministers, heads of agencies, members of collegial regulatory bodies (e.g. Court of Auditors, the Radio and Television Council), district/regional governors and their deputies, members of district/regional councils, mayors and deputy mayors of municipalities, municipal councillors, judges, prosecutors<sup>4</sup>, etc.

These offices belong to the three branches of power – legislative, executive and judicial. Some public office holders are chosen through direct elections, whereas others are elected by Parliament or appointed. These individuals are involved in the adoption of the most important decisions and legal instruments in the country. All these offices are part of the government apparatus and have different areas of competence.

There are conflicting legislative decisions regarding public office holders in different administrations – of the president, the parliament, executive bodies, including local and judicial authorities. In some countries they are all obliged to comply with the conflict of interest regulation and to make disclosures (e.g. in Bulgaria and Latvia), in other countries (like Croatia) only those holding a management position in the public administration (like heads of directorates) are obliged to comply. In a third group of countries (Great Britain, France and the Czech Republic) experts are not considered accountable persons.

Some countries are starting to expand the list of accountable persons to include positions from the private sector. In recent years, the list of persons obliged to comply with the conflict of interest regulation has grown to include state and municipal representatives in the managerial and supervisory bodies of companies and non-profit legal entities with state or municipal participation, managing directors of publicly funded private hospitals, as well as notaries and private bailiffs. These bodies are involved in



the management of public funds or assets or carry out duties assigned by the government (like notaries and private bailiffs). This is the reason for adding these positions to the list of accountable persons. This is an acceptable argument because conflict of interest can arise not only out of the performance of the duties of a government official, but also out of the handling of public funds or the performance of duties assigned by the government.

The lists of accountable persons in European countries have several other characteristics:

- They are exhaustive, i.e. they include all accountable persons.
- They are limitative, i.e. the conflict of interest regulation and obligation for disclosure do not apply to persons that are not included in the lists and consequently these persons cannot be held accountable for their non-compliance.

In principle, only natural persons are held accountable under the respective laws. Where a conflict of interest is found to exist, a legal entity<sup>5</sup> may be held indirectly liable for a specific constituent element of the administrative offence. The fact that a person has lost their status of a public office holder does not mean that they cannot be held liable for a particular offence. An important requirement for holding somebody accountable is for them to have been a public office holder at the time the offence was committed, and not at the time when they are held liable for it.

### **3. LEGAL DEFINITIONS**

The legislation of most European countries where there is a conflict of interest regulation contains a legal definition of this phenomenon. Based on the analysis of these definitions, a theoretical definition of the phenomenon can be formulated to include all its essential elements provided by law.

#### **“Conflict of Interest”, “Private Interest” and “Related Parties”**

There are two approaches to defining the term “conflict of interest”. In both cases it is seen as a specific situation. The first approach defines conflict of interest as a collision or clash between the public and private interests of a public office holder, who chooses to further their private interests despite the fact that they are obliged to promote and protect public interests (e.g. in the Czech Republic, Slovakia, Hungary, etc.). The second approach defines conflict of interest as the exercise of official powers or duties by a public office holder in order to further their own private interest or the private interest of a related party, which can influence or affect the objective and impartial performance of functions/exercise of powers (e.g. in Bulgaria, Russia, Serbia, Bosnia and Herzegovina, etc.)

By summarizing these two approaches, we can derive three main elements for the presence of conflict of interest according to the applicable legislations of the European countries. These three main elements have a cumulative nature.

#### **A Public Office Holder**

Only a person holding a public office as per the exhaustive list laid down in the respective national law can be involved in conflict of interest. The most common examples of such persons have been listed in

## ***Conflict of Interest for Corruption and Abuse of Public Power***

item 3. The person should have exercised their official powers or duties. These official powers or duties should be assigned to them by law or a legal act if the person holds a high-ranking public office, or should be specified in their job description if the person holds an expert position. These official powers or duties should have been exercised.

Undoubtedly, the presence and ascertainment of conflict of interest depend on the public official's acting in the exercise of their official powers and duties. This exercise of official powers or duties should be recorded and proven.

The following interesting question consequently arises: is it possible for conflict of interest to occur not only through action, but also through inaction? It is only possible if it has been explicitly specified in the relevant legislation. On the other hand, the basic requirement for the exercise of official duties suggests the active involvement of the public office holder. So far, no legislative decision, theory or practice have been known to suggest that conflict of interest can arise through inaction. To the contrary, the Supreme Administrative Court of Bulgaria has ruled twice on specific cases that conflict of interest can arise only through action.<sup>6</sup>

The first two elements point to normal and ordinary social relationships – a public office holder exercises their official duties assigned to them by law or as specified in their job description. This social relationship is “distorted” and becomes socially harmful and detrimental which requires a restriction to be imposed on this behaviour as described by the third element whose presence is mandatory for conflict of interest to arise.

### **Private Interest of the Public Office Holder or a Related Party**

The public office holder should have exercised their official duties in order to further their private interests. It is exactly this element that makes their behaviour illegal and turns it into an administrative or criminal offence.

Private interest is a subjective element. It is present in the mind of the public office holder and is defined as a perceived need. The important thing here is that this private interest should result in a benefit for the public office holder or a related party. The potential for personal gain is an integral part of the concept of conflict of interest. The violation itself stems from the fact that when private and public interests collided, the person acted to further their private interest for personal gain thus ignoring public interests.

All special national conflict of interest laws contain a definition of the term “private interest”. In §3, para. 1, sentence 2 of Law No 298 of the Czech Parliament<sup>7</sup> “private interest” has been defined as follows: “*any interest securing any private benefit or preventing possible reduction of any material or other benefit.*”

Article 53 of the Anti-corruption and Forfeiture of Illegally Acquired Assets Act of the Republic of Bulgaria<sup>8</sup> defines private interest as “any interest which results in a tangible or intangible benefit for a senior public office holder, or for any parties related thereto, including any obligation assumed.”<sup>9</sup>

According to applicable legislations, private interest has several characteristics.

The benefit gained can be both tangible and intangible. Examples of a tangible benefit include money, dividends, exemption from a fine, acquisition of real estate property at an advantageous price, etc. The presence of a tangible benefit as part of the definition and as a constituent element of conflict of interest gives it the characteristics of a “financial crime”. Examples of intangible benefits include support, influence, assistance, etc.

As regards the person whose private interests result in the occurrence of conflict of interest, this could be the public office holder who exercises their powers or a party related thereto. An analysis of the case law of European courts shows that in most cases conflict of interest has arisen in relation to the private interests of a related party. There are many different legal definitions of the term “related party”. This is an important issue as it defines the scope of conflict of interest with regard to the interested persons (Rafay, Sadiq & Ajmal, 2016).

Related parties are organized into two main groups – individuals and legal entities. Here, just like with the group of accountable persons, the principle of legality should be strictly observed – only the persons or entities specified in the law can be seen as parties related to the public office holder. Examples of individuals related to the public office holder include relatives and family members. This list can vary, but it always includes lineal relatives (regardless of the degree), collateral relatives (to a certain degree), and affinity relatives by marriage within the second degree. An interesting fact is that the partner with whom a public office holder is cohabiting also has the status of a relative who is a related person.

Regarding the definition of related legal entities, legislators use three possible approaches: related parties are not defined,<sup>10</sup> related parties are broadly defined, or related parties are strictly defined.

An example of a broad definition can be found in Bulgarian legislation: *“a person on whom the public office holder is economically and politically dependent, which causes reasonable doubts as to his/her impartiality and objectivity”*. This definition includes companies in which the public office holder is a shareholder, companies in which the public office holder is part of the managerial and supervisory bodies, political parties. It, however, does not include non-profit legal entities in which the public office holder is a member of the managerial and supervisory bodies if the public office holder does not receive remuneration as there are no economic relationships involved.

Strict definitions include specific numbers and parameters to describe the relationship between the public office holder and the company. For example, §4b and §4c of Law No 298/2016 of the Czech Parliament prohibits the award of public procurement contracts, the provision of subsidies or investment incentives from the state budget to companies in which public office holders listed in §2 of the Law hold at least 25% of the shares.

Article 3, §1, B. “i” of the Law on Conflict of Interest in Government Institutions of Bosnia and Herzegovina defines financial interest as any ownership interest held by a public office holder which represents a value of at least ten thousand convertible marks (10,000 KM) of an enterprise, partnership, limited partnership, joint stock company or company with limited liability.

#### **4. SCIENTIFIC DEFINITION**

The existing legal definitions do not cover some key characteristics of the conflict of interest phenomenon. The need for a theoretical definition stems from the need for a broader definition of the basic characteristics of conflict of interest in European legislations. From a methodological point of view, this scientific definition should include characteristics of the main points outlined herein – nature of the phenomenon, characteristics of the three key elements according to the legal definitions, accountable persons, proceedings for ascertaining and prosecuting conflict of interest, competent authorities responsible for conducting these proceedings, final decision in the proceedings and sanctions.

Based on these criteria, the following scientific definition of conflict of interest is proposed based on the legislation of European countries.

## **Conflict of Interest for Corruption and Abuse of Public Power**

*Conflict of interest is an administrative or criminal offence which represents an act of corruption and involves the exercise of official powers or duties by certain public office holders as defined by law in order to further their own private interest or the private interest of a related party, which has been ascertained by an administrative body or prosecutor by conducting the necessary proceedings and an administrative or a criminal sanction has been imposed in the form of a fine or other sanctions specified in the relevant national law on sanctions.*

## **5. PROHIBITIONS WHOSE VIOLATION RESULTS IN CONFLICT OF INTEREST**

Most national laws introduce specific prohibitions whose violation results in conflict of interest. The term “prohibition” is even legal and refers to a prohibition system that applies to conduct that constitutes conflict of interest. The facts and circumstances under these provisions include the prohibitions themselves. They are not very different from the definition of conflict of interest. Each fact and circumstance of these prohibitions includes the three cumulative elements laid down in the definition of conflict of interest – a public office holder, private interest, either their own or of a related person, which can result in personal gain or the exercise of official powers or duties to further this private interest. The difference between the prohibitions themselves and between the prohibitions and the general legal definition is the act itself. Each prohibition specifies different official powers/duties affecting a private interest.

These prohibitions are laid down in §3, para. 2 of the Czech Parliament, articles 55-62 of the Anti-corruption and Forfeiture of Illegally Acquired Assets Act of the Republic of Bulgaria, articles 11-13 of the Latvian Law on the Prevention of Conflict of Interest in the Activities of Public Officials and article 7 of the Croatian Law, article 6 of the Serbian Act on the Prevention of Conflict of Interest in the Discharge of Official Duties, etc.

We are going to look at some of the constituent elements of these prohibitions, whose violation creates conflict of interest.

### **Voting According to One’s Private Interest**

Bulgaria, Croatia, Bosnia and Herzegovina, etc. are typical examples of collegial bodies – members of parliament, ministers, municipal councillors. The most important power vested in these officials is their capacity to participate through their votes in the shaping of the collective will of the respective body for adopting or rejecting a decision. In order for conflict of interest to arise, it does not matter if the decision has been adopted or rejected, or how the voting has been done – by show of hands, by an electronic system or by roll call. A person can vote according to their private interest regardless of the way they have voted – affirmatively (in favour), negatively (against), or neutrally (abstained).

### **Preparing and Issuing an Administrative Act According to One’s Private Interest**

In this situation (e.g. in Latvia, Croatia, Bulgaria, Ireland, etc.) the prohibition can be violated by experts (via preparation) or a single authority body (via issuance). Administrative acts can vary in nature – they can be orders, construction permits, dispute resolutions, etc. Administrative acts are the most common way of exercising power in a country. The acts that are of relevance are the ones that create rights. Such

acts include general, normative and individual administrative acts<sup>11</sup>. The preparation of the act includes activities such as drafting, coordinating, submitting and giving an additional opinion, etc. The issuance of the act requires the exercise of powers typical of single authority bodies and is similar to voting in the case of collegial bodies.

A case in point which was being discussed in Italy was allowing the daughter of a famous rich Italian family to serve her prison sentence under house arrest with a special authorisation from the Minister of Justice, whose son was a senior manager at one of the family's companies.

## **EXERTING INFLUENCE ACCORDING TO ONE'S PRIVATE INTEREST**

In order for conflict of interest to arise in this situation (e.g. in Slovakia, Croatia, Bulgaria, Hungary, etc.) there should be two accountable persons involved according to the list laid down in the relevant national law. The main prerequisite is for one of the persons to exert influence on the other one. The violation is committed by the public office holder exerting the influence. Influence shall mean exercising one's powers to have an effect on someone in order to gain a benefit for oneself or a related party. An element of the violation is not whether the person being influenced has given in or not. According to the elements of this violation, the influence can be general or within the scope of a certain procedure which has been explicitly defined as part of the elements constituting the violation – concluding a contract, preparing, approving and issuing acts, or performing monitoring or investigating functions. The difficulty in substantiating the charge lies in finding the evidence to prove undue influence. While influence can be exerted through a written act or order, it is more frequently done over the phone or face to face.

A well-known case in point is the case with the Prime Minister of Hungary, whose son-in-law was on the Management Board of a company that between 2011 and 2015 won public procurement contracts with EU funding for the improvement of street lighting in several Hungarian municipalities.

## **Concluding Contracts According to One's Private Interest**

This power (e.g. in Latvia, Croatia, Bulgaria, Bosnia and Herzegovina, etc.) is vested in single authority bodies which have managerial and representative functions in the respective department (Ministers, chairmen of agencies, mayors, etc.). In legal theory these are also known as administrative contracts (de Laubadere, 1991 *et al.*; Sodan, 2005).

Contracts are also a main administrative tool for performing activities and transferring resources from the public to the private sector. The contract must be concluded by a competent official. The intent to conclude the contract is not part of the constituent elements of the prohibition. Conflict of interest can arise out of any kinds of contracts – sales contracts, exchange contracts, lease agreements, public procurement contracts, concession contracts, employment contracts, etc.

A well-known case in point is the case of the former Prime Minister of France, who while he was a senator employed two of his five children and used public funds to pay them to do non-existent jobs.

## **Prohibition to Perform Monitoring and Control Functions, Conduct Inquests and Impose Punishments According to One's Private Interest**

This prohibition (e.g. in Latvia, Croatia, Bulgaria, etc.) refers to the exercise of powers or duties related to control and sanctioning proceedings as well as to the sentencing itself. The monitoring and control functions are identical. The first two powers are in the field of administrative control. Control is a typical legal institute of administrative law and procedure (Alibert, 1926). There are a lot of control proceedings which can give rise to conflict of interest – construction supervision, tax inspections, customs control, food and hygiene control, financial and audit control, etc. Exercising one's power of control to further one's private interest is most often proven by written evidence – records, checklists, audit reports, etc. The second group of powers exercised to further one's private interest refers to two separate stages of the criminal proceedings, i.e. inquest (pre-trial investigation for committed crimes) and sentencing (court proceedings). The term “sentencing”, however, covers court decisions that impose punishments for committed crimes and administrative sanctions through criminal orders.

## **Using Information for Personal Gain**

The information can be used (e.g. in the Czech Republic, Slovakia, Bulgaria, Latvia, Croatia, etc.) both by the public office holder and by a third party to whom it was made available by the public office holder to further their own private interest or the private interest of a related party. The information used constitutes the object of the administrative violation. Here the legislators have laid down several requirements. The information has to be official and the offender should have acquired it in the course of their official duties. The information has to be confidential and it must not be in the public domain and common knowledge. If the information has been published on the website of the respective institution and has been disclosed to a third party by a public office holder for personal gain, it should not give rise to conflict of interest, because the principle of equality before the law will not have been violated. All individuals have access to that website. The difficulty of proving that second hypothesis in administrative practice lies in the burden of proving when and how the public office holder who has committed the administrative offence disclosed the information to the third party.

## **Commercial Advertising and Using Public Office Symbols and Signs for Personal Gain**

With this prohibition the intentions of national legislators (e.g. in Slovakia, Latvia, Croatia, Bulgaria, etc.) are to prevent someone from using their public office to advertise a certain private business activity which is compatible with their public duties. However, national laws often lack a definition of the term “commercial advertising”. The use by public office holders of symbols and signs of the institutions where they work to support a certain private business activity or in their private correspondence is a projection of the prohibition to engage in commercial advertising in their private communications.

## **6. WAYS OF PREVENTING CONFLICT OF INTEREST**

### **Withdrawal**

This is the most popular form of preventing conflict of interest provided for in all national legislations. The public office holder is obliged to withdraw from performing a particular duty or exercising a particular power if the public office holder or a related party thereto has a private interest in the matter. If such a situation arises, the person concerned does not have any discretionary power and has to withdraw. It is important that the person should withdraw before they perform the respective official duty. They should notify their immediate superior of the presence of a private interest in relation to the assigned task. It is recommended that public office holders should submit a written and reasoned request for withdrawal. In such cases their superior must appoint another officer to perform said duties.

### **Removal**

The immediate superior has the right and obligation to remove an official. The superior has the right to order a public office holder not to perform a certain duty that falls within their competence provided that (1) the superior has evidence that the public office holder or a related party thereto has a private interest in the specific matter and (2) the public office holder has not requested withdrawal.

Removal is a safeguard clause that ensures withdrawal. This measure is used when the person who is obliged to withdraw has not taken the initiative to request withdrawal. The decision for removal must also be reasoned. In order to prevent conflict of interest, public office holders should be removed before they perform their duties.

### **Consulting an Ethics Officer from the Respective Department**

European legislations lay down a provision that requires each department to have a so-called ethics officer (Article 9 of the French Law on Ethics, Rights and Obligations of Civil Servants from 2016). Public office holders often times do not know whether a certain situation constitutes conflict of interest and how to act. The job of the ethics officer is to explain the law and provide legal advice to public office holders who come to him/her with questions about its application. The ethics officer makes a preliminary review. This is a new practice in conflict of interest prevention.

## **7. COMPETENT AUTHORITY FOR CONDUCTING CONFLICT OF INTEREST PROCEEDINGS**

Conflict of interest is an offence which is subject to investigation and prosecution. The authority which is entrusted by law to conduct the proceedings for ascertaining and sanctioning conflict of interest depends on the nature of the offence according to the relevant national legislation (criminal or administrative offence) and the nature of the proceedings themselves (administrative, criminal or mixed).

The question about the competent authority is part of a more global process. In the last 20 years, European legislators have adopted two anti-corruption measures – adopting special anti-corruption laws and setting up specialized anti-corruption bodies. This tendency has been driven by two factors –

globalisation and the United Nations Convention against Corruption adopted in 2003 which imposed requirements for the setting up of specialized investigating and prosecuting authorities and specialized anti-corruption bodies (Zolkafilil, Nazri & Omar, 2021).

The existing institutional systems for ascertaining and sanctioning conflict of interest can be organised into three main types. Interestingly, they exist in several modifications.

## **Independent Administrative Body**

This system of competent authorities is most widely used on the continent. It is characteristic of the legislations which define conflict of interest as an administrative offence, and these are the predominant ones on the continent.

In this case, the body is obliged to perform both functions – to ascertain the presence of a conflict of interest and to impose the relevant administrative sanction. Of course, the penal decree is subject to judicial review.

The general characteristics of this body are discussed here. The body belongs to the executive branch and is essentially an administrative body. This is because it carries out and enforces a law. Its functions are typical of the executive branch, i.e. governmental functions. It holds public authority or imperium. This body is set up either by Parliament, or by the respective national government, or by both. The body is composed of officials who are nominated and elected for a fixed term. In a number of their characteristics, these independent European bodies in charge of regulating conflict of interest are akin to the independent regulatory agencies in the USA (Strauss, 2002; Funk, 2005). They conduct administrative and administrative penal proceedings, where any unresolved issues are settled in accordance with the general administrative procedure law. They have the functions of a regulatory body and can be defined as a regulator of conflict of interest. At the end of the proceedings the relevant bodies issue administrative and administrative penal decrees. During the proceedings these bodies exercise the power to impose administrative sanctions which is typical of administrative bodies.

It is interesting that in some countries the scope of authority of the body covers only conflict of interest (e.g. in Croatia, Macedonia, etc.). The specialized bodies that have been recently set up to perform functions in the field of conflict of interest have a wider scope of authority. It covers all administrative anti-corruption measures – prevention of corruption, declarations of assets and interests, incompatibility, conflict of interest, etc. Such powers have been vested in the relevant competent bodies in Poland, Romania, Bulgaria, Montenegro, etc. The more consolidated approach taken by these national legislators is to some extent justified. There is a certain link between these different legal institutes belonging to administrative law and procedure.

In terms of their structure, these bodies can be divided into two main types – collegial (commissions) and single authority. Commissions are usually composed of 5 members who are appointed by Parliament. The governmental function of ascertaining and sanctioning conflict of interest is performed by commissions in Croatia, Slovenia, Bulgaria, Macedonia, etc. Of particular interest is the commission in Ireland, which is composed of 5 members, two of whom are the ombudsman and the auditor general (Cambell, 2007). The commissions hold regular meetings and sessions.<sup>12</sup> The decisions on the presence or absence of conflict of interest are taken in compliance with quorum and majority requirements.

Single authority bodies are usually set up as bureaus or agencies. This administrative unit is headed by a director who has one or two deputies. The director is also elected by Parliament or appointed by the government for a fixed term. This is the organization of the independent bodies in Latvia (KNAB –



Corruption Prevention and Combating Bureau), Poland (the Central Anti-Corruption Bureau of Poland) etc. The important thing here is that the function of ascertaining and sanctioning conflict of interest is performed solely by the head of the respective office. Over the last 5 years there has been an interesting tendency of transforming collegial bodies into single authority ones.

The collegial form of the anti-corruption body is more appropriate. It ensures in a much better way one of the main characteristics that these bodies should possess, namely independence. This is achieved through two mechanisms – three votes are needed to achieve majority (if the body is composed of 5 members) and the members of collegial bodies almost always include representatives of the opposition.

The proceedings conducted by the respective body are *ex parte* proceedings. The sole party to the proceedings is the public office holder accused of conflict of interest. These proceedings are usually instituted by the competent authority after an alert has been issued by a citizen or an organization or based on a media publication. Most European countries do not allow anonymous alerts. The body conducts the administrative phase of the proceedings. The purpose of this first phase is to issue a decree on the presence or absence of conflict of interest, where in the former case it also imposes a sanction. The independent body is obliged to collect all relevant evidence on its own. The interesting thing here is that the right of defence of the accused is well-rounded as the laws oblige the administrative body to hear the person under investigation before issuing its decree, to collect and admit the evidence provided by him/her, etc. The second phase of the proceedings is the judicial phase. It is contingent and depends on whether the case has been referred to the court by the accused public office holder (if the presence of conflict of interest has been ascertained) or by a prosecutor (if the presence of conflict of interest has not been ascertained). The proceedings are conducted in accordance with the general procedural law and involve an assessment of the legality of the administrative act issued.

### **The District Court Is the Place Where the Offence Was Committed (in Case of Referral)**

Czech legislation<sup>13</sup> explicitly stipulates that the authority that is competent to rule on the presence or absence of conflict of interest is the district court in the place where the public office holder is based or is on a visit. This is an unusual decision and to the best of our knowledge it has not been adopted anywhere else except in the Czech Republic. The important thing here is that the function of ascertaining and sanctioning is performed by the court. The usual practice is for administrative offences to be ascertained and sanctioned by the competent administrative authority. When the case is referred to the court, the court exercises control over the legality of the issued administrative act.

The court conducts ascertaining and sanctioning proceedings. This puts the court in the unusual position of collecting the evidence on its own and of ascertaining the presence or absence of an offence. In order to rule on the case, the court has to be seised with a report from the body that has appointed the public office holder, in which the body should provide facts and reasons why it thinks that there is conflict of interest. The report should be accompanied by evidence which the appointing body has collected. The proceedings conducted before the courts are *inter partes* proceedings where the two parties are the appointing body that has seised the court and the public office holder accused of conflict of interest. Here the court is in its usual position. Although it may require all the evidence it may see fit, in these proceedings it settles a legal dispute with a judicial decision. If the court rules that there is conflict of interest, it will have to impose an administrative sanction within the limits stipulated by law.

The court's decision can naturally be appealed both by the accused and by the appointing body before a higher instance court.

### **The Prosecutor's Office With the Assistance of the Police as an Investigative Body and the Court as a Penalizing Authority**

This institutional framework for prosecuting and sanctioning conflict of interest is typical of the countries where this offence has been defined and punished as a crime. These are mainly countries that belong to the so-called German legal system: Germany, Austria, Hungary, as well as Spain and Romania, and in some cases Ireland.

Just like the specialized bodies, this institutional model is organised into two groups. The first group includes those countries where the functions of prosecuting and sanctioning conflict of interest are performed by the general prosecutor's office (e.g. in Germany and Hungary). The second group includes countries which have set up specialized anti-corruption prosecutor's offices which form part of the structure of the prosecutor's office (e.g. Spain, Austria, and Romania).

The rules of the classic criminal procedure apply to this institutional framework. The first phase of the proceedings (the pre-trial phase) is conducted by the investigative bodies (the police) under the authority of a prosecutor. At the end of these proceedings, the prosecutor terminates the initiated pre-trial proceedings or files an indictment in court. The criminal court is the authority that is competent to issue a verdict which finds the accused public office holder guilty and imposes a sentence that complies with the Criminal Code. According to criminal procedure rules, anyone who has knowledge of committed criminal conflict of interest can submit an alert to the prosecutor's office.

### **The Right of Defence is Exercised Under the Criminal Procedure Rules**

An interesting example is the experience of the Kingdom of Spain where the specialized prosecutor's office has been investigating corruption crimes to fight organized crime and corruption. Like in Ireland, this specialized prosecutor's office is composed of experts from other executive bodies – the tax agency, financial inspectorate, the national police – who have been delegated to work on certain investigations.

As far as Ireland is concerned, it should be noted that when in the course of its operations the specialized commission of mixed experts finds evidence of a crime committed by a public office holder, it is obliged to notify the Irish prosecutor's office.

## **8. SANCTIONS**

The sanctions should be organized into two major groups – sanctions when conflict of interest is seen as an administrative offence and sanctions when conflict of interest is defined in the national legislation as a criminal offence. The main provisions on administrative sanctions and penalties under the Criminal Code are typical of and applicable to each of the two groups, to the extent to which national laws do not specifically provide otherwise.

## **Administrative Sanctions for Conflict of Interest as an Administrative Offence**

It should be noted that traditionally when there is conflict of interest the offender to be sanctioned is an individual who is a public office holder. In some cases, however, a sanction is also imposed on the related legal entity which has benefited from the conflict of interest.

Apart from the subject of sanctions, a second criterion for classifying administrative sanctions is whether they are pecuniary or not:

### **Pecuniary Administrative Sanctions**

*“Imposing a Fine on the Individual who has Committed Conflict of Interest”* is the most common administrative sanction. When this sanction is imposed, the offender is liable to pay a certain amount of money. Different legislations opt for one of two ways of determining this amount. The first approach is for the sanction to be determined in absolute terms with an upper and lower limit. Examples include the legislation of the Republic of Bulgaria. Pursuant to Article 171 of the Bulgarian law, the fine imposed for a first offence related to conflict of interest ranges from BGN 5,000 to BGN 10,000. The second approach is for the sanction to also be determined based on the offender’s salary. In Slovakia this fine can be as high as twelve monthly salaries. In Croatia this sanction involves a suspension of payment of part of a monthly salary and is limited to no more than a year, and the amount ranges from HRK 2,000 to HRK 40,000, but not more than 50% of the monthly net salary.

Another sanction is *“Forfeiture of the remuneration received for the period during which conflict of interest has been concealed”*. This sanction is imposed in Bulgaria and involves the forfeiture of the net amount of the remuneration for the date/dates on which the offence constituting conflict of interest was committed.

Another form of sanction is *“Forfeiture of the tangible benefit which the public office holder or a related party thereto has received as a result of the conflict of interest”*. This benefit (e.g. in Bulgaria) can be a payment received by the related party under a concluded contract constituting conflict of interest, a salary paid to a family member or relative who has been appointed to an administrative office which gives rise to conflict of interest.

In some cases (e.g. in Ireland) pecuniary sanction is applicable for the individual/related legal entity that has received a benefit as a result of conflict of interest.

## **NON-PECUNIARY ADMINISTRATIVE SANCTIONS**

### **Premature Termination of a Term of Office or Employment**

This is probably the most severe sanction when conflict of interest has been ascertained by an effective act. It is imposed in relatively few countries (e.g. in Slovakia, Bulgaria, etc.). The grounds for premature termination of the term of office/employment have been laid down both in the special law, and in the labour law. What is interesting is that it is applicable both to elected and appointed positions. This sanction is imposed only by an effective decision ascertaining conflict of interest. The authority competent to impose it is the body stipulated in the relevant legislation. For members of Parliament – a parliamentary committee (e.g. in Slovakia – with a 3/5 majority), for municipal councillors and mayors – the members

## ***Conflict of Interest for Corruption and Abuse of Public Power***

of the Municipal council (e.g. in Slovakia – with a majority of ½) or the Municipal election commission (e.g. in Bulgaria – with a majority of two-third), for experts in administrations – the relevant appointing authority. Each act terminating the term of office/employment of a public office holder issued on these grounds is subject to appeal before a court.

### **Prohibition to Hold a Public Office for a Period of 1 Year After the Decision Whereby a Conflict of Interest Is Ascertained Becomes Enforceable**

The former public office holder loses the right to hold a public office (e.g. in Bulgaria), including to be directly elected to office. The measure is imposed for a period of 1 year and aims at re-educating the offender and deterring other members from committing the same offence.

### **A Warning**

Article 43 of the Croatian law provides for the possibility not to impose a pecuniary sanction on a public office holder who has committed conflict of interest provided that it constitutes a minor offence.

### **Public Announcement of the Decision Ascertaining Conflict of Interest**

This is usually done on the Internet page of the respective institution (e.g. in Croatia). In most of the countries the decisions ascertaining conflict of interest are usually published on the web pages of the institutions even if such a sanction has not been provided for by law.

*The next three aspects which are going to be discussed, namely incompatibility, declarations of assets and interests and restrictions after vacating a public office, do not belong to the field of conflict of interest and their violation does not constitute conflict of interest. However, these three aspects are directly related to conflict of interest, because compliance with these rules curbs conflict of interest or represents a natural continuation thereof after vacating the public office. To some degree, the regulations relating to these three aspects are more fully developed in national legislations than those relating to conflict of interest.*

## **9. INCOMPATIBILITY**

The theoretical definition of incompatibility is the legal prohibition to exercise a certain profession or perform certain activities which are in conflict with the nature of the office held, limit or prevent the independent exercise of powers or duties, damage a person's integrity or the good name of the body or institution.

Incompatibility must have a sound legal basis. Only these circumstances which are laid down by law shall constitute incompatibility. Every legislation contains an incompatibility clause. It is included both in the special law, and in the Constitution as well as in various organic laws. Incompatibility is an autonomous legal norm which aims to limit the activities of public office holders while they hold a public office in order to ensure that they exercise their powers and duties objectively and impartially. Compliance with incompatibility rules precludes or greatly limits the possibility for conflict of interest to occur. It is a tool for conflict of interest prevention and management.

There are two approaches that European legislators adhere to when they define the legal basis for incompatibility. With the first approach these grounds are defined in the general anti-corruption law for all or most public office holders (e.g. in the Czech Republic, Latvia, etc.) and with the second approach the general law refers to various special laws where these grounds are provided for (e.g. in Bulgaria, etc.) The legal basis for incompatibility is always comprised of specific facts and circumstances.

The facts and circumstances that result in incompatibility under EU law can be organized into three groups:

## **Business Interest**

There are three restrictions:

1. prohibition to be part of a managerial or supervisory body in a company
2. prohibition to hold a share of the capital of the company
3. prohibition on a sole proprietor or a company in which the public office holder is a shareholder to conclude contracts with the state authority or municipality where the public office holder is employed.

A violation of any of these three restrictions constitutes incompatibility. These prohibitions aim to ensure the objective and impartial exercise of public powers and duties when commercial interests are concerned.

Various laws prohibit public office holders to be part of the managerial and supervisory bodies in companies and partnerships or to be sole proprietors.<sup>14</sup> Such laws have been introduced in most countries both in respect of public office holders and in respect of experts in public administrations.

In some countries public office holders are prohibited to hold stocks and shares in companies. Article 16 of the Croatian conflict of interest law states that an official who owns 0.5% or more shares of a company capital shall transfer his/her shares to another person for the duration of his/her term of office. The official has the right to be informed once a year on the state of the company. The business entity is obliged to inform the Croatian commission prior to concluding a contract with a state authority body or units of the local self-government. This hypothesis is different from the previous one because holding company shares imparts dividend rights and voting rights at the general meeting of shareholders, which is neither a managerial nor a supervisory body.

In France, Great Britain, Portugal,<sup>15</sup> Spain and Latvia public office holders are prohibited to own private companies which have business relations with the public sector or when public officials need to regulate, supervise and conclude contracts with them. §4B and §4C of Law No 159/2006 of the Czech Parliament prohibits companies in which a public office holder or a related party thereto holds 25% or more of the shares to be involved in public procurement procedures, as well as to receive subsidies from the budget as subcontractors.

## **Holding Other Positions**

This legal basis for incompatibility is divided into two subcategories – positions in the public sector and positions in the private sector. There is a total ban on holding other positions in the public sector at national level. No public office holder, whether he/she is an elected official or an expert, may be al-

lowed to hold another public office. However, there are two big exceptions. In Great Britain it is not prohibited and incompatible for a member of parliament to also be a cabinet member. Quite the reverse: ministers are chosen from the members of the House of Commons and House of Lords. According to a long-standing tradition and an existing organic law adopted pursuant to Article 25 of the Constitution, in France members of parliament may also be mayors. In Hungary the situation is exactly the same.

At municipal level, things stand a bit differently. It is not prohibited and incompatible for municipal councillors to be employed as experts in a state authority body or to even be heads of a territorial unit of local state government, but they are prohibited to hold an office in the municipality where they serve as municipal councillors. When it comes to private sector jobs there are also exceptions to the bans. For instance, public office holders are allowed to hold teaching positions or members of parliament may also simultaneously serve as lawyers.

## **Political and Civic Activities**

The legal basis for incompatibility here is related to prohibitions on holding leadership positions in political parties and non-governmental organizations. In France, Germany, Russia, Latvia, Poland, Spain and Great Britain politically appointed officials are not allowed to be simultaneously involved in non-governmental organizations during their term of office. In Hungary, Poland and Great Britain high-level officials may not hold senior positions in political parties. In Bulgaria this requirement has been adopted for experts in public administrations. In all European countries there is a prohibition on magistrates, military and police officers to be members of political parties.

Incompatibility constitutes a formal offence. Incompatibility arises when certain facts and circumstances are present. It is not necessary for specific results or intentions to have been achieved. The most severe consequence in the event of incompatibility is premature termination of office or employment. It is typical for almost all legislations.

Under European law incompatibility is to be established by the electing or appointing body or another competent authority. For members of parliament and ministers this authority is the Parliament or the Constitutional Court; for mayors and municipal councillors – the municipal councils or municipal election commissions; for experts in various public administrations – their appointing body; for magistrates – the Supreme Judicial Council/Supreme Council of Magistracy, etc. The competent authority decides if there is incompatibility and orders the premature termination of office or employment after conducting the necessary proceedings. In the course of the proceedings the person concerned has to be notified and given the opportunity to defend himself/herself. The act terminating the term of office/employment due to incompatibility is subject to judicial review for legality.

The similarities between incompatibility and conflict of interest under European law lie in the fact that they are both in the field of anti-corruption, their presence can be established only after conducting the proper proceedings and require a legal basis – only those acts laid down by law shall constitute incompatibility/conflict of interest. Moreover, both phenomena constitute formal and not material offences.

There are also significant differences. Conflict of interest constitutes a criminal or administrative offence, whereas incompatibility constitutes a violation of a prohibition which results in unlawful conduct. Conflict of interest is always associated with active behaviour, whereas incompatibility is viewed as passive behaviour, i.e. it has not been terminated within a specified period of time provided that it has existed at the time of entry into office.

The two phenomena have different constituent elements. Conflict of interest always involves a conflict between the public duties and the private interests of a public office holder or a related party thereto, whereas incompatibility does not necessarily involve private interests. The penalties for conflict of interest rarely include premature termination of office or employment, while in almost all European countries this is the main penalty for violating the incompatibility prohibitions.

## **10. DECLARATIONS OF INCOMPATIBILITY, ASSETS AND INTERESTS**

The declarations of incompatibility, assets and interests form an integral part of administrative anti-corruption measures. The obligation to declare incompatibility is often laid down in the same legal act that regulates conflict of interest. There is a connection between the two legal phenomena, albeit an indirect one. The obligation to declare one's assets and interests prevents corruption and conflict of interest in several ways. When, upon entry into office, a public office holder declares his/her interests, he/she becomes aware in advance of the circumstances which may give rise to conflict of interest so that he/she can withdraw himself/herself from the performance of any official duties assigned to him/her due to conflict of interest. The annual declaration of assets, the verification of its accuracy and the publication of this declaration prevents and significantly impedes corrupt practices.

These declarations have a specific feature which significantly distinguishes them from conflict of interest. All public office holders are obliged to file a declaration at least once a year. This obligation is applicable to all accountable persons, whereas proceedings ascertaining conflict of interest are initiated in respect of no more than 0.1-0.3% of all accountable persons per year.

There are some differences between the declarations of incompatibility, assets and interests in different countries. These differences are related to the persons who are obliged to file them, their public disclosure, content, conditions for performing checks and penalties for not filing the necessary declarations.

The individuals who are obliged to file declarations are the same as the persons accountable under the conflict of interest regulation. It should be noted, however, that the list varies from country to country. In most countries the individuals who are obliged to file all three types of declarations are high-ranking government officials – the president, members of parliament, the prime minister, ministers, second-highest ranking officials in the executive branch, mayors, magistrates. These countries include France, Croatia, Slovakia, the Czech Republic, Finland, etc. In Germany, Great Britain and Hungary this obligation is incumbent only on members of parliament. In Poland and Spain this obligation applies to high-ranking elected local government officials and political appointees. In other countries, however, all public office holders (e.g. in Bulgaria, Latvia) are obliged to file declarations under different conditions relating to their disclosure.

The declaration is to be made on the declaration forms approved by the relevant competent authority. This unifies the procedure, facilitates the verification and ensures that all accountable persons are treated equally by the law. The authority to which these declarations have to be submitted varies from country to country. The options for declaration under the different EU legislations are as follows:

1. to a specialized body – commission, agency or bureau (e.g. in France, Poland, Romania, Croatia)
2. to the Council of Ministers for executive branch officials (e.g. in the Czech Republic)
3. the electing or appointing authority (e.g. in Latvia and in Great Britain the ministers file a declaration of interest with the Parliament)

## ***Conflict of Interest for Corruption and Abuse of Public Power***

4. to a specialized body as regards the declarations of assets and interest submitted by high-ranking public officials and to the electing or appointing authority as regards the declarations of incompatibility submitted by all public office holders as well all declarations submitted by experts in public administrations who are not public office holders (e.g. in Bulgaria).

These declarations have to be submitted within the time limit stipulated by law. It varies between one and two months and starts to run from the moment that public office holders take or, in some cases, vacate their office. Annual declarations of assets usually have to be submitted by a specific date for the previous year (e.g. 15<sup>th</sup> May, 30<sup>th</sup> June, etc.) Failure to file any of these declarations constitutes an administrative offence which is punishable by a fine.<sup>16</sup>

All countries have enforced requirements on the registration of the declarations, as well as prohibitions on their disclosure if they are exempt from the publication requirement. In France the disclosure of such confidential information constitutes a crime, and in the Czech Republic it is punishable by a fine and the matter is brought directly to the personal data protection authority to investigate the misuse of personal data.

The purpose of declaring different circumstances is for them to be published and brought to the attention of the general public in whose interest these public officials have to act. This allows for popular control over government. The declarations are published on the website of the competent authority collecting the declarations. The disclosure regimes vary.

Most countries disclose the declarations of high-ranking public officials (e.g. in Great Britain, France, Croatia<sup>17</sup>, Slovakia<sup>18</sup>, etc. Other countries (e.g. Latvia, Bulgaria<sup>19</sup>, etc.) disclose the declarations of all public office holders. In Russia, all data contained in the declarations under Article 19-20 of the Law on State Civil Service of the Russian Federation<sup>20</sup> are confidential. Their disclosure is punishable by law. Only data on officials appointed by the president or the government may be disclosed by their superior only to journalists.

Very few countries (e.g. the Czech Republic, Bulgaria<sup>21</sup>, etc.) verify the accuracy of these declarations. The verification is intended to check whether the information disclosed in the declaration corresponds to the information recorded in the relevant public registers. In the event of discrepancies or submission of false information, the relevant official is punishable by a sanction. In Bulgaria if there is a discrepancy in the declaration of assets and interests, the verifying authority has to notify the person concerned and give him/her 14 days to rectify the discrepancies. If the official fails to submit the declaration of assets and interests on time and to rectify any discrepancies within 14 days of being notified thereof, he/she shall be punished by a BGN<sup>22</sup> 20,000 fine and his/her assets shall be subject to an inspection in accordance with civil forfeiture laws (Nikolov, 2011).

There are different types of declarations:

### **Declaration of Incompatibility**

Few countries (e.g. Ireland, Bulgaria, Portugal, Russia, etc.) have introduced this declaration regime. It has to be submitted within a specified period of time from the entry into office. In this declaration the person who takes a certain public office declares that he/she does not hold any other incompatible public office in the public, private and non-governmental sector. Through this declaration public officials assess their own incompatibility at the time of entry into office and promptly eliminate the incompatibility in question. If the public official carries out a job or profession which is incompatible with his public



duties, he/she has to declare this fact and within a certain period of time of making this declaration of incompatibility he/she has to take the necessary steps to eliminate it or to declare it again before the competent authority.

## **Declaration of Assets**

In the declaration of assets public office holders have to declare both their own assets and the assets of three other groups of people – spouse, minor children and common-law partner. The assets that have to be declared include real estate property, limited real rights, movable property, cash, bank accounts, receivables and payables, shares in companies, income for the previous year, including the salary and income declared on the tax return, gifts, etc.

Most countries have three types of declarations of assets: preliminary declaration of assets (upon entry into office), annual declaration of assets and declaration of assets after termination of employment. The assets declaration regime is seen as a tool for combating corruption because the accountable person has to disclose not only the price at which the property has been acquired, but also the source of funding. When carrying out inspections of these declarations, the verifying authority can conclude whether the public official or a member of his/her family had the legal resources to acquire said assets.

Latvia has adopted a non-selective approach in its legislation which stipulates that all public office holders have to submit annual income declarations to their superiors<sup>23</sup>. In all EU Member States, except Germany, all members of parliament, members of the government, and local elected officials have to declare their assets.

Declarations of gifts and hospitality are either part of the declarations of assets or separate declarations. Gifts are subject to monitoring and inspections in most European countries because they are forms and signals of corruption. In Latvia declarations of gifts have to be submitted by all public office holders, including those who are not elected officials. In Bulgaria gifts received over the previous year are declared in the declarations of assets if the value of the gift received by the public office holder or a member of his/her family exceeds BGN 1,000. In Poland declarations of gifts have to be submitted only by local elected officials and political appointees, and in France and Hungary – only by members of parliament regardless of the value of the gift. British and German members of parliament have to declare gifts whose value exceeds 1% of their salaries and EUR 5,000. In both countries, apart from members of parliament, gifts also have to be declared by ministers and political appointees.

## **Declarations of Interests**

In these declarations public office holders have to promptly declare after entry into office facts and circumstances that could give rise to conflict of interest. This is a general declaration of interests. The purpose of this declaration is for the public office holder to declare shortly after taking office if he/she holds any shares in companies, is part of the managerial or supervisory bodies of legal entities, and other relationships and interest provided for by law that could give rise to conflict of interest if he/she exercises his/her powers or duties. The facts and circumstances that have to be declared are: shares of the capital of a company, participation in managerial and supervisory bodies of legal entities, contracts concluded between the public office holder and other parties, related parties whose interest could give rise to conflict of interest, etc.

Here are some interesting facts and good practices adopted in different countries.

Usually in these declarations are disclosed only the private interests of the public official, but in Great Britain in the declaration that they submit to their parliamentary secretary ministers also have to disclose the private interests of their spouses/partners and children, as well as facts about their constituency and partisan interests. In Slovakia every elected official has to declare not only his/her private interests, but also those of the political party it represents which are known to him/her.

In Finland, declarations of private interests are filed only by senior public officials in accordance with the State Civil Service Act, and in Latvia, Ireland, and Bulgaria such declarations are filed by all public office holders. In Latvia such declarations are also known as “declarations upon assuming office”. In Ireland these declarations are part of Annex II to the national law.<sup>24</sup> In Bulgaria the declarations of interest are part two of the general declaration of assets and interests approved by the specialized body. In the event that the circumstances disclosed in the declaration change in the course of the year, this change has to be declared by public officials to the relevant competent authority within a month of its occurrence (e.g. transfer of shares in a limited liability company, being elected chairman of an NGO, etc.).

### **Declaration of Interests in a Specific Case**

This declaration is a conservative way of preventing conflict of interest. It is an ad hoc declaration of private interests in relation to the exercise of specific duties. The modern way of preventing conflict of interest is for the public office holder to withdraw from the performance of the specific duty due to the presence of private interests, either his/her own or of a related party, in a specific situation or on a particular occasion. The declaration has to be submitted prior to or before the performance of the obligation, but not after its completion. It should be made in writing, but it can also be in the form of a statement, which means that the ad hoc declaration of private interests is deemed duly made if it has been recorded in the minutes of a session of a collegial body.

The list of individuals who have to submit such a declaration is quite varied. In France, Portugal and Hungary it is mandatory only for members of parliament, and in Germany and Spain – for local elected officials. In Great Britain high-ranking public officials, including members of parliament and local elected officials, have to submit such a declaration whenever they have private interests which could reasonably be considered likely, both by the interested person and others, to influence improperly the official’s performance of their duties.

## **11. RESTRICTIONS AFTER TERMINATION OF PUBLIC OFFICE**

The restrictions after termination of public office are a natural continuation of conflict of interest regulations after the term of office or employment ends. They both aim at eliminating the possibility of companies with ties within the public sector to gain an unfair advantage over other businesses and safeguard the principle of equality before the law. Both phenomena essentially constitute restrictions on the performance of certain activities stipulated by law to further the private interests of a public office holder, a former public office holder or a related party thereto. The main difference between them lies in the fact that unlike conflict of interest, these restrictions refer to individuals who no longer hold an office in the public sector, have the status of former public office holders and consequently do not exercise their powers or duties to further their private interests, but operate in the private sector.

Another reason for the introduction of these restrictions is to eliminate the risk that the public office holder may perform their official duties in favour of a private business in order to secure preferential treatment to get a job in said company after the end of his/her term of office.

There is an interesting development with regard to the individuals who have to comply with these restrictions. Traditionally, such individuals include former public office holder in their capacity as natural persons. In Spain, Portugal and Poland only those individuals who have held positions as political appointees have to comply with these restrictions. In Bulgaria these restrictions apply to both public office holders and experts in public administrations in the three branches of power and local government units. In Latvia the restrictions are applicable to chairmen of municipal councils, municipal councillors, mayors and state officials who have been responsible for the monitoring and penalizing corruption in public procurement procedures for the supply of goods to state and local government bodies.

Bulgaria has recently introduced in its legislation a restriction banning all legal entities in which a public office holder who is involved in public procurement procedures or EU fund absorption procedures has shares or is a manager or a member of a managerial or supervisory body from participating in said procedures.

These restrictions are not indefinite. The restriction period adopted in different European countries varies from one to five years. In Poland, the Czech Republic and Bulgaria these restrictions apply for a period of 1 year, whereas in Great Britain, Russia and Latvia they remain in place for two years, and in France – for five years.

Some countries (Bulgaria, Poland and the Czech Republic) have set a precondition which triggers these restrictions, namely if in the last year of office, the public office holder has performed any actions involving disposition, regulation or control or has concluded any contracts with said company. In this case the restrictions apply only to the company in relation to which said duties have been performed. In other countries such conditions do not exist and the restrictions apply to all.

The restrictions after termination of office have four different manifestations in European legislations:

### **Restriction on Holding Shares of the Capital or Pursuing a Career in a Private Company**

Former public office holders may not

- be partners, acquire stocks or shares,
- be managers, members of the managerial or supervisory bodies, or
- be conclude employment or consultancy contracts with a company in respect of which they have performed any public duties (e.g. in Bulgaria,<sup>25</sup> Poland,<sup>26</sup> the Czech Republic, Latvia, Spain, Portugal, etc.). France has enforced strict regulations on the employment of public office holders after termination of office. In Great Britain state officials have to report every job offer they receive, including those made by NGOs.

### **Restriction on Participation and Representation in Two Financial Procedures**

The public office holder may not participate or represent a natural or legal person in any public procurement or EU fund absorption procedures before the institutions where he/she has been employed.

## **Restriction on Employment in Private Companies Operating in Specific Sectors**

If in his/her capacity as a public office holder he/she has been responsible for supervising these sectors – energy, public procurement, nuclear energy, telecommunications (e.g. in Italy, Spain, etc.).

## **Restrictions on Companies Where Former Public Office Holders Are Employed**

In case former public office holders who are members of the managerial or supervisory bodies of these companies or hold shares of the capital, such companies may not receive subsidies from the state budget or be granted debt relief (e.g. in Slovakia). In Bulgaria, such companies may not participate in public procurement or EU fund absorption procedures carried out by the institution where the former public office was employed if said public office holder was involved in such procedures in the course of his public duties.

## **12. CONCLUSION**

This overview of the various aspects of conflict of interest regulations leads to several conclusions. The regulations enforced by different legislations differ in detail, but have the same main elements in common. Each country's conflict of interest regulation contains a list of accountable persons that have to comply with the conflict of interest regime and related regimes /incompatibility, declarations and restrictions after termination of office/. Each list includes high-ranking public officials in the respective country and has a different approach to including experts to the list of accountable persons under relevant national legislations.

The fact that there are two different approaches adopted by national legislators, namely to define conflict of interest as an administrative or a criminal offence, does not influence the main conclusions that for European societies and the legislators that represent them conflict of interest constitutes an illegal act that contravenes the main legal principles coined on the continent, such as sovereignty, separation of powers, equality of citizens before the law and rule of law.

The two aspects that have the greatest similarities are the specific prohibitions whose violation results in conflict of interest, and the declaration regime applicable to every public office holder.

Conflict of interest regulations are a main tool for citizens to exercise control over the government and to fight corruption. The alert, which is the most common ground for instituting proceedings for ascertaining and sanctioning conflict of interest, can be submitted by a citizen or an organization that has evidence of conflict of interest even if their rights or legitimate interests have not been directly or indirectly affected by said conflict.

The differences in the structure and composition of the supervisory bodies and whether they are specialized /commissions, agencies, bureaus/ or classic /prosecutor's office, court/ depend on the time this matter was regulated in the national legislations. The newer the regulation, the more common it is for the function of ascertaining and sanctioning conflict of interest and verifying the declarations to be assumed by a body with special competence.

An interesting aspect is the increasing number of obligations<sup>27</sup> imposed on legal entities which are somehow related to public office holders and the pecuniary sanctions for non-compliance.

The introduction of the figure of the ethics officer and the increasing number of prior authorizations required by the supervisory body are strong new measures for conflict of interest prevention, which has always been a priority on the European continent. A somewhat perplexing aspects is the inconsistent policy of many legislators as regards the disclosure of all declarations submitted by high-ranking public officials and the verification of the accuracy of these declarations.

In conclusion, it can be said that despite the differences in national traditions and legislative techniques, the different national regulations are in the process of being unified.

Conflict of interest is not a classic financial crime. Practice shows that conflict of interest most often involves showing favouritism towards one's own business or a family business and generating benefits for the public office holder and his/her related parties. Such abuses of power arising from conflict of interest often have six- or seven-figure dimensions. More importantly, conflict of interest undermines fundamental principles of modern society and state. Therefore, regardless of whether it is defined as an administrative or a criminal offence, conflict of interest and the fight against it is a vital part of the anti-corruption measures of the modern state.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in his personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task

## **REFERENCES**

- Alibert, R. (1926). *Le controle juridictionnel de l administration au moyen du recours pour excès de pouvoir* [Judicial control of the administration by means of the appeal for abuse of power]. Payot.
- Cambell, L. (2007). Theorising asset forfeiture in Ireland. *The Journal of Criminal Law*, 75(11), 441–460.
- de Laubadere, A., Venezia, J. C., & Gandement, Y. (1991). Traité de droit administratif [Treaty of Administrative law]. *International Comparative Law Review*, 43(4), 941.

## **Conflict of Interest for Corruption and Abuse of Public Power**

Funk, W. F., & Richard, H. S. (2005). *Administrative Law. Examples and Explanations*. Aspen Publishers.

Nikolov, N. (2011). General characteristics of civil forfeiture. *Journal of Money Laundering Control*, 14(1), 16–31. doi:10.1108/13685201111098851

Rafay, A., Sadiq, R., & Ajmal, M. M. (2016). The Effect of IAS-24 Disclosures on Governance Mechanisms and Ownership Structures in Pakistan. *Lahore Journal of Business*, 5(1), 15–36. doi:10.35536/ljb.2016.v5.i1.a2

Sodan, H. & Ziekow, J. (2005). *Grundkurs öffentliches Recht* [Basic course in public law]. Verlag C.H.Beck oHG.

Strauss, P. L. (2002). *Administrative justice in the United States*. Carolina Academic Press.

Zolkafilil, S., Nazri, S. N. F. S. M., & Omar, N. (2021). Factors Influencing the Outcome of Money Laundering Investigations. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

## **ADDITIONAL READING**

Nikolov, N. (2013). Conflict of interest in European public law. *Journal of Financial Crime*, 20(4), 406–421. doi:10.1108/JFC-06-2013-0042

## **ENDNOTES**

<sup>1</sup> In the ancient Roman Republic, the consuls had executive power and exercised *imperium domi*. Their power was not absolute and the following mechanisms were put in place to prevent power abuse: (1) there were always two consuls elected in power at any time; (2) they served for only one year – from 1 January to 31 December; (3) they were elected by the citizens of Rome who had the right to vote; 4/ the next consul elections were held on 1 July, so the successors who were to fill the place of the current consuls were known to the public halfway through their term; 5/ their work was controlled by the Senate, which met on a daily basis, etc.

<sup>2</sup> Corruption in the widest sense of the term includes both corrupt practices that are punished and prosecuted under criminal law and procedure, as well as those that are punished and prosecuted under administrative law and procedure.

<sup>3</sup> Italy is a notable exception in that respect.

<sup>4</sup> There are some differences. In some countries (Hungary and Croatia) only the presidents of Supreme courts and the Prosecutor General are obliged to comply with the conflict of interest regulation and make disclosures, but ordinary judges and magistrates are not.

<sup>5</sup> This issue will be discussed in greater detail in the sanctions section.

<sup>6</sup> Decision No 2513/21.02.2013 of the Supreme Administrative Court of the Republic of Bulgaria in case No 12061/2012 and Decision No 6148/8.05.2013 of the Supreme Administrative Court of the Republic of Bulgaria in case No 1781/2013.

- 7 In force since 2006.
- 8 In force since 22.01.2018.
- 9 Since 2014 when passing judgement in court cases the Bulgarian Supreme Administrative Court has upheld its opinion that in order for conflict of interest to arise, the person has to realize personal gain or benefit. The court has held that when a minister has tabled a report at a meeting of the Council of Ministers and has taken part in the adoption of a decision based on that report on the award of a mining concession to a company in which he/she is a shareholder, this should create conflict of interest in spite of the fact that at the time when the offence has been ascertained by the administrative authority and when the court passed its judgement no contract has been concluded between the company and the state.
- 10 In such cases the group of related parties shall be defined according to case law.
- 11 For more information on individual administrative acts (de Laubadere, *et al.*, 1990)
- 12 There are a number of national specifics when it comes to meetings and sessions. For example, in Bulgaria the Commission for Anti-Corruption and Forfeiture of Illegally Acquired Assets always meets in closed session. In Croatia the sessions of the Conflict of Interest Commission are always open to the public and can be attended by citizens and media representatives.
- 13 §7, para 4 of the Administrative Procedure Code (supplemented in 2006).
- 14 Slovakia has had mixed success in implementing these restrictions. In 2014 out of 133 mayors acting also as managers in private business, only 4 were fined by the Local Assemblies. In 2015 44 mayors were still acting as managers.
- 15 In Portugal, companies in which a public office holder or a related party thereto hold more than 10% shares of the capital cannot take part in public procurement procedures for the supply of goods, works or services to state bodies.
- 16 In Bulgaria, failure to submit any of the declarations of assets and interests on time results in a subsequent inspection of the origin of the assets of the public office holder acquired over the last 10 years.
- 17 In Croatia, the declarations submitted by judges and prosecutors may in certain cases be made public.
- 18 In Slovakia, the declarations of mayors and municipal councillors were exempt from disclosure which was subsequently overruled by the Supreme Court in 2016.
- 19 In Bulgaria, both the declarations of assets and the declarations of interests of high-ranking public officials are published. As regards the other officials who are required to file declarations, only the second part of the declarations /declarations of interests/ are made public.
- 20 In force since 1 May 2009.
- 21 The accuracy of the declarations of assets and interests of high-ranking public officials is always subject to verification, unlike their declarations of incompatibility. The accuracy of the declarations of incompatibility of other public office holders is always subject to verification, unlike their declarations of assets and interests whose accuracy is verified only in three exceptional cases: upon the submission of a report about corruption or conflict of interest, upon disciplinary proceedings relating to cases of corrupt practices, and when the risk of corruption is high in the department where the person concerned works.
- 22 Bulgarian Lev – The currency of Bulgaria
- 23 This income declaration regime in Latvia has been introduced in order to enforce the general rules on civil servant salaries implemented with the Law on Prevention of Conflict of Interest in the

### ***Conflict of Interest for Corruption and Abuse of Public Power***

Activities of Public Officials effective since 10.05.2002. While they hold public office, they may not receive any dividends paid on stocks and shares in companies or on any other type of securities. When a member of parliament also acts as a minister, parliamentary or state secretary, he/she may receive a salary for only one of the two positions held.

<sup>24</sup> An interesting characteristic of the Irish declaration of interests is that public officials have to declare silent partnerships.

<sup>25</sup> Bulgaria has enforced all three restrictions, whereas the other countries – only one or two.

<sup>26</sup> In Poland, a former public office holder may be appointed to such a position in the private sector only after obtaining proper authorization from the competent state authority.

<sup>27</sup> The obligation to request authorization from the supervisory body to conclude certain contracts, the obligation to comply with the restriction not to conclude public procurement and EU fund absorption contracts if a former public office holder who used to work in these spheres holds shares in the company or is part of the company's management.



## Chapter 8

# Regulatory Ambiguity: The Underbelly of Insider Trading

**Laura Pinto Hansen**

*Western New England University, USA*

### ABSTRACT

*Ordinarily “black money” is considered a part of illegal transactions involving cash payments. However, in the case of illegal insider trading, illegal profits are often hidden in the purchase of luxury items and financial investments through offshore accounts. Aiding in this particular white-collar crime is the ambiguity of regulation, often dependent on the political whims of whatever party is in office at the time. Adding to the confusion is the fact that in some cases, “insider traders” are acting legitimately, as in the case of senior executives with stock buying options within their compensation or with lower-level employees participating in employee stock ownership programs (ESOPs). Though there are exhaustive ways by which illegal trading information is passed around, there are certain industries, including finance, that lend themselves to greater risk for employee involvement in illegal insider trading. This chapter includes discussions of mergers and acquisitions frenzies, as well as hedge funds and their contributions to illegal insider trading.*

### INTRODUCTION

White collar crime, unlike “conventional crime”, has always been more difficult to control. Yet it is conventional crime (e.g. homicide) that is headline grabbing. There are far more financial losses every year as a result of white collar crime, than all conventional crimes combined (Hansen, 2021). Yet as Georg Simmel observed (1990), money is an abstraction, with arbitrary and subjective meaning to people. It has properties of invisibility and secrecy (Simmel, 1990). When someone has been a victim of a robbery of cash, it is not uncommon for the sympathetic to say something along the lines of, “It’s only money. At least you didn’t lose your life.” For most people, they are more likely to be fearful of becoming the victim of a violent crime than a financial crime (Hansen, 2021).

For the white collar criminal, as in the case of conventional drug dealers, illegitimate financial gains have to be hidden from authorities. One of the biggest mistakes that any criminal can make is to spend

DOI: 10.4018/978-1-7998-5567-5.ch008

## **Regulatory Ambiguity**

money on luxury items like fancy cars and large homes, when there does not appear to be a legitimate means to support that type of life style. In the case of white collar criminals within the financial sector, most have access to information on how to squirrel away money from criminal enterprises in less conspicuous places.

Within this chapter, we will explore the nature of the crime of insider trading and how the regulatory environment can either inhibit or enable elite criminals. It is the very ambiguity of regulation that assists in the crimes occurring in the first place, plus aids in criminals hiding money in places beyond the reach of regulators. Regulation is every bit a political beast, dependent on the whims of those holding political office, even when it operates within alleged independent agencies. Though in theory ran by non-partisan employees of the government, as in the example of the United States Securities and Exchange Commission (SEC) that are the first to investigate and oversee insider trading cases, regulatory agencies are subject to the whims of partisan politics.

Additionally, we will examine some of the market conditions that create more opportunities to commit insider trading. These include trends that gain popularity from time to time, as in the case of mergers and acquisition frenzies or certain investment instruments, like hedge funds. In some cases, these trends go unabated until an apparent crime has been committed, in which case there is regulatory reaction.

We should also consider that individuals are not the only ones that are difficult to regulate. Corporations likewise can offend, when there is irregularities in their reporting of real income (Hansen, 2020). In fact, corporations, and the whole financial industry for that matter, can set up a cultural environment where playing by the rules (in this case, regulations) is viewed as playing it too safe (Hansen, 2021; Hansen and Movahedi, 2010).

Whether regulatory agencies vaguely or concretely try to prevent financial white-collar crime from happening, it occurs all too often. And because anyone who commits a financial crime, at least the smart ones, do not want their ill-gotten proceeds to be detected, it requires them to hide the money. This may mean money laundering or securing the funds in offshore bank accounts, where there is even less rigorous regulatory oversight (Lokanan & Chopra, 2021; Rafay, 2021). It may also mean hiding the funds within the Dark Web, with cryptocurrency. One way or another, the money can often end up as part of an underground economy and black money revenue streams.

## **Insider Trading Defined**

Insider trading is defined as the illegal buying and selling of investments, including stock, based on information that has not yet made public. If we stick with Sutherland's (1939) strict definition of white-collar crimes occurring within the context of one's occupation, then insider trading does not neatly fit this typology. We can speculate that much of insider trading does happen as a direct result of access to privileged information, particularly in financial institutions and companies intimately involved in research and development, as well as the banking industry in general (Rafay *et al.*, 2016). However, we can't discount the fact that individual investors may also benefit from insider information and may act on it in advance of public notification of changes that might affect investments.

By strict legal definition, insider trading is defined more narrowly and more closely mirrors the essence of Sutherland's original definition of white-collar crime:

*Illegal insider trading generally occurs when a security is bought or sold in breach of a fiduciary duty or other relationship of trust and confidence while in possession of material, nonpublic information. (SEC, n.d.)*

There are few types of financial crimes that are as difficult to define as definitively white collar crime, much less prevent, than insider trading. What makes it all the more confusing is that there are legitimate insider traders. For instance, a CEO or owner is not prohibited from buying and selling stock in their own company, in fact many times compensation packages include stock options for senior executives. There are also stock option plans for employees (ESOPs) where anyone in a company can invest in it as part of their benefits. The philosophy behind any internal stock option program, whether for executives or any employee, is that they will show more loyalty and be more motivated in their jobs, if they have financial investment in their company.

However, ESOPs again runs the risk that employees could conceivably have insider information and illegally buy or sell stock in the company outside of their employee compensation plans, based on information that has yet to be reported publicly outside the company. Like in the case of senior executives, any transactions ESOP participants make are only legitimate if they are conducting trades based on information that has already been made public.

There is another type of insider trader who learns insider information indirectly. An example of this would be the Martha Stewart case, where securities fraud charges were made by the SEC against her and her former stockbroker, Peter Bacanovic (SEC, 2003). In the charges, Bacanovic was alleged to have given Stewart insider information about the pharmaceutical company, ImClone, that Stewart had investments in, just before the stock was anticipated to plunge on the disappointing news that a promising cancer treatment would not receive U.D. Food and Drug Administration (FDA) approval. To demonstrate just how challenging it is to prosecute these cases, Stewart ultimately pled guilty only to obstruction of justice charges. Of course, we cannot discount the privilege of having the ability to afford the best legal representation in negotiating the best plea bargain possible.

What we should note with the Stewart case is the intersectionality of white collar crime and gender. Women are generally more risk-averse, not as impulsive as men, with jobs that offer fewer opportunities to manage or operate businesses where white collar crimes are more likely to occur (Liu and Miller, 2019; Huffman, *et al.*, 2010; O'Fallon and Butterfield, 2013; Byrnes, *et al.*, 1999; Daly, 1989; Adler, 1975; Simon, 1975). So, in our discussions of illegal insider trading, as well as hiding money made from it, like other white collar crimes, males predominately are the guilty parties. However, as insider trading is as ambiguously committed as it is regulated, the true numbers are not known, nor the actual disparity between male and female insider trading criminals.

Illegal trading does not happen randomly, but rather purposefully. Insiders who stay within the law and regulations, avoid making profitable trades or sell stocks in companies they have intimate information on prior to any public disclosure. However, insider traders who operate outside the law will sell stocks in advance of the release of bad news and purchase stock in advance of an anticipated rise in prices when there is good news.

Company insiders are not the only ones who possess insider information. Another potential for illegal insider trading is within regulatory agencies and political offices. For instance, if someone at the Federal Drug Administration (FDA) knows that a drug is going to be approved in advance of the information being made public, they could potentially purchase stock in that company before any announcement is made, gambling (rightfully so) that the stock prices will go up. This is not a farfetched idea, as given

## **Regulatory Ambiguity**

the example of Gordon Jackson, who entered a settlement agreement with the SEC in 2016, after admitting to participating in an insider trading scheme, while working for the FDA (*Securities and Exchange Commission v. Sanjay Valvani and Gordon Johnston*, Civil Action No. 16 Civ. 4512, U.S. SEC, 2016).

## **Criminological Theories to Explain Insider Trading**

We should start by dismantling the myth that greed, or fear for that matter, is an individual trait. Like a number of other white collar crimes are thought to be single acts by desperate individuals. This could not be further from the truth when understanding the financial crimes committed by Wall Street elites where it is more likely to occur within social and professional networks (Hansen and Movahedi, 2010).

In the social and cultural climate of Wall Street, both feed on people as a contagion. This is not to say that there are some individuals who act alone. However, the greater majority of cases reported involve conspiracies of two or more people (Hansen, 2021). The collective greed can be encouraged, as demonstrated in the fictional story of Gordon Gekko in the movie *Wall Street* (20<sup>th</sup> Century Fox, 1987) or by the real-life biography of Jordan Belfort in *The Wolf of Wall Street* (Belfort, 2011; Hansen, 2021).

According to Kolhatkar (2018), a former hedge fund analyst, there are two types of people attracted to Wall Street professions:

- The offspring of wealthy parents who attended the “right” prep school, obtained an Ivy League education, who once on Wall Street, immediately fit in. Fall in the category of “trust fund babies”, who do not rely on their jobs necessarily to accumulate personal wealth.
- The second type is described as “street smart” and “scrappy”, coming from modest means, with parents who worked hard all their lives with little to show for it. They more than likely attended public schools and universities. They can be ambitious out of resentment and see their success as a form of payback, want to be filthy rich, or both. There is no trust fund to fall back on.

Add to Kolhatkar’s typologies the driving forces of greed and fear, it can make for a potential criminological cocktail for insider trading.

Other explanations to explain insider trading include *Normalization Process Theory* (Foucault) where “bad” behavior becomes “business as usual”, when a whole group or in this case, culture within financial institutions that handle securities, has neutralized the moral code (Donaldson, 2012). In fact, it becomes a near impossibility to get anyone to return to more ethical behavior and follow regulations to the letter of the law, once malfeasance becomes normative (Hansen, 2021).

Finally, in conjunction with *Normalization Process Theory*, we should consider the role of victim neutralization theories in explaining why insider trading occurs. As ambiguous as the regulations are, likewise the face of the victim. Likewise, we should consider classic *Rational Choice Theory* (RCT), where the reward of acting on insider information illegally, outweighs the perceived possible punishment as well as possible harm to the public who do not possess the same information and cannot act on it to further enhance or preserve their own investments.

## **Regulatory Environment: The Ideal**

Regulatory agencies make up the frontline defense against rule and law violations. As Gunningham (2015) suggests, “Regulation is one of the most important mechanisms used to curb white-collar and

corporate crime....” Regulatory agencies do not operate in silos. In other words, they don’t live in an independent vacuum. In the United States, many regulatory agencies are an extension of the Executive Branch of the government. As we have noted, in theory, regulatory agencies should be non-partisan. In reality, they are dependent on whatever political party is in power at the moment for funding, staffing, and support for regulatory enforcement efforts.

Regulatory agencies, including the SEC, primary function is to make sure that the public, consumers, and customers, including the government, are not taken advantaged of or put in harm’s way. For instance, as the health of the environment, and in turn, the health and welfare of all living things on earth became a concern after the Industrial Age, there were social movements to address the problem of increased pollution in the air and water. The environmental protection movement of the 1960s and 1970s pushed for regulation, which in turn gave birth to a number of acts passed in Congress, as well as the formation of the Environmental Protection Agency (EPA). Similarly, there have been a number of laws and regulations put into place after the Great Depression, insider scandals of the 1980s, and more recently, after the 2008 “Great Recession” caused partially by the bust of the home mortgage industry.

U.S. laws and regulations protect investors in one primary way. All traders, including investors, are prohibited to profit from private information, based on Section 10b5 of the Securities Exchange Act of 1934 (White, 2020). A second protection is the *short-swing profit* rule that requires that company insiders are required to return profits made from purchase or sale of company if both occur within six months of one another (Lewis, Park & Berkowitz, 2013). Though it begs the question of how many of these short-swing profit transactions are detected.

## **Securities and Exchange Commission (SEC)**

In existence for nearly 100 years, the Securities and Exchange Commission (SEC) was formed during the Great Depression that was spurred on by the collapse of the stock market in 1929. Besides other measures to protect investors’ money, the SEC was given the authority to regulate capital markets. The authority of the SEC has evolved over time, ebbing and flowing on the basis of changing international markets. The current primary functions of the SEC, based on its mission statement is “to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation.” (Atkins & Bondi, 2008; SEC, 2006)

The SEC has to walk a fine tightrope between the demands of industry, investors, and whatever political party is currently in power. The SEC professionals themselves are, in theory, apolitical. Their employment is not dictated by political party, but rather their qualifications in financial investigations. However, the appointment of the head of the SEC at any given time is anything but apolitical.

As Coffin reports (2017), the first employees of the SEC were eager young professionals who believed that criminals in the financial system needed to be stopped. By the 2000s and on the heels of the scandals earlier in this century, including Enron and Bernie Madoff, the SEC seemed to be poised for reform where even the most minor offenses would be prosecuted, in order to deter larger ones from occurring (Coffin, 2017). The election of Donald Trump in 2016 marked the end the push for these reforms, as being part of the Republican Party that historically pushes for less regulation, and the changes to how the SEC operates never materialized (Coffin, 2017).

More recently it has been reported that SEC enforcement of insider trading laws has diminished dramatically under President Trump. Though Jay Clayton, then chairman of the SEC pledged at his confirmation hearing that there is no room for malfeasance in capital markets, the number of insider trading investigations and charges under his leadership (and that of Trump’s) dropped to levels that have

## ***Regulatory Ambiguity***

not been seen since the Reagan administration, another era where there was a sharp increase in illegal insider trading activity, as witnessed by the likes of Dennis Levine and Ivan Boesky (Dreisbach, 2020). In 2019, there were only 46 charges of insider trading, as compared to the over 160 charges made by the SEC in 1998, under President Clinton (Dreisbach, 2020). Again, we cannot emphasize enough that any ill-gotten gains from investments many times have to be hidden and becomes part of the underground economy, further encouraged in the face of diminished interest by the SEC to investigate insider trading.

## **10-Q and 10-K Filings**

For the uninitiated, 10-Q filings are mandatory quarterly reports to the SEC that reveal a lot of information about the financial health of publicly trading companies. 10-K filings are yearly reports that similarly to the 10-Q are required by the SEC. Unlike income tax filings, there is far more information on the 10-Q and 10-K filings. As the SEC reports (SEC, n.d.), the “Form 10-Q [and 10-K] includes unaudited financial statements....” There is where one danger lies. Audits provide, in theory, an objective and unbiased examination of financial statements that might be able to detect any red flags, including those detected within the personal portfolios of key officers in a company.

There is some evidence that illegal insider trading actually is infrequent just prior to the release of 10-Q and 10-K filings to the public. Even though insiders have the discretion, however misguided, to trade information that has yet to be publicly disclosed, the threat of professional or legal sanction, coupled with concerns for possible shareholder class-action law suits against them in civil court, appear to offer some deterrence to illegal trading (Huddart, Ke & Shi, 2007). However weak the correlation is between insider trading and release of filings or public earning statements, it does not mean that the criminal behavior is all together absent.

## **Compliance**

Individuals are not always to blame for regulations being ignored. Organizations, companies, and corporations might be encouraging employees to ignore regulations if it is hurting the bottom line of profits. In less nefarious cases, the organization is clueless as to the letter of the law with regulations under which they are expected to operate. Compliance to regulations is only as good as the management that chooses to follow them. Or not to follow them.

In recent decades, compliance has become a growing field within finance (Hansen, 2021). Companies, for the most part, do not wish to ruin their reputations with crimes being committed within their organization, including insider trading. If for no other reason than appearances, compliance officers are now a regular fixture in financial institutions, acting as watch-dogs in their companies. As laws and regulations change, it is their responsibility to keep administrators and employees apprised of these changes.

## **Self-Regulation**

One means by which to control illegal insider trading behavior is professional organizations. There is the real possibility that some individuals may be non-compliant with regulation due to ignorance or carelessness. Or due to an “everybody’s doing it” mentality. By requiring individuals to possess licensing in order to sell securities, this negates most claims of not knowing the law.

Professional organizations, like those for financial advisors and brokers, have within their means to sanction non-compliance members. For example, certified financial planners (CFPs) go through extensive training in order to pass exams required by law to sell securities. If they have not kept up with training, they run the risk of losing their licenses. If they break the law, it may mean losing membership, a suspension of a license or permanent forfeiture, depending on the outcome of a court case and deliberation of the professional organization, like the Certified Financial Planner Board of Standards.

In some cases, similar to the American Bar Association for lawyers, sanctions do not go further than the professional organization. It is not always in the best interest of professional organizations to refer to law enforcement or regulatory agencies, except in extreme cases of malfeasance, as scandals reflect badly on the organization in general. It is, however, difficult to keep financial wrongdoing secret, only revealed in the confines of the professional organization. In the age of cyberspace, news spreads fast, and reputations of individuals and professional organizations can be tarnished nevertheless.

## **Regulatory Ambiguity: The Reality**

As much as the regulatory environment in financial markets is meant to keep investors and advisors in line, there is a considerable amount of confusion. Regulatory ambiguity, as described in this chapter, is the extent to which laws and regulations are vague, subjectively interpreted, or selectively enforced. This means that some white collar offenders are punished and others are ignored. We have to look at the reality that regulation, at its best, is ambiguous and inconsistent. Much of this inconsistency is due to the political and economies of a free market system. As Chomsky and Pollin noted in an interview about a capitalist society and its relationship to the slow government response to the COVID-19 virus in the United States, government interference in business is viewed as “bad” and inhibiting to free market systems (Polychroniou, 2020).

Even though insider trading prohibition is clearly spelled out in the Securities and Exchange Act of 1934, there was little in the way of real enforcement of the insider trading provisions until the 1960s. Any interest in academic research on the ambiguity of regulation has been spotty, similarly to the enforcement of regulations themselves. There have been a number of debates among economists and financial market experts as to whether insider trading should even be a crime. That in itself makes the laws ambiguous. One argument is that insider trading provides more informative stock prices, the opposing side arguing that it limits the gains that outsiders might be able to realize if they had the same information (Fernandes & Ferreira, 2009).

The other concern for the actual effectiveness of insider trading regulation is that there are, in some cases, exceptions argued and won in court cases. In the case of the short-swing profit rule (Section 16, Securities Exchange Act of 1934), it was undermined when in the case of *Gibbons v. Malone*, a court of appeals determined that purchase and shares within a six month period was not prohibited in the case of trades of investments in different stocks within a single company (United States Court of Appeals, Second Circuit, 2012).

Also contributing to regulatory ambiguity is in the way in which inspections and audits are conducted (Khan, *et al.*, 2020; Ramzan, *et al.*, 2020). Without criminal forensic auditing, particularly of stock portfolios, it is too easy for offenders to pass off financial irregularities as accounting errors. Or to claim ignorance all together, as we witnessed with Andrew Fastow’s defense in the Enron case. For those of you less familiar with the Enron case, key executives sold off their personal stock in the company in advance of the public being informed that there were serious, criminal accounting irregularities within

## **Regulatory Ambiguity**

the company. Just after the announcement and the predictable bankruptcy filing took place, Enron's stock plummeted, paying only pennies on the dollar for shares of stock.

In reaction to the Enron scandal, U.S. Congress acted to address the failings of regulations across the board in corporate America. The Sarbanes-Oxley Act (2002) included provisions so that Chief Financial Officers (CFOs) in the future, like Fastow, cannot make the claim that they were clueless to the accounting and financial reporting malfeasance. However, since the Sarbanes-Oxley Act was passed, there continues to be an effort by some in political office and on Wall Street to loosen the regulations that were put in place with the 2002 legislation.

Adding even further confusion is the historical ambiguity within the court systems. In particular, the criminal court system is somewhat straight jacketed by political pressures when it comes to the discretion to prosecute white collar criminals vs. "conventional" criminals. Hagan, Hewitt & Alwin (1979) that the American criminal justice is a "loosely coupled system" with judges not ruling or governing, but rather managing the wishes of others outside of the system. This can include politicians and pressures from Wall Street.

Whether is viewed as political or apolitical, the SEC is not completely passive in recommending ways by which to make the laws clearer. In 2000, the agency implemented new rules to address three issues:

*The selective disclosures by issuers of material nonpublic information; when insider trading liability arises in connection with a trader's 'use' or 'knowing possession' of material nonpublic information; and when the breach of a family or other non-business relationship give rise to liability under misappropriation theory of insider trading. The rules are designed to promote the full and fair disclosure of information by issuers, and to clarify and enhance existing prohibitions against insider trading. (SEC, 2000).*

The caveat to the new rules was is that detractors continue to argue that the rules are unnecessary as the insider trading regulations are adequate without them. So, the pushback continues against the efforts to clarify existing insider trading laws.

Added to the mess is how the insider trader is defined and where liability of criminal activity lies. If strictly interpreted, as in Sutherland's definition of white collar crime, an insider trader is only liable if they are also violating a fiduciary responsibility. Based on this interpretation, only those who are placing the trades, including stock brokers, are liable for prosecution in insider trading cases. It is only recently, as addressed later in this chapter, that passing information on insider information by anyone is subject to criminal liability. Along with individuals who act on that insider information, even if they are not technically insiders themselves. Yet it was an impossibility to convict Martha Stewart. In a more recent case of insider trading, the golf pro Phil Mickelson was investigated, but not convicted on insider trading when his gambling buddy, William Walters was convicted on securities fraud and wire fraud, which included jail time (SEC, 2018). Yet allegedly Mickelson benefited from the insider information that Walters shared with him.

## **Insider Trading and Black Money**

If we take the stereotypical Hollywood movie image of a criminal who has made a lot of money, in particular, cash, from their crimes, they have to have a place to put all that cash. They might be depicted as purchasing expensive homes, cars, and jewelry, which we have already established is one of the most



foolish ways to hide it, as it sends up a red flag to investigators. Some criminals might be depicted purchasing expensive art works in a fictional movie or book, of which there will always be a real life black market for stolen or forged goods.

In all reality, individuals working in financial institutions, are more likely to be cautious of how they spend their money, as most, if not all, are aware of the pitfalls of a paper trail. As a result, their purchases and where they put their money from insider trading are more covert operations. Any flashiness that they may display in their lifestyle choices can be passed off by their legitimate successes within their careers, within reason.

Some insider traders do not trade directly under their own names, nor do they store the illegal proceeds from their trades in domestic banks on U.S. soil. There are so many jokes about offshore banking and for good reason. For instance, if a wealthy person anticipates a messy, expensive divorce where no prenuptial agreement exists, they may try and hide their assets in an offshore bank and downplay their true financial position. Even in the most stable of marriages, financial infidelity may be happening, including stock transfers, secret bank accounts or safe deposit box, credit cards, even real estate transactions.

More nefariously, dictators and depots from Hitler to Mobutu have been suspected of using Swiss banks in order to launder billions of dollars stolen from people during their leadership (Komisar, 2003). As Komisar (2013) advises within her investigative reporting of financial crimes: "Follow the money offshore."

Another common use of offshore accounts is to avoid paying taxes. This in itself is murky as far as regulation goes. Again, we run into the issue of inconsistencies across international borders. In theory, the prohibition of section 7201 of the Internal Revenue (IRS) code dictates that it is a felony for anyone to avoid paying taxes to the United States Government agency (Workman, 1982). The reality is that offshore tax havens are erratically regulated by their host countries (Hansen, 2021). Because of this, the full magnitude of just how much illegal use of offshore tax havens is unknown (Workman, 1982). Even with the electronic footprint of banking transactions, the actual dollar amount of lost tax revenue to the IRS is still a mystery.

There is a second reason why profits gain from illegal insider trading is hidden. Some white collar criminals wish to shield their families from legal fallout in the event that they are caught. In the case of Bernie Madoff of Ponzi scheme fame, his wife was not charged with criminal fraud as she was allegedly left in the dark about his crime, even though she did have to forfeit some \$75 million (USD) in assets, including a New York City townhouse that was deeded in her name (Cohn, 2018). Spouses and offspring are no doubt always investigated in the case of financial crimes, as they may possibly be helping to hide assets earned through criminal enterprises.

Offshore banks have historically offered tax shelters for the wealthy. Though notorious for charging high fees and commissions, these are no way near the dollar amounts that the IRS would levy on investment gains. We should note that in recent years, capital gains tax laws have become friendlier to investors. However, these laws ebb and flow, with some administrations pushing for greater tax revenue from capital gains; others pushing for deregulation and lower capital gains taxes. So much is dependent on the political environment as to how much the government can extract from capital gains on investments.

One of the biggest insider trading network schemes fell apart due to a diligent banker at Merrill Lynch. Suspecting an unusual transaction occurring at an offshore bank, this banker notified the S.E.C. of the irregularity, setting in motion the downfall of Dennis Levine and his co-conspirators (Stewart, 1991). However, Levine had been operating, as far as we know historically, an insider trading racket from 1979 through 1986 (Hansen, 2021; Stewart, 1991). Like Bernie Madoff and his infamous Ponzi

## ***Regulatory Ambiguity***

scheme<sup>1</sup>, Levine got away with his illegal stock trading for several years before getting caught, amassing nearly \$11 million in illegal profits, hidden in Swiss bank, Bank Leu (Stewart, 1992).

### **“Bad Boys” of Wall Street of the 1980s: Mergers and Acquisition Frenzy**

Before the 1980s, merger mania or waves occurred just prior to the Great Depression and again in the 1960s. There are times when the economic conditions and whatever current financial bubble intersect to create perfect conditions for creating black money from insider trading. One of the periods in Wall Street history that was particularly vulnerable to this was during the mergers and acquisitions frenzy between 1979 and 1986, not so coincidentally happening at the same time as a rise in insider trading. Table 1 shows the rise of mergers and acquisitions during this period of time:

*Table 1. Mergers and Acquisitions (1979-1986)*

Year	No. of Mergers and Acquisitions
1979	1531
1980	1558
1981	2328
1982	2299
1983	2395
1984	3176
1985	3490
1986	4471

(Source: Stearns and Allan, 1996)

Mergers and acquisitions, simply put, are the niche in finance that involves the combining (mergers) or purchase (acquisitions) of companies. There are a number of economic and social consequences of mergers or acquisitions. First off, when two companies merge, there are obvious duplications of personnel. For example, you now have two CEOs. This is usually ironed out in the details of the transaction, but it is not uncommon for one or both of the original companies to let go duplicate personnel. For instance, both companies would have a head of human resources. Since companies generally only have one department head for each department, one would be let go or moved to another position in the new company, not necessarily one that the person desires.

From a white collar crime perspective, those working in the mergers and acquisition business, including stock brokers and financial institutions, are privy to information on these transactions in advance of public announcement. Stock value in the companies is inevitably affected. This means that there is the potential for taking that unpublished information and making a substantial amount of money in stock transactions illegally. This is precisely what happened during the mergers and acquisition frenzy during the 1980s.

Insider trading associated with mergers and acquisitions during this period appeared to be ignored by the SEC. There were approximately 1000 investigations annually beginning in 1979 dropping below that number 1986, even in the face of the rise in mergers and acquisitions until eventually a number of

insider traders were caught red handed, including Ivan Boesky and Dennis Levine (Stearns and Allan, 1996). This reflected President Reagan's years in the White House, where the political environment called for less regulation.

## **Hedge Fund “Frat Boys”**

We might appear to be over emphasizing the male gender in this chapter, in the age of gender neutrality. As we noted earlier, based on who is more likely to occupy positions that have access to insider information, the overwhelming number of them are male. Though there is some shift in the workplace and more women are working in elite positions in financial institutions, financial markets are largely being run by men.

In the elite pool of investment instruments available to the wealthy, perhaps the most elite, are hedge funds. You can only invest in hedge funds if you are extremely wealthy and demonstrate that you have extensive experience in investments. As *Forbes Magazine* reports, you can only participate in hedge funds if you have at least \$100,000 (USD) to \$1 million to invest, a figure that is beyond the abilities of the average American (Sherman, 2000; Ross, 2020). It is nearly impossible for the small investor to participate in hedge funds.

Even the wealthy have to protect their money from erratic changes in the market, with hedge funds advertised as a means to offer some income stability. The reality is that hedge funds are riskier investments, as some of the means by which to buy stock within them is to borrow money. The investor is essentially betting that the investment will pay off and will more than justify the fees and interest involved in borrowing money to buy stock.

Hedge funds step further into the murky waters of regulatory ambiguity. One appeal of hedge funds to both managers and investors is that they are not held to the same SEC constraints of other investments. Though hedge funds are subject to prohibitions against fraud, they are, unexplainably not required to file public reports with the SEC (SEC, n.d.).

It is the very reason that hedge funds are high stakes that they are subject to the occasional case of insider trading, primarily involving hedge fund managers acting on information they have obtained inadvertently or illegally, advising their clients to buy and sell within the funds in advance of public announcements that could affect stock prices.

## **Personal Benefit Test**

The courts may still be our best bet in stemming the flow of insider information. As in the case of prostitution, where historically it was the prostitute who was targeted by law enforcement, while the paying customer was largely ignored, prosecutors are increasingly going after people who allow insider information to leak, either directly or indirectly.

*Personal benefit*, as it is defined by law, means that an individual is receiving some benefit or gain, by their actions. Even though the Securities Exchange of 1934 prohibits insiders to knowingly pass on information that has yet to be made public, there was little effort to go after the leakers. In 2016, in the first Supreme Court decision in twenty years on insider trading, the court decided that personal benefit can be considered gifting of confidential trading information the same as a cash exchange, in *Salman v. United States* (Haray *et al.*, 2016). We can make the argument, that even though information is not physically cash payment or gifting, it is part of the underground economy of “black money.”

More recently, the benchmark of “personal benefit” in insider trading cases was tested. In *United States v. Blaszczak*, the court decided that it was not necessary for the government to prove that an insider trader had benefited personally in order to be convicted on insider trading charges (Cohen *et al.*, 2020). This further opens the door to not only convict people who act on tips, but on those who pass the tips along without actually financially benefitting. However, nothing comes for free and we have to assume that some other exchange is being made, like social capital or promise of future business, when someone illegally divulges insider information, without receiving financial compensation. The difficulties in prosecuting these cases is in pinpointing, based on evidence, exactly when people received the insider information and from whom. And like the prostitution example given earlier, how much stomach do prosecutors have for prosecuting the people who divulge insider information illegally, particularly if they are part of the elite class?

## COVID-19 AND THE POTENTIAL FOR ILLEGAL INSIDER TRADING

Though at the time of this writing, we are only six months into the 2020 worldwide pandemic brought about by the COVID-19 virus, those of us who study white collar crime are already anticipating an uptick in illegal insider trading.

Let’s consider a hypothetical. In early 2020 we were thrown into the economic, emotional, and serious medical threat from the deadly coronavirus pandemic (COVID-19). At the time, there was no vaccine. For those who fell gravely ill, there was no clear protocol in the beginning as to how to treat patients, beyond conventional drug and respiratory therapies. There were some controversial drugs that had not yet been used in drug trials for therapeutics to test their legitimacy in combating COVID-19, including the anti-malaria drug, hydroxychloroquine (Baker, *et al.*, 2020). It was a period of global chaos and confusion as to what was going to be successful in not only treating those who displayed symptoms of COVID-19, as well as finding an effective vaccine moving forward. Of greatest concern was the unusual number of people who tested positive for COVID-19 that were asymptomatic that could unknowingly carry the deadly virus to others.

On April 6, 2020, in his daily televised news briefing, President Trump listed a number of biomedical and pharmaceutical companies that were speeding up research and medical trials in order to find a vaccine and treatments, as well as manufacturers of protective gear, as soon as humanly possible (U.S. Office of the Press Secretary, 2020). If either White House insiders or people at these companies were to purchase stock in these specific pharmaceutical manufacturers before there was a public announcement of which companies were participating in the research efforts, this could be viewed as illegal insider trading.

In real life, this hypothetical is all too real in circumstances where companies are working on innovation. There have already been a number of investigation of U.S. Congress members, accused of buying or dumping stock, allegedly in advance of insider trading information related to COVID-19, as in the example of Senator Richard Burr of North Carolina (BBC, 2020).

Whether real or imagined within hypothetical examples, these types of transactions are illegal as it gives unfair advantage to the people to buy stock based insider information. Stock prices will rise on good news, fall on bad news. The rest of the stock buying public will have to either pay higher prices for the same stock as insiders did or may suffer far greater losses than those who illegally sold in advance of bad news.

## CONCLUDING REMARKS

Though we ordinarily think of “black money” as being cash, we cannot discount seemingly invisible money in the form of bank accounts and stock transactions. We cannot also ignore that the exchange or leading of information as being the same as a cash transaction, as defined in the Supreme Court decision in *Salmon v. United States*. We should also consider the rise in the use of cyber currency, including Bitcoins, in order to conduct illegal commerce within the Dark Web, including hiding money made from investment transactions that were illegally executed (Hansen, 2021).

In the case of illegal insider trading, white collar criminals cannot merely have their profits deposited into a standard brokerage account. It can also be hidden in secret offshore bank accounts and depending on the location, may go undetected because of loosely regulated financial institutions. This is particularly true in the use of overseas banks that are more secretive about their clientele, even legally, as given the example of Switzerland being a safe haven for some assets.

One of the biggest consequences of hiding illegal profit is that it does not get taxed, which translates into untold millions of lost tax revenue. In addition to this, when scandals break, investors lose confidence in the free market system and this tears as the social fabric of financial transactions. Though economists would argue that this in itself is part of market forces, it none-the-less can have a negative impact on the investment sector in the long run.

Even when professionals in financial institutions, research and development companies, and manufacturing live under the threat of embarrassment, banishment from their professions, and in extreme cases, federal prosecution, they do not always comply with regulations. The problem is two-fold. The regulations themselves are many times ambiguous and in some industries like finance, the corporate culture can encourage turning a blind eye to malfeasance, as long as a profit is being made (Hansen, 2021).

The good news, if any, is that since the scandals and market downturns at the beginning of the 21<sup>st</sup> century, compliance has become more consciously part of corporate life, including in financial institutions. Companies increasingly include dedicated departments and key personnel whose jobs are to make sure that they comply with regulation. Though the SEC is continually influx, dependent on the political environment to function (or not), there appears to be more movement towards self-regulation in professions and in companies in general.

With the increased focus on corporate responsibility, even if it is a public relations ploy, along with the increased efforts to go after the leakers of insider information, we might be more optimistic on the ability for regulation to become clearly written, with straight forward, unambiguous language. However, any efforts to control insider trading or financial crime in general, are only as good as regulators and prosecutors have the stomach to do so. Regulation and prosecution is unfortunately is too often a pawn in whatever political climate is dominating at any given moment.

## DISCLAIMER

The contents and views of this chapter are expressed by the author in her personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## REFERENCES

- Adler, F. (1975). *Sisters in Crime: The Rise of the New Female Criminal*. McGraw-Hill.
- Atkins, P. S., & Bondi, B. J. (2008). Evaluating the mission: A critical review of the history and evolution of the SEC enforcement program. *Fordham Journal of Corporate and Financial Law*, 13(3), 367–418.
- Baker, P., Rogers, K., Enrich, D., & Haberman, M. (2020, April 6). Trump's aggressive advocacy of malaria drug for treating coronavirus divides medical community. *The New York Times*. Retrieved from <https://www.nytimes.com>
- BBC. (2020, March 30). Coronavirus: US senator probed for alleged insider trading – reports. *BBC News*. Retrieved from <https://www.bbc.com>
- Belfort, J. (2011). *The wolf of wall street*. Hachette.
- Byrnes, J. P., Miller, D. C., & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. *Psychological Bulletin*, 125(3), 367–383. doi:10.1037/0033-2909.125.3.367
- Coffin, B. (2017). A brief history of the SEC. *Compliance Week*, 14(157). Retrieved from [https://go-gale-com.wne.idm.oclc.org/ps/i.do?v=2.1&u=mlln\\_w\\_westnew&it=r&id=GALE%7CA535100987&p=GPS&sw=w](https://go-gale-com.wne.idm.oclc.org/ps/i.do?v=2.1&u=mlln_w_westnew&it=r&id=GALE%7CA535100987&p=GPS&sw=w)
- Cohen, D. A., & Gatta, J. D. (2020, January 19). Recent developments in charges of insider trading. *Harvard Law School Forum on Corporate Governance*. Retrieved from <https://corpgov.law.harvard.edu/2020/01/19/recent-developments-in-charges-of-insider-trading/>
- Cohn, S. (2018, December 11). 10 years later, here's what became of Bernie Madoff's inner circle. *CNBC*. Retrieved from <https://www.cnbc.com>
- Daly, K. (1989). Gender and varieties of white-collar crime. *Criminology*, 27(4), 769–794. doi:10.1111/j.1745-9125.1989.tb01054.x
- Donaldson, T. (2012). Three ethical roots of the economic crisis. *Journal of Business Ethics*, 106(1), 5–8. doi:10.1007/10551-011-1054-z

- Dreisbach, T. (2020, August 14). Under Trump, SEC enforcement of insider trading dropped to lowest point in decades. *NPR*. Retrieved from <https://www.npr.org/2020/08/14/901862355/under-trump-sec-enforcement-of-insider-trading-dropped-to-lowest-point-in-decade>
- Fernandes, N., & Ferreira, M. A. (2009). Insider trading laws and stock price informativeness. *Review of Financial Studies*, 22(5), 1845–1887. doi:10.1093/rfs/hhn066
- Gunningham, N. (2015). Regulation: From Traditional to Cooperative. In *The Oxford Handbook of White-Collar Crime*. New York: Oxford University Press.
- Hagan, J., Hewitt, J. D., & Alwin, D. F. (1979). Ceremonial justice: Crime and punishment in a loosely coupled system. *Social Forces*, 58(2), 506–527. doi:10.2307/2577603
- Hansen, L. L., & Movahedi, S. (2010). Wall Street Scandals: The Myth of Individual Greed. *Sociological Forum*, 25(2), 367–374. doi:10.1111/j.1573-7861.2010.01182.x
- Hansen, L. P. (2021). *White Collar and Corporate Crime: A Case Study Analysis Approach*. Wolters Kluwer.
- Haray, J. W., Hillebrecht, J. M., Saleski, C. G., Masella, J. A., & King, J. D. (2016, December 7). *What is a personal benefit? US Supreme Court issues major insider trading decision – key takeaways*. White Collar Alert, DLA Piper Publications. Retrieved from <https://www.dlapiper.com/en/us/insights/publications/2016/12/what-is-a-personal-benefit/>
- Huddart, S., Ke, B., & Shi, C. (2007). Jeopardy, non-public information, and insider trading around SEC 10-K and 10-Q filings. *Journal of Accounting and Economics*, 43(1), 3–36. doi:10.1016/j.jaccoco.2006.06.003
- Huffman, M. L., Cohen, P. N., & Pearlman, J. (2010). Engendering change: Organizational dynamics and workplace gender desegregation, 1975–2005. *Administrative Science Quarterly*, 55(2), 255–277. doi:10.2189/asqu.2010.55.2.255
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Kolhatkar, S. (2018). *Black Edge: Inside Information, Dirty Money, and the Quest to Bring Down the Most Wanted Man on Wall Street*. Random House.
- Komisar, L. (2003). Offshore banking: The secret threat to America. *Dissent*, 50(2), 45–45.
- Lewis, L. J., Park, J. K., & Berkowitz, D. (2013). The Second Circuit holds the short-swing profit rule inapplicable to insider's purchase and sale of different types of stock in the same company. *Insights: The Corporate and Securities Law Advisor*, 27(2), 37–39.
- Liu, L., & Miller, S. L. (2019). Intersectional Approach to Top Executive White-Collar Offenders' Discourses: A Case Study of the Martha Stewart and Sam Waksal Insider Trading Scandal. *Sociological Inquiry*, 89(4), 600–623. doi:10.1111/oin.12265
- Lokanan, M., & Chopra, G. (2021). Money Laundering in Real Estate (RE): The Case of Canada. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

## **Regulatory Ambiguity**

O'Fallon, M. J., & Butterfield, K. D. (2013). A review of the empirical ethical decision-making literature: 1996–2003. In *Citation Classics from the Journal of Business Ethics* (pp. 213–263). Springer. doi:10.1007/978-94-007-4126-3\_11

Polychroniou, C. J. (2020, April 10). Chomsky and Pollin: To heal from COVID-19, we must imagine a different world. *Truthout*. Retrieved from <https://truthout.org/articles/chomsky-and-pollin-to-heal-from-covid-19-we-must-imagine-a-different-world/>

Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Rafay, A., Sadiq, R., & Mohsan, T. (2016). X-Efficiency in Banking Industry – Evidence from South Asian Economy. *Global Management Journal for Academic & Corporate Studies*, 6(1), 25–36.

Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.

Ross, S. (2020, March 4). Can you invest in hedge funds? *Investopedia*. Retrieved from <https://www.investopedia.com/ask/answers/011915/can-you-invest-hedge-funds.asp>

SEC. (2000). Final Rule: Selective disclosure and insider trading. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/rules/final/33-7881.htm>

SEC. (2003, June 4) SEC charges Martha Steward, Broker Peter Bacanovic with illegal insider trading. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/news/press/2003-69.htm>

SEC. (2006). 2006 Performance and Accountability Report. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/about/secpar/secpar2006.pdf>

SEC. (2016, Nov 14). SEC announces settlement with former government official in insider trading case. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/litigation/litreleases/2016/lr23688.htm>

SEC. (2018, April 30). SEC obtains final consent judgements against William Walters and Thomas Davis. Litigation Release No. 24125. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/litigation/litreleases/2018/lr24125.htm>

SEC. (n.d.a) SEC Enforcement Actions: Insider Trading Cases. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/spotlight/insidertrading/cases.shtml>

SEC. (n.d.b). Fast Answers: Form 10-Q. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/fast-answers/answersform10qhtm.html>

SEC. (n.d.c). Fast Answers: Hedge Funds. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/fast-answers/answershedgehtm.html>

Sherman, L. (2000, July 15). Hedge fund investing 101. *Forbes*. Retrieved from <https://www.forbes.com/2000/07/15/feat.html#72a0f2e23994>

Simmel, G. (1990). *The Philosophy of Money*. Routledge.



- Simon, R. J. (1975). *The Contemporary Woman and Crime*. National Institute of Mental Health.
- Stearns, L. B., & Allan, K. D. (1996). Economic behavior in institutional environments: The corporate merger wave of the 1980s. *American Sociological Review*, 61(4), 699–718. doi:10.2307/2096400
- Stewart, J. B. (1992). *Den of Thieves*. Simon and Schuster.
- Sutherland, E. H. (1939). White-Collar Criminality. *American Sociological Review*, 5(1), 1–12. doi:10.2307/2083937
- U.S. Court of Appeals. Second Circuit. (2012). *Gibbons v. Malone*. Retrieved from [https://scholar.google.com/scholar\\_case?case=13272908530594532132&q=Gibbons+v.+Malone&hl=en&as\\_sdt=6,32&as\\_vis=1](https://scholar.google.com/scholar_case?case=13272908530594532132&q=Gibbons+v.+Malone&hl=en&as_sdt=6,32&as_vis=1)
- U.S. Office of the Press Secretary. (2020, April 6). Remarks by President Trump, Vice President Pence, and members of the Coronavirus Task Force in press briefing. *White House*. Retrieved from <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-vice-president-pence-members-coronavirus-task-force-press-briefing-21/>
- White, R. M. (2020). Insider Trading: What Really Protects US Investors? *Journal of Financial and Quantitative Analysis*, 55(4), 1305–1332. doi:10.1017/S0022109019000292
- Workman, D. J. (1982). The use of offshore Tax Havens for the purpose of criminally evading income taxes. *The Journal of Criminal Law & Criminology*, 73(2), 675–706. doi:10.2307/1143111

## ENDNOTE

- <sup>1</sup> *Bernie Madoff was convicted and sentenced to 150 years in federal prison in 2009 due to an illegal pyramid investment scheme that he ran for approximately 26 years. It all fell apart with the sudden downturn of the stock market in 2008, when it was revealed that Madoff was illegally paying older investors with newer investors' money. A number of people lost substantial money in Madoff's scheme, including some Hollywood celebrities. More information on Madoff is available at Biography (2019), <https://www.biography.com/crime-figure/bernard-madoff>.*

# Chapter 9

## Legislation for Public Procurements and Disposal of Public Assets: The Case of Uganda

**Simeon Wanyama**

*Uganda Martyrs University, Uganda*

### **ABSTRACT**

*This chapter is about corrupt practices in the public procurement cycle. Taking the example of Uganda, it identifies what takes place at each of the stages of public procurement and examines the perspectives of stakeholders regarding alleged corruption, misappropriation, and fraudulent practices during the public procurement process. It also reviews the governance systems that have been put in place to try and stem out these malpractices and ensure proper governance in the administration of public procurement. The research followed a qualitative approach aimed at getting the views of stakeholders and understanding whether what is in place is adhering to the principles of public procurement which foster good governance and value for money. The findings of the study indicate that the perception of the majority of the respondents is that corruption is pervasive in public procurement in Uganda despite good laws, regulations, and guidelines that have been put in place and that it manifests itself at all the stages of public procurement.*

### **1. INTRODUCTION**

Provision of public services in any country is dependent on public procurement. Government cannot provide public services without public procurement. In all countries public procurement takes up a significant portion of the national budget. In countries like Uganda, public procurement is said to account for about 70% of the national annual budget. A lot of money is involved in this process, so questions arise about whether this money is being used properly in (1) providing services to the people and (2)

DOI: 10.4018/978-1-7998-5567-5.ch009

taking care of the developmental needs of the respective nations. It is not uncommon to hear allegations of corruption, misappropriation and other fraudulent practices in public procurement.

The World Bank defines procurement corruption as the offering, giving, receiving or soliciting; directly or indirectly, of anything of value to influence the action of a public official in the procurement process or in contract execution (World Bank, 2004). It involves a clear misuse of public office. First, the act must be intentional. Second, the person must derive some recognizable benefit from the act. Third, the benefit derived must be a direct return from the act of corruption (Rafay, 2021).

This chapter concentrates on procurement by state owned entities of Uganda that use public funds to procure goods, works and services. The procurement cycle will be used as the basis of study to establish the perceptions of various stakeholders as to whether corruption takes place at any or all of the stages of the procurement cycle. The principles of public procurement will be reviewed to see whether they are actually being applied in public procurement and whether these affect the level of corruption and lack of integrity in some of the procurements. The chapter will examine, among other things, whether non-observance of these principles may be due to corruption and whether non-observance leads to compromise in the procurement process.

## **2. PUBLIC PROCUREMENT IN UGANDA**

Section 2 of The Uganda Anti-Corruption Act of 2009 makes it an offence to be involved in a corrupt act either as a giver or a beneficiary of the corrupt act. Corruption in public procurement mostly consists of violating the principles of transparency, accountability, fairness, maximization of competition, ensuring value for money and promotion of ethics, including integrity.

Section 3 to The Public Procurement and Disposal of Public Assets (Amendment) Act, Act No. 11 of 2011 describes procurement as “*acquisition by purchase, rental, lease, hire purchase, license, tenancy, franchise, or any other contractual means, of any type of works, services or supplies or any combination*”. Similar section defines public funds as “*monetary resources appropriated to procuring and disposing entities through budgetary processes, including the Consolidated Fund, grants and credits put at the disposal of the procuring and disposing entities by foreign donors; and revenues generated by the procuring and disposing entities*”. These entities generally consist of Government Ministries, Departments and Agencies (MDAs) but they include all institutions that make their procurements from funds drawn from the consolidated funds of the country.

### **2.1 Regulatory and Legal Environment**

Each country has its own system of oversight over the procurement process. In Uganda, for instance, there is the PPDA Act (2003) as amended in 2011 and the PPDA Amendment Bill 2019 (still to be assented to by the President at the time of writing this chapter in July 2020). There are also Regulations that were made in 2014 to operationalize the 2011 Act and various Guidelines that have been issued to assist in the implementation of the PPDA Act and Regulations. In addition to the Act and Regulations applying to the Central Government, there is the Local Government (Amendment) Act 2 of 2006 and Regulations issued in the same year. The official Regulatory Authority is the Public Procurement and Disposal of Public Assets Authority (PPDA) which is supervised by the Minister responsible for finance. PPDA has a Board appointed by the respective Minister. The Board exercises oversight over PPDA. However, ag-

grieved parties have an avenue to appeal against the decisions before the PPDA Appeals Tribunal. This chapter will examine whether these legal and regulatory mechanisms are able to stem out any improper practices in the procurement process and to identify areas that are prone to corruption.

## **2.2. Principles of Public Procurement**

Section 43 of the Ugandan PPDA Act (2003 as amended) states that all public procurement and disposal shall be conducted in accordance with the following principles:

1. Non-discrimination;
2. Transparency, accountability and fairness;
3. Maximization of competition and ensuring value for money;
4. Confidentiality;
5. Economy and efficiency; and
6. Promotion of ethics.

The principles also include integrity of the procurement process and integrity of the individuals involved in the procurement process (the regulators, the public procurement officials in various ministries, departments and agencies, as well as the suppliers of goods, services and works).

## **2.3. Procurement Planning**

The procurement plan allows for the monitoring of the procuring process to determine how actual performance compares with planned activities. Control measures can then be taken and adjustments made so that the procurement plan is adhered to or necessary adjustments are made to the plan in view of the prevailing realities.

All procurements are supposed to be in accordance with the procurement plan that was approved by the respective boards as part of the budgeting process. Section 34 (2) of the PPDA Act, 2003 and PPDA Regulation 60 require the User Department to prepare a work plan for procurement based on the approved budget. It describes a procurement plan as a comprehensive statement of requirements to be procured over the life of the plan – usually one year. It starts with users such as departments and functions developing their individual (departmental/sectional) procurement plans which are eventually amalgamated into master procurement plans for the entire organization/ministry. It is this procurement plan that forms the basis of the procurement process as specified above. The plan should specify the nature, quantity and timing of the requirement. The procurement schedule is then developed establishing the timelines for carrying out each step in the procurement process up to award the contract and the fulfillment of the requirement. Similar requirements from different user departments can then be consolidated into one master plan to achieve economies of scale.

## **2.4. The Procurement Process**

The procurement process usually includes the following:

1. Identification of requirements

2. Specification of requirements
3. Selection of procurement method to be used
4. Preparation of bid documents
5. Call for bids or for Expression of Interest (EOI)
6. Evaluation of Bids
7. Selection of best evaluated bidder
8. Contract with best evaluated bidder
9. Management and enforcement of contract performance

#### **2.4.1. Identification of Requirements**

The identification of requirements is normally carried out as part of procurement planning and is based upon the goals, objectives, strategies and agreed upon activities for each objective. Required resources are then specified for each activity. These may include human resources, goods, works or services, including consultancies at various levels. Requisitions for those requirements are then made in accordance with the laid down procedures as specified in the procurement guidelines of the entity.

#### **2.4.2. Specification of Requirements**

A specification is a detailed description of the goods, works or services required, and forms part of an invitation to supply or invitation for Expressions of Interest (EOI) document. Specifications reflect the needs of the customer and user group. The following specifications are normally made for the requirements of an entity depending on whether the procurement is for goods, works or services. The UN Practitioner's Handbook (2006) specifies the following types of specifications for requirements:

1. **Functional Characteristics** which concentrate on what a product is to do and is less interested in materials and dimensions.
2. **Performance Characteristics** which describe what is to be achieved rather than providing a fixed description of how it should be done.
3. **Technical Characteristics** which describe the exact design and details of a good.

The requirement for specific brands is avoided to maximize competition except where it is specifically mentioned that equivalents are acceptable. Emphasis is placed on functional, performance and technical characteristics and bids accepted from various suppliers as long as their products satisfy the three categories of specifications.

#### **2.4.3. Selection of Procurement Method**

Following an identification of need and specification of requirement, the entity determines whether the need can be satisfied in-house or contracted out. In the event that a procurement needs to be acquired externally, the contracts committee of an entity or the equivalent of the contracts committee determines the procurement method to be used. The Ugandan PPDA Act (2003) allows for the following methods:

1. Open domestic bidding;

2. Open international bidding;
3. Restricted domestic bidding;
4. Restricted international bidding;
5. Quotation method;
6. Direct procurement; and
7. Micro procurement.

Methods for consultancies include publication of notice inviting Expression of Interest (EOI) and developing a short list or short listing without publication of expression of interest. PPDA issued guidelines in 2014 specifying the thresholds that apply for each of the procurement methods.

#### **2.4.4. Preparation of Bid Documents**

Bidding documents are documents issued by the Procuring Entity to provide the prospective bidders all the necessary information that they need to prepare their bids. The bid documents must be clear and available to all eligible providers who wish to bid. These must not be designed in such a way as to favor specific suppliers or brands. The specifications in the bid should be based on the functional, performance and technical characteristics without appearing to favor certain brands or suppliers. The documents also specify the criteria that will be used in evaluating the bids so as to select the best evaluated bidder.

PPDA has issued Standard Bidding Documents which can be tailored to fit specific bids and can be used for all solicitations for bids. These are found on the PPDA website. Approval from PPDA has to be sought by procuring and disposing entities if they want to depart from what is specified in these documents.

#### **2.4.5. Call for Bids or for Expression of Interest (EOI)**

Sending out calls for bids or expression of interest (EOI) will depend upon the method of procurement that is adopted for the procurement. Bids for open domestic bidding are published in public media that have national circulation while open international bid documents must be published in media that are accessible internationally. Invitations for restricted bids are circulated only to those entities or individuals who are selected in a short list to participate in the restricted bids whether nationally or internationally. Solicitations for quotation are also sent to the individuals whose quotations are being solicited. It is recommended that at least three quotations are sought. The lowest quotation who meets the required standards is selected.

Calls for expression of interest may be circulated in public media such as newspapers and professional publications that have national or international circulation for open bidding. An entity can then develop a short list of potential bidders. The shortlisted bidders are then asked to provide financial bids which will be analyzed and the selection for the best evaluated bidder will be based upon the financial bids since all these bidders have already qualified from the aspect of technical bids which they submitted in the original call for expression of interest. Alternatively, a short list may be developed from the PPDA Register of providers or from the list of professionals who are registered by their regulatory bodies. An entity may also use a short list that has already been developed by a similar entity in the same industry or profession. The calls for financial proposals are sent directly to the short-listed entities or individuals for their response.

#### **2.4.6. Evaluation of Bids**

Each procuring and disposing entity are required to set up an evaluation committee composed of members who are competent to evaluate the specific bids. External expertise may also be sourced to assist in the evaluation where the evaluation committee does not have the required technical expertise to handle the evaluation of the bids.

Evaluation of bids and selection of best evaluated bidder has to adhere strictly to the criteria that were specified in the bid documents. The evaluation committees can only waive certain criteria if the waiving applies to all bidders and not to selected bidders. It must be observed that no new criteria can be introduced during the evaluation process if these criteria had not been specified in the bid document.

The evaluation report is submitted to the contracts committee for review and adoption of the report after which the contracts committee sends its recommendation to the accounting officer for award of contract.

#### **2.4.7. Selection of Best Evaluated Bidder**

Section 88A of the PPDA Act presents the following methods for the selection of consultants:

1. Quality and cost-based selection method;
2. Quality based selection method;
3. Fixed budget selection method;
4. Least cost-based selection method; and
5. The consultants' qualifications selection method.

The same section states that a procuring and disposing entity may source a consultant who has the capacity to perform the required assignment if the conditions for using the direct procurement method are satisfied.

Direct procurement may also be practiced where the value of the new works, services or supplies do not exceed fifteen percent of the value of the original or existing contract and the original contract and the existing contract was awarded through a competitive process. PPDA also provides that where direct procurement is used more than once under these circumstances, the value of all new works, services or supplies shall not exceed twenty five percent of the value of the original or existing contract.

#### **2.4.8. Contract With Best Evaluated Bidder**

Contracts with the best evaluated bidders are supposed to be entered into only after getting clearance from the Solicitor General / Attorney General of Uganda. This applies to contracts above two hundred million Uganda shillings or its equivalent.

Section 88 of the PPDA Act specifies the following types of contracts that are permissible:

1. Lump sum contracts;
2. Time-based contracts;
3. Admeasurement contracts;
4. Framework contracts;
5. Percentage based contracts;

## ***Legislation for Public Procurements and Disposal of Public Assets***

6. Cost reimbursable contracts;
7. Target price contracts;
8. Retainer contracts;
9. Success contracts;
10. Other types of contracts with the permission of the Authority (PPDA) (Sec. 88L).

A contract with the best evaluated bidder may not be entered into until the lapse of ten days after the display of the notice of the best evaluated bidder and on condition that there are no pending applications for administrative reviews which have to be disposed off.

### **2.4.9. Management and Enforcement of Contract Performance**

Contract management is the whole process of relationship with customers, vendors and partners to ensure delivery of a cost effective and reliable service, supply or works at an agreed standard and price. It includes negotiating the terms and conditions in contracts, monitoring performance and certifying compliance with the terms and conditions and agreeing and documenting any changes that may be made to the contract as it progresses together with the justification for the changes made.

The Ugandan Public Procurement and Disposal of Public Assets (Contracts) Regulations (2014) require a procuring and disposing entity to appoint a contract manager. Section 51 of the Regulations states that the accounting officer or a person appointed by the accounting officer from the user department shall manage the contract. It should be noted here that the accounting officer bears the ultimate responsibility of managing the contract. Section 52 of the same Regulations states that where a contract is of high value or is complex or forms part of a larger project, the accounting officer shall assign the contract to a contract management team, which shall have the same responsibilities as a contract manager. The same section provides that a contract may be managed by a body or person outside the procuring and disposing entity, supervised by the user department. The responsibilities of a contract manager are specified in section 53 of the PPDA (Contracts) Regulations.

## **3. PUBLIC PROCUREMENT IN UGANDA**

This chapter also looks at the perceptions of stakeholders regarding corruption during the disposal of public assets. Section 87 of the PPDA Act (2003) provides for the following methods for disposal of public assets:

1. Public auction;
2. Public bidding;
3. Direct negotiations;
4. Sale to public officers;
5. Destruction of the assets;
6. Conversion or classification of assets into another form for disposal by sale;
7. Trade-in;
8. Transfer to another procuring and disposing entity; and
9. Donation.



The PPDA Act and its regulations specify the procedures and terms for using each of the above methods. Details are not discussed as the main focus of this chapter is Public procurement.

## **4. METHODOLOGY**

The chapter based itself on current laws and regulations governing public procurement and those relating to corruption taking Uganda as an example. The research followed a qualitative approach aimed at getting the views of stakeholders and understanding whether what is in place is adhering to the principles of public procurement which foster good governance and value for money. A questionnaire survey made up of both structured and semi structured questions, is administered using Google Form to enable the survey to be conducted quickly and to reach a wider range of stakeholders. The author also carried out a field survey to get the perceptions of stakeholders such as regulators, public entities involved in procurement, suppliers / providers and various professionals including accountants and other professionals who are knowledgeable in public procurement and corporate governance.

## **5. FINDINGS OF THE QUESTIONNAIRE SURVEY**

### **5.1. Summary of Findings About Public Procurement**

The previous sections of this chapter have presented the principles of public procurement as well as the various elements of the procurement process. Below is a summary of findings about the perceptions of stakeholders regarding whether there is corruption at the various stages of the procurement process. The responses are presented in percentages.

There is general perception that the procurement process in Uganda is riddled with corruption in all the stages of the process. The lowest percentage of agreement with the respective statements is 66.1% and the highest is 94.7%.

The sections below look at each of the stages of the procurement process and summarize the perspectives of the respondents as to whether there is corruption at those stages considering the principles of public procurement, as well as the PPDA Act and Regulations.

#### **5.1.1. Public Procurement and Corruption**

The first statement in the questionnaire survey asked respondents whether the allegation that the procurement process in Uganda was riddled with corruption was true. Out of the 169 research participants who responded to this question, the overwhelming majority (94.7%) answered in the affirmative. Only 4.7% said that it was not true while 0.6% were not sure. This is a perception that has been echoed by many stakeholders in Uganda, including the President of Uganda and Transparency International. The President declared war on corruption in Uganda but the fight is still going on and corruption in procurement and other sectors of the country is still very much alive.

## Legislation for Public Procurements and Disposal of Public Assets

Table 1.

Statements	Total Responses	In Percentages		
		Yes	No	Not Sure
Is the allegation that public procurement in Uganda riddled with corruption true?	169	94.7	4.7	0.6
Corruption occurs at the identification of requirements stage	170	68.8	12.9	18.2
Corruption occurs at the specification of requirements stage	168	75.0	10.1	14.9
Does corruption occur when selecting and applying any of the procurement methods?	168	78.6	9.5	11.9
Can corruption occur when using any of the methods approved for disposal of assets?	166	92.2	1.8	6.0
Does corruption sometimes occur at the stage of preparing bidding documents?	163	73.0	7.4	19.6
Some people have claimed that there is lack of transparency and equity in sending out calls for bids or expression of interest. Is this true?	165	66.1	9.1	24.8
Is the claim that there is lack of transparency and equity in sending out calls for bids or expression of interest true?	165	66.1	9.1	24.8
Is the claim that there is corruption and lack of fairness when some evaluation committees are evaluating bids true?	156	81.5	3.8	14.7
Is it true that prices charged in public procurement are exorbitant and way above market prices?	164	86.0	4.9	9.1
Is the claim that there is corruption in the management and enforcement of performance of contracts resulting in poor or shoddy work by contractors and lack of value for money true?	156	87.8	2.6	9.6

Figure 1. Public Procurement and Corruption

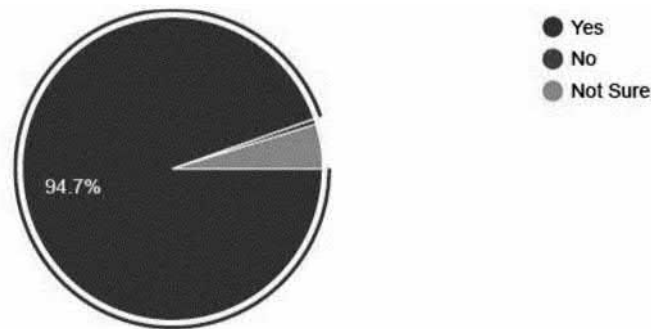
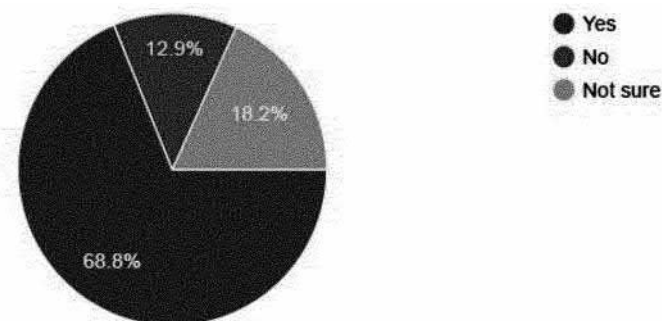


Figure 2. Identification of Requirements



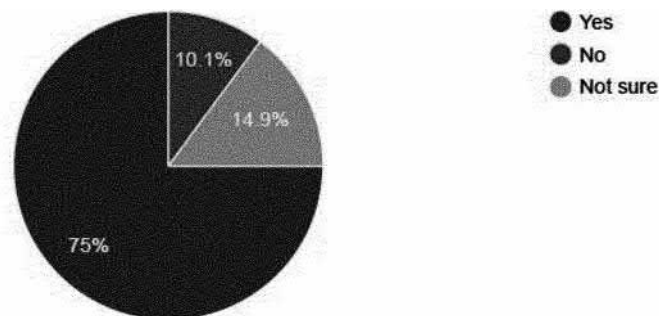
### 5.1.2. Identification of Requirements

The second statement asked respondents whether they think that corruption occurs at the Identification of Requirements stage. Out of the 170 stakeholders who responded to this question, 68.8% were of the view that corruption takes place at the identification of requirements stage. Only 12.9% did not support the statement, while 18.2% stated that they were not sure.

The respondents mentioned the following as being some of the forms of corruption at the identification of requirements stage:

- Including items that are not required;
- Conflict of interest from the technical committee;
- Leaving out some vital requirements;
- Influence peddling;
- Allocating substantive funds to “requirements” that are not of any strategic importance and inflating quantities required.
- Failure to consult the end user or requisition team on the identification of their requirements.
- Falsification of the real needs
- Political influence on the identification of requirements to suit the interests of the politicians
- Favors are agreed at the time of identifying requirements
- Vagueness in the identification of requirements to create room for manipulation

*Figure 3. Specification of Requirements*



### 5.1.3. Specification of Requirements

Respondents were asked for their views regarding whether corruption occurs at the specification of requirements stage. Out of the 168 responses given, 75% agreed that there was corruption at this stage, while 10.1% disagreed and 14.9% said that they were not sure.

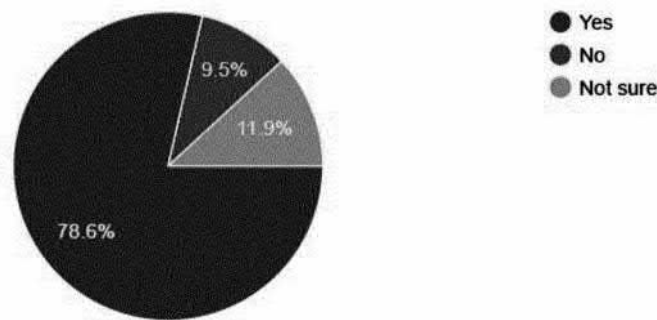
According to the respondents, corruption manifests itself in the following forms during the specification of requirements:

- The specifications and timing of procurement may only favor a particular bidder
- Exaggerated Bills of Quantities, Scope of works, services and supplies.

## ***Legislation for Public Procurements and Disposal of Public Assets***

- The requirements are tailored to the brand of a specific supplier so that the specifications match exactly that brand even if the brand name is not mentioned
- Design of the requirements and terms of reference that are meant to favor particular vendors
- Conflict of interest from the technical committee
- Prohibitive specifications
- Procurement officer asking one vendor to write sample specifications for an upcoming job.
- Customizing the tender requirements (design and specifications) to benefit a specific bidder or provider and lock out other potential suppliers
- Asking for requirements that aren't necessarily value adding but exclude valid and better suppliers.
- The individuals involved in procurement process specifying requirements and conditions that are particular so that they themselves can supply them.

*Figure 4. Procurement Method*



### **5.1.4. Selection of Procurement Method to Be Used**

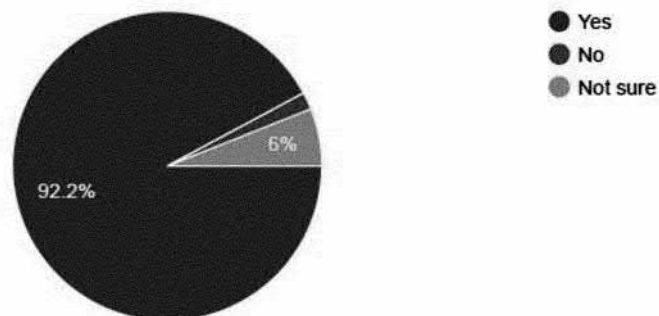
The next area to be examined was whether corruption occurs when selecting and applying the various procurement methods. Responses were received from 168 research participants. Out of these, 78.6% were of the view that corruption sometimes occurs at this stage of the procurement process. Those who said that it did not occur at this stage were 9.3% while the other 11.9% said that they were not sure. Respondents cited:

- Delaying a procurement and procuring at the last moment by direct procurement where a single supplier is selected without competition and justifying this as an emergency procurement.
- Splitting requirements so as to defeat the thresholds for the different methods of procurement
- Not adhering to the respective procurement methods that are specified by the PPDA Act and Regulations to favor certain suppliers

### **5.1.5. Preparation of Bid Documents**

The research participants were asked whether corruption sometimes occurs at the stage of preparing bidding documents.

Figure 5. Preparation of Bid Documents



Out of the 163 responses received for this question, 73% answered in the affirmative, 7.4% in the negative, and 19.6% said that they were not sure. According to the respondents, corruption can occur in the following ways during the preparation of bid documents:

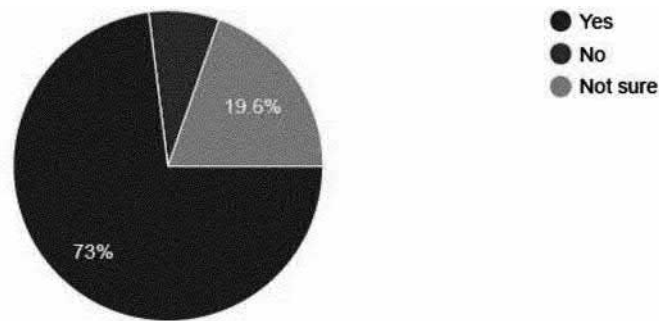
- Officials leaking key/confidential information to some bidders, e.g., information on budgeted cost of a procurement or previous contract values
- Some bidders are told by the procurement officials the exact price to quote
- Terms and conditions are designed to favor some bidders.
- Staff in the procurement function is manipulative with the service providers
- Collusion to suit some suppliers
- Delay to release the bid documents that leads to good bidders not being able to meet the deadlines.
- Some demands can be incorporated to technically eliminate some suppliers
- Under estimating work which is later inflated for additional work
- Including and making mandatory certain requirements and specifications that are not essential to the procurement
- Demanding for bribes to have bidders short listed
- Leaking information of competitors
- Bidders submitting forged documents, experience, capacity, etc.
- The statement of requirements may be designed to favor particular firms while disadvantaging others.
- Use of brand names
- Technical staff in procuring entity are engaged by some bidders to help them prepare bid documents.
- Bribery

#### 5.1.6. Sending Out Call for Bids or for Expression of Interest

The survey sought the perceptions of research participants as to whether the claim by some people that there is lack of transparency and equity in sending out calls for bids or expression of interest is true.

Out of the 165 research participants who answered the question, 66.1% were of the view that there is lack of transparency and equity in some of the procurements, while 9.1% thought that there was no lack of transparency and equity in procurement and 24.8% were not sure.

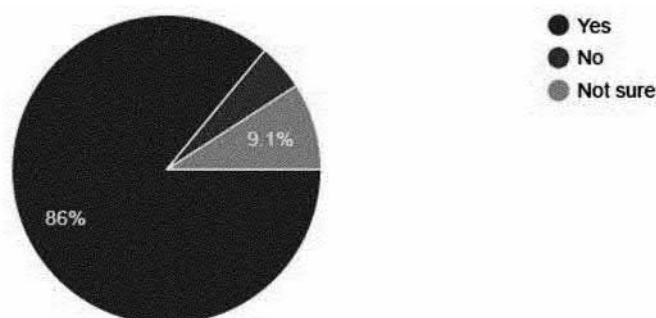
*Figure 6. Calls for Expression of Interest*



The lack of transparency and equity occurs in the following ways:

- Sometimes calls for bidding are sent out when it has already been decided to award the contract to certain suppliers. The call is made just to legalize the process of selecting the supplier.
- Withholding information from some bidders until the last minute
- Insiders alerting their friends, relatives, business partners before adverts are even placed in the papers. Insiders also tell those whom they want to win, what is required and the acceptable prices.
- During restricted method of bidding, some bidders do not get the invitations or get them late
- Sometimes the procurement process is not followed like advertising in papers
- Lack of adequate communication and information to enable bidders to prepare good bids although some favored bidders may be given proper information in advance
- Adverts in limited public media which do not have national or international circulation; this limits access to information by some potential bidders
- Invitations are sometimes sent to only those who offer kickbacks or to those who are personally known to the procurement officials
- Some potential bidders are listed but they never receive the solicitation documents and yet they are recorded as having received them but failed to respond.
- Asking preferred bidders to hold on until others have submitted and then those preferred bidders are given information on what others submitted so that they bid lower values

*Figure 7. Evaluation of Bids*



#### **5.1.7. Evaluation of Bids and Selection of Best Evaluated Bidder**

There has also been a claim by some people that there is corruption and lack of fairness when some evaluation committees are evaluating bids. The survey sought to find out whether the respondents thought that this claim was true.

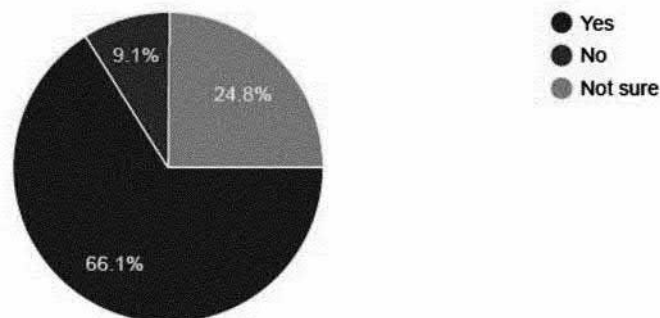
The respondents agreed overwhelmingly with this claim since 81.5% agreed and only 3.8% did not agree. The other 14.7% were not sure. Research participants were of the view that the following practices compromise the evaluation process:

- Not following the evaluation criteria set out in the call for bids or expression of interest; this may be due to wanting to favor some bidders over others
- Disqualifying some valid bids as unresponsive bids over some flimsy excuses
- Selective waiver of some requirements to favor some bidders who may not qualify or introducing new criteria that were not in the original call
- Unfair scoring during the evaluation process and awarding high marks to some favored bidders
- Evaluation committee members being influenced by bribes or other considerations
- Interference in evaluation by the bidders, politicians, middlemen and others in authority.
- Incompetence of the Evaluation Committee that lacks expertise and experience
- Selection of incompetent companies at the expense of competent ones
- Hiding some bid documents away to eliminate bidders from the procurement process.
- Some Evaluation Committee members have vested interests in some of the contracts, so they make decisions in favor of their firms or companies
- Some members of the evaluation committee are offered commissions to influence them to select certain bidders
- Disqualifying members on issues where the PPDA Act and Regulations allow for clarifications to be sought from bidders or where information can be verified from official sources such as the Uganda Revenue Authority and the Uganda Registration Services Bureau.
- Non-disclosure by some evaluation committee members that they have a conflict of interest, including self interest in the procurement process which can compromise their judgement
- During evaluation, some members of the committee can call bidders to submit additional vital documents that they did not submit in time and help them to go through
- Some bids can be adjusted to favor certain bidders
- Plucking out of documents from the files of certain bidders so as to disqualify them
- Some evaluation committee members collude with bidders to change the bid prices during the evaluation process

#### **5.1.8. Prices Charged in Public Procurement**

Respondents were also asked whether they thought that the prices charged in public procurement were exorbitant and way above market prices. Eighty six percent (86%) out of the 164 participants who responded to this question were of the view that the prices charged in public procurement were above market prices. Only 4.9% disagreed with the statement and 9.1% were not sure. These responses confirmed what has been widely discussed in the public media in Uganda. Following are some of the reasons that the respondents gave for the exorbitant prices in public procurement:

*Figure 8. Prices Charged*



- Corruption and deliberate intention to defraud
- To enable the procurement officers to swindle some of the money
- Delays in paying providers: the providers add interest and a premium for this delay which ties down their capital and also the time value of money arising from the delays in payment
- To make up for additional cost of bidding
- Failure to undertake proper market assessment of actual market prices
- To cater for kickbacks to procurement officials, evaluation committee members, and commissions to middlemen who connect the providers to the procurement officials
- Overstating the requirements in view of making a deal with the suppliers, e.g., exaggerated bills of quantities
- Suppliers who quote lower prices may be eliminated on technical grounds if they do not offer kickbacks to procurement officials
- Some payments may not be processed if the suppliers do not offer kickbacks; these kickbacks are factored in the price charged
- The additional cost for preparing and processing bids is factored in the price charged

#### **5.1.9. Management and Enforcement of Contract Performance**

Research participants were asked whether the claim that there was corruption in the management and enforcement of performance of contracts resulting in poor or shoddy work by contractors and lack of value for money true. Once again, the overwhelming number (87.8%) said that it was true. Only 2.6% said that it was not true, while 9.6% indicated that they were not sure.

According to these respondents, the impact of this poor contract management or lack of enforcement of contractual terms in contracts on fulfilling the objectives of public procurement was as follows:

- No value for money
- Poor service delivery
- Loss of funds and time
- Poor quality work/ late delivery
- Loss of money and confidence in the procurement entity



- The public suffers heavily, for example a poorly constructed road hindering businesses hence high prices, incomplete structures, bridges giving way in a few months of construction, buildings collapsing, poor quality items supplied and at worst supply of air
- Shoddy work may be reported as good work in anticipation of kickbacks
- Organizations do not attain their intended objective resulting in repetitive expenditure
- Inability to adhere to the desired objectives and goals
- Time and Cost Over runs - Quality affected - Delayed Service delivery
- Delays in execution of contracts, variations in contracts, poor contract implementation and escalation of costs
- Incomplete work which may be of poor quality could cause law suites due to unfulfilled contractual obligations
- Contracts not renewed in time when they expire because no one is monitoring them; this can lead to disruption in service or delivery of products that are fundamental to a business and cost them revenue.
- Breach of Contract.
- Contractors can overwhelm a company with additional costs by increasing the scope of projects.
- Shoddy or substandard works are signed off costing taxpayer's money;
- Sometimes projects are never completed or completed very late
- Long delays in paying contractors which leads to loss of confidence and some contractors hiking prices to make up for lost income.

## **5.2. Summary of Findings About Disposal of Public Assets**

Respondents were asked whether they thought that corruption sometimes occurs during the disposal of public assets. Most of the respondents (86%) were of the view that corruption sometimes occurs during the disposal of public assets. The respondents noted the following ways that corruption can be carried out during the disposal process:

- Members of the Board of Survey being compromised or having self interest in selecting items for disposal and fixing reserve prices
- Collusion between procuring and disposing unit and the potential buyers
- Bribery and collusion
- Undervaluation of assets so as to sell to selected people at a lower price
- Lack of transparency in the selection of potential buyers to negotiate with
- Elimination of potential buyers in public auction on some technicalities
- Disappearance of some assets
- Self-interest and conflict of interest
- Influence peddling
- Insider dealing where some staff members front others to bid on their behalf
- Disclosure of reserve price and performance conditions of assets to selected bidders
- Demanding kickbacks during direct negotiation
- Officials negotiating price with potential buyers before the auction date
- Disposal method selected to favor some individuals
- Falsely claiming to have destroyed a certain asset and later selling it for self-gain

## ***Legislation for Public Procurements and Disposal of Public Assets***

- Not advertising the disposal but rather buying it cheaply claiming that there were no other bidders
- Fabricated evaluation reports to understate the value of the assets
- Auctioneers may have a conflict of interest and not be transparent
- Abandoning assets and later claiming that they are of very low or of no value
- Assets can be classified as scrap when actually are good for use
- A single bidder can front a number of proxies to try to drive down the prices of an asset due for disposal
- Some of those bidders who want to buy the items cheaply tend to lobby and compromise the officials who are involved in the process

## **6. RECOMMENDATIONS FOR PUBLIC PROCUREMENT**

### **6.1. Corruption in the Procurement Process**

The Electronic Government Procurement (eGP) system has been touted as one of the major solutions to counter corruption in public procurement in Uganda. This system was launched in 2018 and is being rolled out gradually. All government procuring and disposing entities will be required to conduct all their procurement using this on-line system right from posting of bid notices, to uploading bid/tender documents and finally making payments to suppliers. At the same time, the private sector (for example suppliers / bidders) will also be required to submit their bids through this on-line system. The system is meant to promote efficiency, transparency and accountability. All bidders will have access to the same information at the same time and the submission of bids can be monitored and verified electronically. However, it is unlikely that the eGP will be the silver bullet that will get rid of all corruption in procurement since there will always be a human element at all stages of the procurement process. The answer appears to be on the quality of the staff and all the individuals who are involved in the process. Their integrity and moral uprightness, as well as transparency and accountability will make a big difference. The monitoring and regulatory mechanisms both at state and individual entity level also matter greatly if we are to tackle this monster of corruption. There have also been proposals that the cost of corruption should be made very expensive and risky to discourage corrupt procurement officials. Currently government officials who are found corrupt are subject to imprisonment and/or fined. It is argued that the term of imprisonment is not long enough to discourage corruption. Fines are also found to be insufficient because culprits who have benefitted from illicit acts can go back to enjoy their wealth after serving the term of imprisonment. It has been suggested that officials found guilty of corruption and similar offences should have their property which they gained from illicit practices confiscated and sold off by government in addition to fines and imprisonment.

It has also been suggested that all procurement officers should belong to a professional body such as the Institute of Procurement Professionals (IPP) and that this body should play a regulatory function by registering, monitoring, reviewing the work of procurement officers and disciplining them as and when necessary. Each procurement officer must be licensed and those without licenses should not be allowed to head the procurement function. Their licenses should be renewed annually in line with other professional bodies. This would enable the IPP to have control over its members and help to minimize corruption in public procurement.

The procurement control environment that includes the Board and top management of the entity must not condone corruption and must monitor and enforce ethical values and strict adherence to the principles of public procurement.

## **6.2. Identification of Requirements**

The user departments and all those involved in the identification of requirements must be honest when identifying genuine needs. Integrity, with zero tolerance to corruption, is an absolute requirement right from the start of the procurement process. There should also be a panel to review the requirements that have been identified. The panel should have people with expertise in the respective areas where procurement is being suggested, especially for high value procurements. All items identified for procurement must be in the entity's approved procurement plan and budget. The internal controls need to be strengthened to ensure that only required items are included in the procurement plan. Senior officers should review the list of requirements and verify whether these are genuine requirements at a particular time. For commonly required items, it would be good for the entity to develop a list of the commonly used items and services which can be re-stocked as and when required according to the inventory policy of the entity. The identification of requirements should be a transparent process which can be viewed and verified.

## **6.3. Specification of Requirements**

This should be done by people with expertise in the area of requirements and should be guided by technical knowledge, honesty and integrity. The use of brand names must be avoided. Emphasis should be placed on functions, performance and technical specifications. Where a brand name is used, provision must be made for equivalents that have similar functions, performance and technical specifications without being restrictive or appearing to exclude other brands. These specifications should be reviewed by an independent team of competent people. There is also a need to coordinate with user departments to ensure that the specification of requirements meets the actual needs of the users without having exaggerated requirements that will not be needed by the users. The people making the specifications should not be the ones who are involved in the procurement so as to avoid a conflict of interest. Also, there should be no collusion between the procuring entity and a specific supplier where the specifications are tailored to that supplier to restrict competition. Generic specifications should be used as long as the function, performance and technical requirements are met.

## **6.4. Selection and Application of Procurement Method to Be Used**

A technical committee should advise the contracts committee on the correct method of procurement that should be used when selecting the relevant procurement method. The oversight authorities such as Boards of the entities and the Public Procurement and Disposal of Public Assets Authority should monitor the methods used for procurement very closely. The Office of the Auditor General should also be strict in auditing procurement methods used when auditing the respective government entities. Firm action should be taken against accounting officers who flout the methods specified for the different types of procurements and the thresholds laid down for the different procurements based on the nature and value of the procurement. Attention should be paid to attempts to manipulate procurement methods by splitting the procurements to dodge the thresholds that would require the entities to use certain procure-

ment methods. Integrity and transparency are important in the selection of the procurement methods. Procurement officials should undergo continuing professional development so that they are kept current on the correct procurement methods that are permissible in public procurement based upon the PPDA Act, Regulations and Guidelines, as well as the standard bidding documents.

## **6.5. Preparation of Bid Documents**

Bidding documents should be prepared by the Procurement Unit of the entity with the assistance of technical people who know the procurement method to be used and the specifications of the requirements in consultation with the User Department. The bid documents should adhere to the sample standard bidding documents (SBDs) that have been approved by the PPDA. The entities are to tailor their requirements according to their specific circumstances to fit the guideline of the SBDs. Permission to depart from these SBDs should be sought from PPDA. These documents should be sent out only after they have been reviewed and approved by the contracts committee. The principles of procurement, namely: transparency, accountability, integrity, honesty, fairness, competition, ethical values and value for money should be reflected in these documents.

Periodic review by a procurement professional body such as the IPP would help to monitor and minimize corruption in the preparation of bid documents. Oversight bodies such as the Boards of the respective bodies and the Office of the Auditor General could also monitor, review and ensure that bids are prepared in the proper way and are not subject to corrupt practices. Online bidding could also help as the bidding documents would be standardized and open to scrutiny by relevant bodies and other stakeholders in a transparent manner.

## **6.6. Sending Out Call for Bids or For Expression of Interest**

Sending out calls for bids or for expression of interest should ensure that everyone gets the same information at the same time. The eGP will ensure more transparency and competition but it will still not eliminate the possibility of procurement officials colluding with potential providers by giving them privileged information or advance information about bids. Staff with proper ethical values and integrity will still be needed to avoid corruption when sending out calls for bids or expression of interest. Calls can also be placed on the websites of the respective entities and the PPDA website and in other media such as newspapers that have wide circulation and radios to widen the accessibility of the information to potential bidders.

Some respondents noted that the way calls for bids and expression of interest are disseminated should be audited by the Auditor General to ensure that they are being done transparently following the laid down PPDA guidelines and manuals developed by the respective entities. It is assumed that the internal auditors audit the calls for bids and expression of interest to get assurance that proper controls and procedures are being followed. The regulators, such as PPDA, need to pay attention to and review the practices of sending out these calls in the respective entities. This necessitates the keeping of proper records for each procurement in accordance with the requirements of the national laws governing the storage of documents and the provisions of the specific laws relating to procurement so that they can be examined when reviewing the manner in which procurements were handled.

## **6.7. Evaluation of Bids and Selection of Best Evaluated Bidder**

Corruption during the evaluation process and selection of best evaluated bidder depends on the team that is evaluating the bids. The members of this team should be people of high integrity and competence. They should exercise their role with fairness and stick to the evaluation criteria that were set out in the call for bids or expression of interest. No new criteria should be introduced during the evaluation process. Any justified waiving of certain requirements should be applied equally to all bidders without discrimination. Any conflict of interest must be declared and the member conflicted should be excluded from the evaluation committee. Bidders should be invited to the bid opening, especially when financial bids are being opened, so that all bidders know bid values of each of the bidders. It is however understood that the selection of the best evaluated bidder will depend on the weighting given between the technical bid and financial bid.

Submission of bids or expressions of interest should be done electronically to ensure that all documents from bidders are recorded and considered without claiming that some documents were not submitted or removing some documents from bids or adding fresh documents in the bids. The date and time of submission of proposals would also be recorded electronically to decrease manipulation where some entities claim that some bidders were out of time or where they allow some bidders to submit documents when the time is over. Arithmetic accuracy as well as the authenticity of the documents submitted should be checked at the beginning of the evaluation process. Some bidders may corruptly submit fake documents to support their bids.

Evaluation committee membership should not be permanent. The members should be rotated periodically and different members appointed for each evaluation process considering their expertise, experience and integrity. These members need training to update themselves on the provisions of the procurement law, regulations and guidelines so that they act within the law. One of the areas that creates controversy during the evaluation process is missing documents and/or information. It is imperative that they know the circumstances under which the committee can disqualify bids due to non-submission of some documents and when they can seek clarification and allow the bids to continue. The same applies to information which can be clarified with bidders or which can be accessed on official websites of regulatory bodies and other government agencies. Another area is one where the evaluation committee needs to seek official guidance and interpretation from other technical agencies that are best qualified to give advice and interpretation. This will help the committee to avoid making wrong decisions or favoring certain bidders and disadvantaging others due to improper understanding of certain circumstances.

Oversight bodies such as the Boards of the respective government entities, the Office of the Auditor General, the Office of the Internal Auditor General as well as the internal auditors should pay particular interest to reports compiled by the evaluation committees to ensure that due process is followed in evaluating bids. The use of parallel bid evaluation where an external professional body or committee is asked to evaluate the bids independent of the entity's evaluation committee can be very helpful especially for high value procurements. The decision of the internal evaluation committee is then compared with the decision of the independent parallel evaluation committee to see if there is agreement. Disagreements have to be reconciled and a final decision arrived at by the procuring entity.

## **6.8. Charging Exorbitant Prices**

Among the reasons mentioned for the higher than market prices are the long time it takes to receive payment from government and the cost of preparing the lengthy and complex bids in public procurement. In addition to this, some corrupt officials ask for kickbacks to win the contracts and to get payment for the work done and this has to be factored in the price charged to the entities.

Timely payment of providers would alleviate the providers who have to think of the time value of money and the interest that they have to pay for loans secured so as to be able to carry out the contracts. This would require the procuring entities to ensure that the money is available before the procurement contract is signed and for the Ministry of Finance to release the money in a timely manner. The process of securing contracts after the bid should also be shortened. Some procurement processes take more than a year before they are concluded. This ties up some of the capital of the bidders leading to lost opportunities. The PPDA Act prohibits awarding contracts where the price of the contract is higher than the market price. This provision needs to be followed up during procurement audits and sanctions taken against accounting officers who flout this provision although the PPDA Act makes the accounting officer personally liable if he/she signs a contract with prices that are above the market price. The challenge here is that it is difficult to establish the market price as prices may vary in different parts of the country and at different times of the supply. PPDA is supposed to come up with a price list for commonly used items but the problem has been how to fix market prices. It is these market prices that are supposed to inform the procurement budget and to set reserve prices in procurement.

## **6.9. Management and Enforcement of Contract Performance**

Respondents suggested that each entity should establish a proper and competent contract management team that has members of integrity to monitor and evaluate each contract. The team should have the ability to manage relationships with providers based on transparency, accountability and value for money without being compromised in any way. The contract management team should report regularly to management and the Board on the progress of the contract and highlight any special circumstances that have occurred but were not according to plan. The main objective of this contract management team should be to ensure that the project is proceeding smoothly and is complying with the terms and conditions agreed upon between the entity and the provider. The contract management committees should have one or more members with technical knowledge of the project being managed. The Board of the entity should take a special interest in each of the contracts and provide the oversight that is required for the implementation of those projects. It would be advisable that the progress of each contract is recorded on the eGP portal for easy and transparent monitoring. Both the internal and external audit function should monitor the performance and progress of these contracts to see if they are adhering to the terms and conditions of the contract. Payment to providers should only be made when a certificate of completion or certificate of progress has been issued by competent and technical people who are authorized to issue the certificate. Any malpractice in issuing those certificates should be pursued vigorously and punished severely as a deterrent to would be corrupt practices. PPDA should provide additional oversight when their staff carry out the performance audits. The accounting officer of each entity is ultimately responsible for performance management of all contracts under his/her ministry, department or agency. The procuring entity is required to retain a percentage of the contract value as retention fee to cater for any defects in the implementation of the contract for a specified period after the end of the contract. This practice helps in the management and enforcement of contracts.

## **7. RECOMMENDATIONS FOR DISPOSAL OF PUBLIC ASSETS**

Each entity should constitute a Board of Survey to review the condition of all the assets and determine whether some of them should be disposed off. The list of these assets should be submitted to management and the Board of the entity for approval after which the disposal is handed over to the contracts committee. Technical people should be used to set the reserve price for each of the assets due for disposal. This committee would then decide on the method to be used for disposing of each class of assets.

The practice by some officials in public entities of abandoning some assets that are in good condition and later selling them off as scrap or as assets that have impaired values should also be scrutinized and avoided. In such cases, the officers of the entity know the real value of the assets but collude with outsiders to bid on their behalf at low prices pretending that the values of the assets have diminished. In some cases, the officials pretend to have destroyed some assets when they have actually kept them for their personal use. There should be methods of verifying whether each of the methods has been used effectively, including the destruction of the assets. Minutes of the Board approving disposal and the minutes of the contracts committee approving the method of disposal must be kept and made available for review by competent persons. The minutes of the actual decisions for final disposal, including the names of the beneficiaries and the price at which each asset was disposed off must also be kept.

## **8. FUTURE RESEARCH DIRECTIONS**

The President of Uganda has voiced his concern about corruption in Uganda on numerous occasions, but this vice continues unabated. It is a bitter sore that is affecting the development of the country and the provision of services to the citizens of the country. Serious research needs to be carried out to see how corruption can be tackled so as to promote good governance and provision of services without this vice. What has been stated here about Uganda applies to many other countries.

## **9. CONCLUDING REMARKS**

This chapter has discussed the practice of public procurement in Uganda and the corruption plague that is affecting it. The findings of the study indicate that the perception of the majority of the respondents is that corruption is pervasive in public procurement in Uganda despite good laws, regulations and guidelines that have been put in place and that it manifests itself at all the stages of public procurement. The regulatory bodies and other enforcement mechanisms such as the Public Procurement and Disposal of Public Assets Authority (PPDA), the Office of the Auditor General (OAG), the Office of the Internal Auditor General and the Accountant General, the Inspector General of Government, the Civil Society Organizations and other mechanisms have not been able to stem out this vice. The top leadership in the country has decried the widespread corruption in the country but it is still to be seen what steps will be taken to eradicate it so that it does not continue affecting development and the provision of services to the people in Uganda. Further research and steps need to be undertaken to rectify the situation.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in his personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to:

- The Public Procurement and Disposal of Public Assets Authority (PPDA) in Uganda, the Institute of Certified Public Accountants of Uganda and the Institute of Corporate Governance in Uganda for the great role that they played in circulating the questionnaire survey to its members.
- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.

## **REFERENCES**

Anti-Corruption Act 2009

OECD. (2016). *Public Procurement Toolbox*. OECD.

Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

The Local Government (Amendment) Act 2006

The Local Government (Public Procurement and Disposal of Public Assets) Regulations, 2006

The PPDA Amendment Bill 2019

The Public Procurement and Disposal of Public Assets Act 2003

The Public Procurement and Disposal of Public Assets (Amendment) Act, 2011

The Public Procurement and Disposal of Public Assets Regulations, 2014

The UN Practitioner's Handbook (2006)

World Bank. (2004). *Mainstreaming Anti-Corruption Activities in World Bank in Assistance – A Review of Progress since 1997*. World Bank.



## Chapter 10

# Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds: The Case of China

**Poshan Yu**

*Soochow University, China*

**Yingzi Hu**

*Independent Researcher, China*

**Maimoona Waseem**

*University of Management and Technology, Pakistan*

**Abdul Rafay**

 <https://orcid.org/0000-0002-0285-5980>

*University of Management and Technology, Pakistan*

### ABSTRACT

*Internet lending is a unique form of the credit market for bypassing banks in which borrowers generate online microloans without leverage or intermediation from financial institutions. Unlike the UK and the US, the Chinese P2P lending market is broader. Although the regulations concerning P2P lending are more comprehensive since 2015, there remains some regulatory gaps and failures, thus identifying these remaining regulatory gaps can help perfect the regulatory framework. This chapter provides a more detailed analysis and an examination of the Chinese legal framework related to P2P lending and identifying the vacuums in the existing framework. The theoretical contribution is primarily to the implications of the latest development of regulatory changes and the established individual credit reference system in China. Furthermore, the chapter also discovered three new regulatory vacuums (i.e., platform exit, a case report of financial crime, and consumer education), thus concluding with detailed insights on future approach towards perfecting the regulatory framework.*

DOI: 10.4018/978-1-7998-5567-5.ch010

## **1. INTRODUCTION**

Formal credit analysis focuses on the conduct of corporate finance. However, as new internet infrastructure progresses, more users prefer Internet borrowing. Internet lending is a unique form of the credit market for bypassing banks in which borrowers generate online microloans without leverage or intermediation from financial institutions. P2P (peer-to-peer) lending/borrowing is one system in which people lend money directly to individual creditors (Gomber, Kauffman, Parker, & Weber, 2018).

Most P2P platforms have been advocating their function as “cost-cutters,” implying that they can provide better returns to investors and cheap loans to borrowers by removing the middleman (banks). Economic developments in the years after the recession and increased mistrust of the banking sector led to the rise of a rising number of start-up technology companies directly involved in providing financial services and goods to end-users. In most cases, the main innovation embedded in its market was a technical infrastructure built and employed by these businesses, making it easier for end-users to access financial products.

The concept behind these platforms is that they serve an alternative, market-based financial intermediation mechanism which allows parties to circumvent the role that banks historically play in providing credit and taking deposits. In reality, alternative platforms appear to attract potential lenders by lowering the costs of intermediation and service and raising returns on deposits in terms of interest. At the same time, borrowers are granted more comfortable access to loans and better terms.

Peer-to-peer lending, also known as P2P lending, is an innovative Internet-based lending model that enables individuals to lend and borrow money without the intervention of conventional financial institutions (Serrano-Cinca, Gutiérrez-Nieto, & López-Palacios, 2015).

A potential borrower applies for a loan on a platform under a standard P2P arrangement. The borrower must usually provide credit information, which is processed and posted on the platform after being checked and accepted. At the opposite end of the platform, creditors (or rather investors) may choose from the available loans that suit their risk and return appetite.

Unlike the UK and the US, where few platforms mainly dominate the P2P lending markets, the Chinese P2P lending market is broader, where the top five platforms constitute only 15% of the lending market in China (Yan et al., 2017).

The development of P2P lending in China can be classified into four stages (Zhang et al., 2015). Stage one is from 2007-2012, with Paipaidai being the first P2P lending platform in China. Stage two is from 2012-2013, which features China’s P2P lending sector’s aggressive growth since 2007 (Yan et al. 2017) and from 2012 onward, witnessed exponential growth as revealed in Figure 1.

Stage three features an explosion of risk, which began in 2013. The aggressive growth prevented regulatory parties from setting adequate legislation to regulate this kind of novel industry (Buckley, Arner, & Barberis, 2016). Various media reveals several platform scandals such as capital misappropriation and high lousy debt rates. These events had a direct impact on investors’ confidence in P2P lending. Due to the increasing industrial risk in this area, regulatory parties began to interfere in 2014, i.e., stage four. Out of pressure, in July 2015, the Chinese government issued the Guiding Opinions on Promoting the Sound Development of Internet Finance to regulate the rapid development of Internet finance. Hence, the rapid growth rate of P2P lending has declined since then.

P2P lending can function with less overhead, contributing to higher returns for lenders and lower interest rates for borrowers. However, as the lenders know the borrowers and invest based on the limited information given by P2P lending platforms, profitable P2P lending often entails a high risk of lending

due to information asymmetry. Therefore, assessing borrowers' credit risk and identifying non-creditable lenders becomes a significant issue for the P2P lending industry. The approaches used to determine the credit risk better (i.e., loan default prediction) are challenging to decide. P2P loans are also more stringent as most lenders on the market are non-experts with little experience and no formal training in evaluating lenders' value. In the meantime, the borrower community is complicated compared with conventional bank loan situations since the lack of compliance with credit requirements and borrowing does not enable any of the borrowers to accept traditional bank loans.

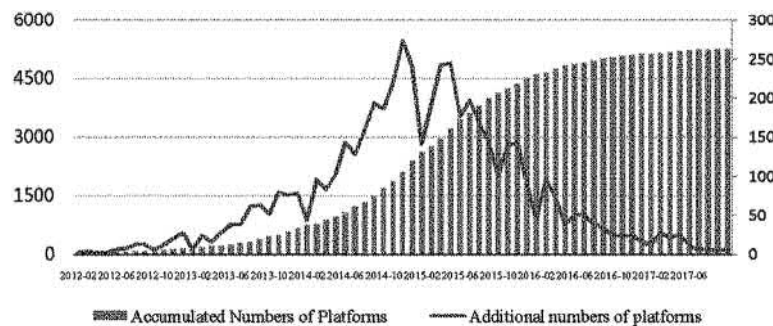
Although the regulations concerning P2P lending are more comprehensive since 2015, there remains some regulatory gaps and failures. Identifying these remaining regulatory gaps can help perfect the regulatory framework of P2P lending and make it serve the economic market in a better way.

Previous research in this area has identified several critical risks of P2P lending and possible solutions to establish the regulatory framework. Since the release of the relevant policies concerning P2P lending, several scholars have transferred their interest in reviewing the effectiveness of the policies issued. However, less work has been done to fix the prevailing issues and mitigating them. This Chapter provides a more detailed analysis and an examination of the Chinese legal framework related to P2P lending and identifying the vacuums in the existing framework.

The remainder of this chapter is organized as follows. Section 2 reviewed the related literature concerning the P2P lending industry's risk, the implication of economic theories such as information asymmetry, adverse selection and moral hazard in P2P lending, and discussion of the current policies. Section 3 discussed the detailed analysis of Ezubao, Hongling Capital, and China's current P2P regulatory framework. Section 4 reviewed the findings based on the identified vacuums in the study. In section 5, the author presented their conclusions briefly. In section 6, the author discussed policy implications for P2P lending by identifying three remaining regulatory vacuums, i.e., platform exit mechanism, legislations related to financial crime, and consumer education. Section 7 provided a brief conclusion and identified the limitations of the chapter and the future research focuses.

*Figure 1. Accumulated Numbers of platforms*

Source: [data.01caijing.com](http://data.01caijing.com)



## **2. LITERATURE REVIEW**

In this section, the author reviewed the literature related to the risk in P2P lending, relevant economic theories, and discussions of the current policies. In the end, the author identified how the chapter's findings add to the work in this area.

### **2.1 Risks in P2P Lending**

P2P lending, based on internet technology, shares knowledge, resource sharing, and capital flow between individuals. Many citizens who cannot receive structured funding from banks or other financial institutions are looking to meet their financing requirements by network loans. The new lending model had rapidly gained market acceptance since 2005, when Zopa, the world's first P2P loan platform, was developed in the UK. As of January 2016, in China, there are 3927 lending sites for P2P, with a total turnover of 1495,615 billion yuan. However, alongside this boom in the P2P lending sector, certain risks were also increased, especially in problem platforms; 1351 such platforms were reported in January 2016.

In addition to China's lack of supervisory bodies in P2P, imperfect legislation and regulations include outdated risk management strategies and expose P2P credit platforms to risk. The risks of networked lending platforms are high of change and spillover due to cross-business and integrated operations. As several small institutions with similar companies can be in trouble simultaneously or have similar implications, this can cause collective significance and lead to systemic risks (Wei & Zhang, 2016)

As a leading innovation, the emergence of P2P lending has inevitably brought many new types of risks into the lending industry. Understanding these unknown risks can be of help for regulators to form more effective regulation policies. Wang et al. (2015a) identified nine types of risks in the P2P lending industry: insufficient credit checking, inadequate intermediation, untimely repayment, lack of liquidity, lack of transparency, operational and technical failure, legal risk, excessive leverage, and lack of ethics. Yan et al. (2015) believe that credit risk is of the most important to be controlled in online lending and credit risk management of P2P lending depends on the platforms' ability to collect and analyze borrowers' credit information. Wei (2015) concluded that due to the Internet's inherent anonymity, the P2P lending sector might encounter fraudulent activities risks such as identity theft, consumer privacy loss, and data protection violations. Kevin and Jacob (2016) identified different risks faced by lenders and borrowers. For lenders, the risks include information asymmetry, investment illiquidity, and agency risks, while for borrowers, the main risk is privacy leaking. Furthermore, among all the risks that have been identified, many scholars, such as Qiu et al. (2012) and Wang et al. (2015b), recognize that information asymmetry is the fundamental problem in P2P lending where borrowers and platforms tend to have more information than lenders.

### **2.2 Related Economic Theories**

The information asymmetry between borrowers and lenders is a fundamental problem in the online P2P lending market: lenders or online platforms do not gauge the buyer's trustworthiness. Asymmetric information, such as moral hazards and adverse selection, can cause problems (Stiglitz & Weiss, 1981). In general, such issues can be mitigated and alleviated through various measures; banks can use the guarantee, daily reporting, and certified accounts in the traditional lending market to improve borrowers' trust. Enhancing and promoting borrowers' confidence would mitigate the issue of unnecessary selection

and moral hazards. Such processes are difficult to carry out in the online world due to their substantial transaction costs and the lack of physical interaction between borrowers and lenders. The loans of Peer-to-Peer (P2P) appear to be beneficial to lenders and borrowers. However, much fewer investors risk using this alternative financing (Suryono, Purwandari, & Budi, 2019).

Furthermore, information asymmetry, adverse selection, moral hazard, and agency problems frequently appear in the literature related to P2P lending. Ma, Zhou, and Hu (2017) recognized that information asymmetry is pronounced in the P2P lending market, which exacerbates adverse selection and moral hazard. Wang et al. (2015b) analyzed the relationship between the perceived reputations and trading trust, perceived information integrity and perceived information asymmetry, perceived information asymmetry, and lending intention. The author concluded that trading trust is influenced by reputation, perceived information integrity, and perceived information asymmetry, while perceived information asymmetry has no significant impact on lending intention. Yan et al. (2017) identified how signaling and search cost affected information asymmetry in P2P lending and traditional lending market and suggested a big-data way to reduce the level of information asymmetry. Weiss et al. (2010) discovered adverse selection effects on P2P lending platforms. Kevin and Jacob (2016) further identified the existence of agency relationship and problems in P2P lending. Zhang and Chen (2017) reviewed prior studies on how lenders exploit information from various sources to address moral hazard and adverse selection problems. They further discovered the existence of herding behavior in the P2P lending market.

## **2.3 Discussion of the Current Policies**

Since the publication of the ‘Guiding Opinions’ in 2015, many scholars showed great interest in discussing the effectiveness and potential improvement in terms of regulatory policies related to P2P lending. Cao (2016) reviewed the ‘Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions’ (the ‘interim measures’) issued by the China Banking Regulatory Commission in detail. The author highlighted several merits of the ‘interim measures’ and put forward some remaining risk areas that had not been covered by the policies. Huang et al. (2014) made a comparison about the regulation approaches between China and the UK and the U.S. Huang et al. (2014) further shed light on the improvement that can be adapted by Chinese regulators based on the experience of the UK and the US. Previous research work conducted by many scholars suggested the following ways of perfecting the current P2P lending regulation framework: clarifying main regulatory parties and their responsibilities, perfecting the market entrance and exit mechanism, perfecting the information disclosure, conducting comprehensive capital depository and improve industrial self-regulation (Ye 2014; Yu et al. 2015; Ding 2017). Most of the suggestions mentioned above have already been included in the latest policies. However, their effectiveness remains to be unseen. As for information disclosure, Zhang (2016) argued that the lack of information disclosure had led to the P2P lending deviating from information intermediary nature. Tu (2017) argued that most P2P platforms merely carried out capital depositories for window-dressing purposes.

In contrast, commercial banks are only committed to the depository provision of their own-interest platforms without recognizing their ability to provide the service, which still has regulatory holes. In December 2017, the National Internet Finance Association of China (NIFA) published ‘Internet Finance – P2P Loan – Specification of Loan Fund Depository Sector’ and ‘Internet Finance – P2P Loan – Specification of Loan Fund Depository System.’ To the best of the author’s knowledge, this is the first chapter to address these two policies’ implications.

## **2.4 Analysis - The Detriment of Regulatory Vacuums**

### **2.4.1 The Risk and Return**

P2P lending has many benefits compared to conventional lending institutions' loan transactions. The primary use of P2P lending is that borrowers can get a loan without collateral at a lower rate, while lenders can get better returns on their investments (Magee, 2011). Despite high returns on microfinance investment still challenged, P2P lending has drawn enormous numbers of investors discouraged by stock market returns and lower bank interest rates (Brennan & Kraus, 1987). Wall Street Journal reports that the leading P2P platforms have produced investors 10% or higher annual returns at historically low rates (Yum, Lee, & Chae, 2012). The next significant gain from P2P lending platforms is openness, flexibility, swift decision-making.

On the other hand, there is no risk-free investment or a P2P loan investment. The conventional position of lending risk assessment in the online P2P lending sector is left to individual lenders rather than financial institutions. There is also the risk of investors being misrepresented concerning their creditworthiness (Yum et al., 2012). The bulk of the loans sought are from borrowers who cannot access a loan from a bank. When a borrower does not repay the loan, it is appropriate to pursue a lawsuit at the cost of not recovering its entire loan. Also, there is a possibility that the P2P lending network would crash.

P2P lending has its merits in speed and simplicity for borrowers and attractive investors' returns (Verstein, 2011). It is supposed to be a financial alternative to Small and Medium Enterprises (SMEs) and individuals; they usually fail to obtain a loan from traditional banks due to a lack of credit guarantee or collateral assets, especially in China (Miriam 2015).

Nevertheless, P2P lending also has its risk for investors, such as default risk due to information asymmetry, investment illiquidity due to maturity matching of borrowers and investors, agency risk resulting from platform failure (Kevin & Jacob 2016). Moreover, the default risk in P2P lending is remarkably higher than in traditional banks (Gao et al., 2017). The risk is relatively lower for borrowers than investors, with privacy leaking being the borrowers' primary risk (Kevin & Jacob 2016). In the P2P lending market, many individual investors lack financial knowledge. In a pseudonymous online environment, the lending experience is lacking (Klaft, 2008)

In managing the risk of peer-to-peer lending, the most robust countermeasure is diversifying assets through various borrowers, creditors, and platforms. It reduces total uncertainty and exposure to loan defaults and bankruptcies, be it the issuer or site for the loan.

In addition to diversifying P2P investments among various borrowers, creditors and platforms, the investment portfolio should include other investment types than P2P lending. Indeed, P2P lending can only form a small part of the portfolio unless there is an exceptionally high-risk management profile and are a specialist in the field of peer lending.

### **2.4.2 The Case of Ezubao**

Because of the increasing number of enterprisers pumping into this sector and information asymmetry, investors found it increasingly hard to distinguish which platform is trustworthy. The nearly eight years' regulatory vacuums had led to substantial platform scandals such as cash shortage and loan default, fraud by posting false information online, run-away without repaying investors (Wei, 2015). Moreover, these kinds of platform failures have considerably driven up the systemic risk of the P2P lending industry. The

case of Ezubao vividly revealed the detriment of regulatory vacuums and demonstrated the necessity of regulation in respect of P2P lending.

Ezubao was an Internet platform operated by Jinyirong Internet Technology Ltd. In February 2014, Chengyu Group acquired this incorporation and made some transformations to the original Internet platform and began to run it as a P2P lending platform since July 2014. However, at the year-end of 2015, relevant police and finance regulation departments noted the irregularity in Ezubao's operation, and later investigations were conducted. The police found that Ezubao was experiencing high liquidity risk and severe cash flow problems through the inquiry. At the same time, Chengyu Group had started to transfer capital, destroy evidence, and several senior directors of the Group had fled without leaving a trace. Seemingly, Ezubao operated as a financial leasing firm, while what they were doing was to disguise the misappropriation by posting fake finance projects and false information relating to guarantee parties. Furthermore, at that time, regulations and policies concerning P2P lending were yet to emerge; thus, the expense of conducting criminals was too vague to deter illegal behaviors. As a result, Ezubao illegally raised around 50 billion RMB, and its victims spread 31 provinces around China (Pi & Xu 2016).

### **2.4.3 Agency Problems**

In P2P lending, operators manage the subsequent physical delivery to the investors of the borrowers' interest and principal repayments, thus creating a principal-agent relationship (Zhang & Chen 2017). Agency problems usually come with this kind of relationship as the two parties have different interests and asymmetric information. In contrast, an agent usually has more information than the principal, such that the principal cannot directly ensure that the agent is always acting in their best interest (Lucian & Jesse 2004). In the case of Ezubao, the agency problem is quite evident where the platform, atypically, enjoys a large income. Simultaneously, it costs investors a large sum of money to invest, and what the platform was doing was entirely in its interest, mainly investors'. Further, it is hardly possible for investors to obtain enough information concerning how they utilize their money. Hence information disclosure is of great significance when it comes to P2P lending regulation because information asymmetry is salient in this market (Zhang & Chen 2017).

### **2.4.4 Information Asymmetry**

Information asymmetry is typical economics in which one party has more or better information than the other, which creates an imbalance of power (Gustav & Marcus 2015). In the P2P lending business, the operators often have more information relating to borrowers' details, risk characteristics of loans, and operational risk of the platform itself. They do not have enough data to judge the authenticity of the projects posted online. In the case of Ezubao, the moral hazard problem arose with the platform illegally applied the borrowed funds to different tasks rather than those agreed, thus, to disguise the misappropriation. At the same time, investors suffered adverse selection as they could not distinguish among borrowers and investment projects with various credit risks due to lack of information disclosure. Moreover, this has resulted in nearly 900 thousand investors being cheated with the false finance project posted on Ezubao.

### 2.4.5 Impacts on the Whole Industry

This incident has had a significant effect on the Chinese P2P lending industry, and investigations are still pursued in the relevant provinces connected with this case. However, Ezubao is just one of the cases among the thousands of problematic platforms; the Table1 shows some typical challenging and problematic P2P platforms which exerted adverse influence on the whole industry.

*Table 1. Typical problematic platforms*

Name of the Company	Location	Date of the Incident	Default Loan / Illegally Raised Amount	Numbers of the Victims
Ezubao	A hui	12/2015	50 billion	Around 900 thousand
Zhongbao investment	Zhe jiang	3/2014	470 million	>1000
CDF-Capital	Shen zhen	11/2013	51.77 million	1325
China-Europe Winton Fund	Shen zhen	2/2014	400 million	>2000
Srong-online	Guang dong	2/2015	921 million	10837

Source: Wangdaizhijia, P2Peye.com

To a certain extent, these malignant incidents dampened investors' enthusiasm and harmed the entire industry, as well as potentially driving up the systemic risk of the whole industry. In P2P lending, unsystematic risk, such as fluctuation of interest rates, could be reduced by investing in different platforms and diversified projects in a small amount separately. Moreover, the borrowers participating in P2P lending are individuals and SMEs whose loan amount required is usually not that large, facilitating diversification. However, if the malignant events mentioned above stay unregulated and unmanaged, systemic risk is sure to increase where diversification of investment can no longer serve to reduce the risk. Nevertheless, as a positive endeavor to address SMEs and individuals' financing difficulties, P2P has its edges in breaking the bottlenecks in business financing and facilitating financial innovation (Lufax 2014). Hence regulations and guidance are required to enable the healthy development of the industry.

## 3. FINDINGS

The aggressive growth of P2P lending sectors, along with the rising of systemic risk due to the rapid emergence of problematic platforms and investors' fury, has exerted massive pressure on China's financial regulatory parties. Hence, in July 2015, the Chinese government issued the Guiding Opinions on Promoting the Sound Development of Internet Finance (the 'Guiding Opinions') to regulate Internet finance's rapid development. The 'Guiding Opinions' acknowledges Internet finance as a brand-new financial business model different from traditional banks. It sets out a series of policies and regulatory rules to encourage innovation and establishes the regulatory framework for different types of Internet



## **Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds**

finance, including P2P lending (Xie et al., 2016). Afterward, more and more detailed policies and regulations concerning Internet finance are unveiled accordingly. Table 2 outlines some necessary information and the main implications of the significant policies released in 2015. These policies covered three core areas of P2P lending regulations, i.e., capital depository, risk rectification, and information disclosure

*Table 2. Significant policies concerning Internet finance and their implications*

Title	Issuing Authority	Date Issued	Main Implications
<b>Guiding Opinions on Promoting the Sound Development of Internet Finance</b> (from now on referred to as the 'Guiding Opinions')	<b>the People's Bank of China (PBOC), the Ministry of Industry and Information Technology, the Ministry of Public Security, et al</b>	7/19/2015	<ul style="list-style-type: none"> <li>Individual online lending institutions shall specify the nature of information intermediary and shall not provide credit enhancement services or conduct illegal fund-raising.</li> <li>The online lending business shall be subject to the supervision of the China Banking Regulatory Commission</li> </ul>
<b>the Implementation Plan for Special Rectification on Risks in Internet Finance</b> (the 'rectification plan')	<b>the General Office of the State Council</b>	4/12/2016	<ul style="list-style-type: none"> <li>The P2P online lending platform shall not set up a pool of funds, shall not grant loans, shall not raise funds illegally, shall not raise funds, shall not provide a guarantee for itself, shall not mislead lenders, and shall not conduct offline marketing</li> </ul>
<b>the Implementation Plan for Special Rectification on Risks in P2P Lending</b> (the 'rectification plan for P2P')	the China Banking Regulatory Commission (CBRC), et al.	4/13/2016	<ul style="list-style-type: none"> <li>Support and keep regulating those complied with 'Guiding Opinions'</li> <li><b>Require those lack of compliance to rectification</b></li> <li><b>Ban those seriously violated relevant law and regulations</b></li> </ul>
<b>Interim Measures for the Administration of the Business Activities of Online Lending Information Intermediary Institutions</b> (the 'interim measures')	the China Banking Regulatory Commission (CBRC), et al.	8/17/2016	<ul style="list-style-type: none"> <li>Recordation Administration</li> <li>Business Rules and Risk Management</li> <li>Protection of Lenders and Borrowers</li> <li>Information Disclosure</li> <li>Supervision and Administration</li> <li>Legal Liability</li> </ul>
Guidelines for Registration of <b>Online Lending Information Intermediary Institutions</b> (the 'guidelines for registration')	the China Banking Regulatory Commission (CBRC), et al.	11/28/2016	<ul style="list-style-type: none"> <li>Recordation and registration with the local financial regulatory department should be conducted within ten working days after obtaining the business license.</li> </ul>
Guidelines for Fund Depository of <b>Online Lending Information Intermediary Institutions</b> (the 'guidelines for fund depository')	the China Banking Regulatory Commission (CBRC), et al.	2/22/2017	<ul style="list-style-type: none"> <li>The practicing institutions shall choose qualified banking financial institutions as capital depository institutions, manage and supervise clients' funds, and set up separate accounts to address clients' funds and practicing institutions' funds.</li> </ul>
Guidelines for Information Disclosure of <b>Online Lending Information Intermediary Institutions</b> (the 'guidelines for information disclosure')	the China Banking Regulatory Commission (CBRC), et al.	8/25/2017	<p>Information such as:</p> <ul style="list-style-type: none"> <li>the operation and management of business activities</li> <li>periodically disclose annual reports</li> <li>laws and regulations</li> <li>relevant online lending regulatory provisions should be disclosed in a separate and clear section on its website</li> </ul>

Source: [cbrc.gov.cn](http://cbrc.gov.cn); [en.pkulaw.cn](http://en.pkulaw.cn)

### 3.1. The Pertinence and Effectiveness of the Current Policies

#### 3.1.1 Overall Impact

With the increasingly tightened regulations and implementation of rectification plans, the rapid growth rate of the P2P Lending sectors in respect of platforms' volume (Figure2) and business turnover together with an industrial interest rate (Figure3) has slowed down and tended to level off as shown in the figures below.

Figure 2. Additional numbers of platforms

Source: [data.01caijing.com](http://data.01caijing.com)

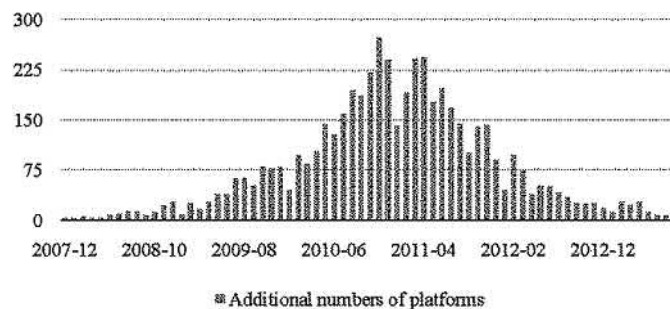
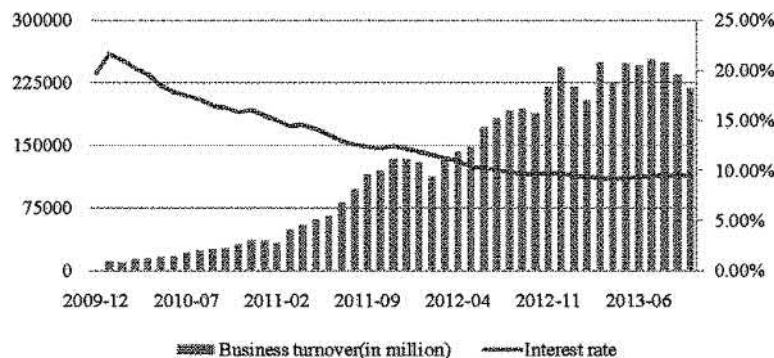


Figure 3. Business turnover and interest rate of the P2P platform

Source: [shuju.wdzt.com](http://shuju.wdzt.com)



#### 3.1.2 Merits and Drawbacks of the 'Interim Measures'

The 'interim measures' released by CBRC in August 2016 was the first comprehensive policy concerning online lending. In response to the risk and problems that had already been revealed in P2P Lending sectors, Article 10 of the 'interim measures' ruled that individual online lending institutions shall only operate as an information intermediary. Moreover, and shall not provide credit enhancement services or conduct illegal fund-raising. With this Article, the situation such as 'self-guarantee' and 'self-lending' occurred in Ezubao's case is expected to be avoided (Cao 2016). As stated by Wang & Huang (2017) in

Field Study Report on American Financial Technology, it is hard for P2P lending to act entirely as an information intermediary, even in the US. It is even harder to realize in China, for the culture of credit and credit reference system are still underdeveloped. Thus, the information asymmetry approach cannot eliminate the platform's risk; it only transfers the investors' risk. Hence, the information intermediary process does not mean the platform should take no responsibilities in platform risk. In contrast, the regulatory policies should clarify that P2P platforms should bear the burdens of investors' rating risks.

In Article 17, the policy set the upper limit of 200,000 yuan for the balance of loans of the same natural person on a different platform and one million for total compensation on all platforms that concerned. Also, it set the upper limits of one million and five million yuan for the same legal person or any other organization under the same conditions. This Article aims to limit the capital to be raised on platforms to a small amount, thus prevents default cases with massive outstanding amounts. At the same time, it still, satisfy the financial needs of SMEs and individuals (Luo et al. 2016).

### 3.1.3 The Impact of 'Rectification Plan'

With the implementation of the 'rectification plan,' it requires platforms to rectify the lack of compliance to conduct relevant process to meet the regulatory requirement, the operating cost and compliance cost of running P2P lending business. These are increased as additional costs relating to auditing, website management, information disclosure, and contract with bank depository could arise. Due to the growing cost of compliance and operating pressures, an increasing number of platforms are recorded as problematic platforms, as reflected in Figure 4. Due to the lack of regulations concerning platform exit, a considerable number of platforms that are unable to meet the compliance requirement simply fled the industry without conducting necessary liquidation or administration procedure, leaving a substantial amount of loans unpaid. According to the data released by Wangdaizhijia, up to September 2017, among the 3,925 accumulated problematic platforms, 1,167 were recorded as 'run-away' incidents, accounting for 29.7% of the total number.

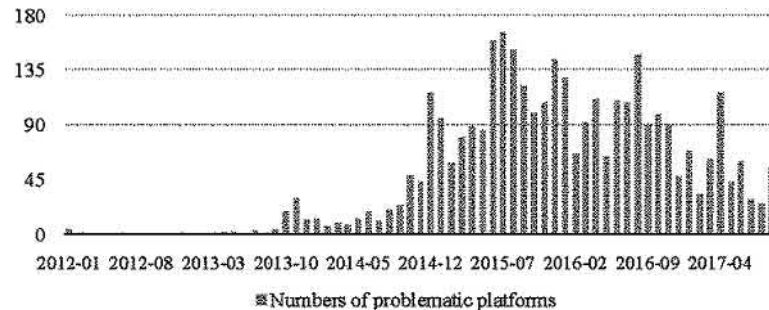
On December 8, 2017, the office of P2P rectification issued the notification for check and acceptance on P2P lending. This notification's critical point was that it specified the deadline for rectification and compliance check, i.e., April 2018 for major platforms and June 2018 for all the other platforms. Many investors are concerned about their funds in platforms that might not pass the rectification check and acceptance. However, according to the notification, the consequence of failing to meet the compliance requirement will vary depending on the platform's performance during the rectification period. If the platforms behaved well and showed cooperation during the rectification period, it allowed them to deal with their remaining business, i.e., gradually, they could still perform the successfully matched loan contract. While for platforms that showed non-cooperation during the rectification period, it will apply an immediate ban, and the investors' fund will suffer.

### 3.1.4 Capital Depository

Since the 'Guiding Opinion' in 2015, the regulatory parties have always emphasized that P2P lending should be of information intermediary nature and shall not assume credit enhancement services or conduct illegal fund-raising. Theoretically, as a pure information intermediary, a P2P lending platform should simply screen and publish borrowers' needs on the platform. The loan contract is primarily between the borrower and the lender. However, as mentioned in 3.1.2, to make P2P lending platforms operate as pure

*Figure 4. Additional numbers of platforms*

Source: [data.01caijing.com](http://data.01caijing.com)



information intermediary in China is far from easy as the culture of credit and credit reference system is still underdeveloped (Wang & Huang 2017). Hence, to attract investors, considerable numbers of platforms use part of the funds from the investors or capitals from the third party to meet the rigid payment when they default. Furthermore, the funds retained by the platform are subject to misappropriation. Many scholars have suggested a bank depository way to ensure investors' funds' safety in response to this.

The policies concerning bank depository in P2P lending experienced three stages.

The 'interim measures' issued in 2016 mentioned the requirement of capital depository in terms of P2P lending. Later, the 'guidelines for fund depository,' released in February 2017, gave additional depository guidance. Table3 summarizes the primary articles of the 'Guidelines for fund depository' and their implications.

On August 24, 2016, CBRC mentioned the bank depository requirement to the issuance of fund depository guidelines. Only 209 operating platforms announced that they had signed the direct fund depository contract with qualified commercial banks, which only accounted for 8.75% of the total platforms (Source: Wangdaizhijia). Shen (2017) argued that the core reason behind the low rate of completion of bank depository lies with commercial banks' concerns about being influenced by the risks brought by P2P lending. The fund depository guidelines also specify and emphasize the bank's responsibility, scope, and independent status as a depository party to enhance cooperation. Furthermore, up to December 25, 2017, according to Wangdaizhijia, 655 platforms completed bank depository constituting 34.11% of the total platforms.

To further encourage commercial banks to serve as depository institutions for P2P platforms, Article 12 of the 'guidelines for fund depository' also foregone the depository requirement. This Article had brought many disputes. Consequently, commercial banks agreed on the depository requirement from the platforms out of self-interest without considering their capability to provide this service (Tu 2017), leading to the false depository or partial depository. Moreover, as revealed on Wangdaizhijia, 15 platforms with bank depository backgrounds have been recorded as problematic incidents.

**In December 2017**, NIFA issued 'Internet Finance P2P lending Specification of lending fund depository business' and 'Internet Finance-P2P lending Specification of lending fund depository system' to mitigate the associated concerns. These two regulatory documents start a new era of bank depository of P2P lending. Article 5.3.8 suggests that depository banks shall ensure control mechanisms and data analysis models. When the deposited platforms show irregularities, the depository bank shall report to the regulatory parties. The depository businesses will also ascertain that commercial banks must have a

depository service and must pass the review stage by the National Internet Finance Association of China. Since commercial banks cannot meet the requirement, thus P2P platforms that have signed depository contracts with the problematic depository, banks to make a change. Since Bank depository is a core factor determining whether a platform can successfully be registered and recorded, this policy also has a considerable influence on whether a platform can meet the compliance requirement.

*Table 3. Main articles of the ‘Guidelines for fund depository’ and their implications*

Articles	Implications
<b>Nature of the fund depository bank:</b>	
Article 2: Qualified commercial banks shall serve as fund depository bank of online lending	<ul style="list-style-type: none"> <li>• Only commercial banks can serve as fund depository banks.</li> <li>• The United depository model encompasses commercial banks that are in control of accounts and capital depositories. Furthermore, an independent third party takes control of the account, and technical support is banned.</li> </ul>
<b>The legal state of the fund depository bank:</b>	
Article 2: Fund depository bank provides no guarantee for online lending transactions and shall not be liable in terms of loan default.	<ul style="list-style-type: none"> <li>• Also, it specifies the independent state of the bank depository bank.</li> <li>• Relieve commercial banks’ worry about being influenced by the risk of P2P lending, thus increasing cooperation.</li> </ul>
<b>The requirement to be met for a fund depository bank:</b>	
Article 10: (1) Specify the primary department responsible for fund depository and management. The establishing of the department should ensure the independence and completeness of the depository operation. (2) The commercial bank shall have a sound credit record (3) The ability to provide investors with the functions to check the information of the fund account	<ul style="list-style-type: none"> <li>• Provided a fundamental way to consider whether a commercial bank satisfied the requirement to be a qualified fund depository bank.</li> </ul>
<b>Responsibility of fund depository bank:</b>	
Article 12: (1) Provide depository report regularly according to relevant legislation and depository contract to client. (2) Properly retain the transaction data, account information, depository report concerning bank depository operation for at least five years (3) Disclose deposited platforms’ transaction scale, remaining loan amount, depository amount, numbers of lenders, and borrowers regularly.	<ul style="list-style-type: none"> <li>• It also showed a loose approach towards bank depository, thereby allowing commercial banks to reduce operational costs.</li> <li>• Sensitive information such as default rate, rate of the non-performing loan, and lending cost will not be required to disclose, thus reducing depository bank’s cost of information disclosure.</li> </ul>
<b>Responsibility of deposited platforms:</b>	
Article 9: (1) Properly retain the transaction data, account information, depository report concerning bank depository operation for at least five years (2) Arrange for independent audit on clients’ fund account and report to the client (3) Cooperate with depository bank in filing their duty of anti-money laundry	<ul style="list-style-type: none"> <li>• Deposited platforms are supposed to be more actively involved in performing their duties to protect investors’ funds.</li> </ul>

Source: Wind, CIB Research, Huatai Securities

## Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds

Table 4. Problematic platforms with bank depository background

Name of the Platform	Depository Bank	Incident
Xuexindai	Zhejiang Mintai Commercial Bank	Cash shortage
Putian Anjin	Hengfeng Bank	Cash shortage
Lala Caifu	Huishang Bank	Cash shortage
Hehai Finance	Huaxing Bank	Cash shortage
Ronghedai	Guizhou Bank	Run-away
Dasheng Licai	Guizhou Bank	Cash shortage
Zhongzhi Mofang	Hengfeng Bank	Run-away
Donghong Finance	Hengfeng Bank	Cash shortage
Aitou Yidai	Tianfu Bank	Cash shortage
Yiqi Jucai	Huaxing Bank	Cash shortage
Kuying Net	Huishang Bank	Cash shortage
Xiang Dangdang	United Bank of Haikou	Run-away
Tuotudang	Guizhou Bank	Cash shortage
Guocheng Finance	Zhejiang Commercial Bank	Cash shortage
Chengxindai	Huaxing Bank	Cash shortage

Source: Wangdaizhijia

Further, the three stages of the policy development concerning capital depository revealed regulatory parties' determination to eliminate rigid payment in P2P lending. As mentioned before, as a pure information intermediary, the platform shall not retain any capital from investors or gain capital from other sources to meet the rigid payment when the borrowers default. However, eliminating rigid payment in the Chinese P2P lending market is 'yet' not a very sound choice due to the relatively low return of P2P lending than the high risk of the industry, significant information asymmetry, and incomplete credit reference system, and the lack of investors education.

### 3.1.5 Information Disclosure

As mentioned above, information asymmetry is a typical phenomenon in P2P lending, and information asymmetry is one of the significant risks faced by P2P investors. Furthermore, the lack of information disclosure had led to the P2P lending deviating from information intermediary nature (Zhang 2016). Zhang (2016) argued that most P2P platforms operate in a 'safety promise' pattern due to a lack of information disclosure. He used the game theory approach to prove that if the information disclosure is adequate, the platform's best choice is not to provide safety promise for investors. On the other hand, in the case of inadequate information disclosure, the game's equilibrium is that the platform must provide safety guarantees for investors or not engage in P2P lending. In the latter scenario, the platforms' operating expense will increase, but the industry's systematic risks will accumulate.

To protect the potential investors and let P2P lending move back to an information intermediary nature, the 'guidelines for information disclosure' requires P2P operators to disclose information concerning its registration detail, organization structure, project information, auditing information, potential risk, and

others. The website and other social media allow investors to diminish information asymmetry between the platform and investors. However, according to Wangdaizhijia, up to September 2017, only less than 100 platforms have met half of the requirement regarding information disclosure. There is still a long way to go before platforms can fully satisfy the CBRC's requirement in terms of this area.

The desperate status quo of insufficient information disclosure in China's P2P lending may partly lie with the underdeveloped credit system (Wei, 2015). Even the most mature credit reference system, i.e., the Credit Reference Center of The People's Bank of China, has covered only 800 million individuals. The significant population with stable economic capability is only 300 million. The remaining 500 million people only record the necessary information in the center (Source: Wind).

However, as an endeavor to address the problem, in December 2017, the People's Bank of China (PBOC) has decided to establish an individual credit information database called 'United information' ultimately controlled by the central government with the joint contribution of the NIFA, Ali Finance, Tencent and others. For a long time, most individual credit references are conducted by an independent institution such as Ali Finance or Tencent, as mentioned above. However, as independent institutions, an individual's credit data is isolated, which means a person with a good credit record in Ali Finance may not be recognized by the Tencent credit system or *vice versa*. This kind of inconsistency is the result of a lack of data sharing. With the establishing of 'United information,' data isolation can be well addressed, and P2P lending will benefit from it as borrowers identified default would be marked in the system. His borrowing behavior will be limited by every platform that has access to his credit history. Moreover, this loss of credit will further influence other life aspects of the borrowers. At the same time, an investor could also have a more reliable source to screen investment projects and make sound decisions based on the potential borrowers' credit history.

## **4. DISCUSSION**

The current policies have covered several risk areas relating to P2P lending by implementing capital depository, information disclosure, industry entry limitation, and 13 red lines concerning operating activities.

Furthermore, as mentioned above, the aggressive growth rate of P2P lending platforms has already been under control with the policies' setting. Nevertheless, evidence has reflected that even platforms that showed good compliance and background are being marked as problematic platforms. According to incomplete statistics based on P2Peye, from January 2017 to October 2017, among the 274 problematic platforms, 48 platforms have backgrounds such as bank depository, ICP permit, and memberships of Internet Finance Association. Typical problematic platforms with good backgrounds are listed in Table 5.

Most of the current policies are set to protect investors. However, evidence has demonstrated that some regulatory vacuums remain in P2P lending, and the current policies themselves have already revealed some possible regulatory failures. Furthermore, investors' enthusiasm and confidence towards the P2P lending market have been harmed, as reflected in the reducing number of investors since August 2017. It is also the first time that the number of borrowers exceeds the number of investors. (Figure 5) This kind of situation calls for perfecting the current regulations.

## Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds

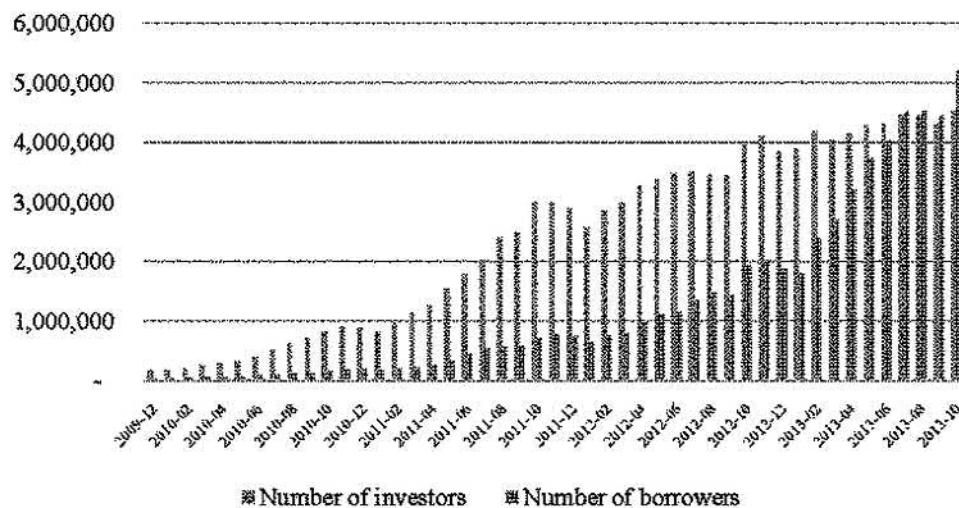
Table 5. Problematic platforms with good background

Name of the Platform	Background	Incident	Date of the Incident
Xuexd	<ul style="list-style-type: none"> <li>• Bank depository</li> <li>• ICP</li> <li>• Internet Finance Association (Nanning City): member</li> <li>• Venture Capital</li> </ul>	Cash shortage	09-18-2017
Dangpoo	<ul style="list-style-type: none"> <li>• Bank depository</li> <li>• ICP</li> <li>• State-owned Capital</li> </ul>	Run-away	09-25-2017
99Caifu	<ul style="list-style-type: none"> <li>• Listed: Share code:300167</li> <li>• Venture Capital</li> <li>• State-owned Capital</li> <li>• ICP</li> </ul>	Cash shortage	09-13-2017
Hehai Finance	<ul style="list-style-type: none"> <li>• Bank depository</li> </ul>	Cash shortage	08-01-2017
Miaozi Finance	<ul style="list-style-type: none"> <li>• Internet Finance Association member of China: member</li> </ul>	Police Interfered	08-09-2017

Source: P2Peye.com

Figure 5. Number of investors and borrowers

Source: [shuju.wdzj.com](http://shuju.wdzj.com)



### 4.1 Platform Exit

One of the most significant vacuums is the lack of detailed platform exit regulations when the platform is faced with going concern problems. As mentioned above, with the increasing compliance cost and operating pressure due to scrutiny, most of the problematic platforms fled without repaying investors. However, Article 24 of the interim measures that when an online lending institution is terminated, it shall appropriately handle existing loan businesses and the liquidation matters according to relevant laws and regulations. Besides, the current 'PRC Enterprise Bankruptcy Law' and 'Company Law of



PRC' themselves have considerable vulnerabilities in private financial markets, which further calls for perfecting the exit mechanism of P2P lending (Ding 2017).

However, platforms do exist where platforms did not run away from their responsibilities and set good examples concerning platform exit and shed light on relevant policy settings.

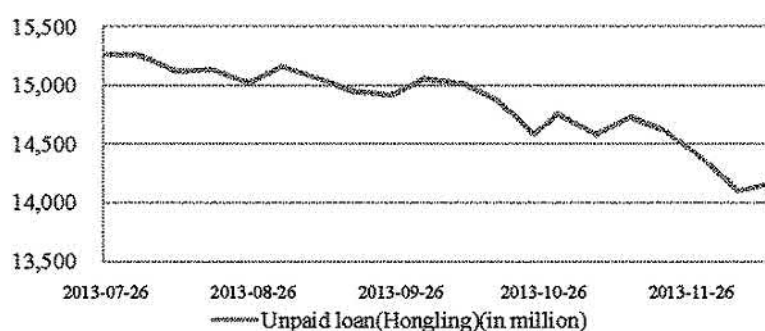
#### **4.1.1 Case of Hongling Capital**

Hongling Capital is an old and successful incorporation that began to conduct P2P lending in March 2009 in Shen Zhen. Up to October 31, 2017, Hongling has accumulated a business turnover of nearly 288 billion, 127,982 borrowers, and 530,264 investors (Source: [data.01caijing.com](http://data.01caijing.com)). However, on July 27, 2017, Zhou Shiping, the legal representative and chairman of Hongling, made a post on Hongling's bulletin board system, informally stating that Hongling will liquidate its online lending operations within three years. Four days later, at the conference relating to Hongling's strategic transformation, Zhou Shiping formally declared the liquidation plan, and an explanation concerning this event was made to the media. As claimed at the conference, Hongling had been on the way to dispose of its non-performing assets. Three years were anticipated before completing the whole liquidation procedures, with the commitment that Hongling would act in the investors' best interest. 'The liquidation decision concerning P2P operation is mainly due to the frequent bad debts and increasing cost of compliance faced by Hongling since 2015, as stated by Zhou Shiping at the conference.

Currently, Hongling is continuing its general operation, and information relating to its P2P business's liquidation process keeps updating on the website. Moreover, the amount of unpaid loans is declining since July 27, 2017, as reflected in figure 6, which suggests that Hongling is trying its best to repay its investors.

*Figure 6. Unpaid loan amount of Hongling Capital*

Source: [data.01caijing.com](http://data.01caijing.com)



#### **4.1.2 Regulation Moves Towards Platform Exit**

Just two months later, on September 29, 2017, the first policy concerning platform exit in respect of online lending, i.e., 'Guidelines for Exit Requirement of Online Lending Information Intermediary Institutions (draft)' (the 'guidelines for exit') was released by the Internet Finance Association of Shen Zhen. Although the policy is applied only to Shen Zhen, it has shed light on the overall policy. In response to

the platform's problem fled, Article 4 of the policy ruled that the operating location shall not change during the exit process. The platform's website shall not shut down, and the platform's senior officers shall not be out of contact. Article 5 and 6 made it clear that an exit plan and a group to conduct this procedure should be formed. Article 7 ruled that information such as reasons for the exit, volume of the unpaid loan, and disposal plan concerning non-performing assets shall be disclosed to the investors. This Article prevents platforms from leaving the market for reasons other than going concern problems.

#### **4.1.3 Regulations Concerning Platform Exit in Foreign Countries**

The United Kingdom is the first country in the world that witnessed the emergence of the P2P lending platform, i.e., Zopa, in 2005 (Ulrich & David 2016). Moreover, it has a relatively sounder regulatory system relating to the P2P lending sector.

In terms of firm failure, the FCA's 'Regulatory Approach to Crowdfunding over the Internet and the Promotion of Non-readily Realisable Securities by other Media' ruled that platform operators shall create programs that ensure loans can be managed to maturity in case of platform failure (Tarun et al. 2015). Moreover, according to the 'Peer-to-Peer Finance Association Operating Principles,' the operators shall make plans such as administration or mergers before bankruptcy to ensure that the loan contract is still enforceable and managed appropriately. Relevant workforce and senior officers shall remain in contact to conduct the repaying process (Zheng et al., 2014).

#### **4.2 Case Report of Financial Crime**

On December 18, 2017, Beijing No. 3 Intermediate People's Court and Beijing Finance Work Bureau, and the National Internet Finance Association of Beijing held a news conference to report the lawsuit related to online lending heard at Beijing No.3 Intermediate People's Court. The data and information from the court revealed that:

1. The cases are mainly related to the loan contract. Statutorily, P2P lending is of civil lending nature, and the defendant and claimant should be limited to the lenders and borrowers. However, as the cases show, most cases involved the claimant requiring the platform to conduct the rigid payment rather than directly claiming damages from the borrowers. This phenomenon further suggested that the 'safety promise' pattern rather than the information intermediary pattern can bring a huge risk to the platform itself.
2. In the resolved cases, as the value of the incident is generally small, over 50% of cases received the result by civil procedure bulletin with both defendant and even claimant unwilling to go to the court. Furthermore, the appeal rate is only 0.3% compared with the 6.5% appeal rate of standard loan civil cases.
3. The legislation lacks reviewing electronic evidence, which made it even harder to decide the cases.
4. Some cases are of both civil and criminal nature, e.g., Ezubao, which also made some cases hard to be assessed.

## **5. POLICY IMPLICATIONS**

Due to the complicated legal nature of P2P platforms and lack of substantial evidence, many police authorities are either unwilling or unable to file the cases reported by the investors, especially for platform run-away incidents. As data released by Wangdaizhijia, 1171 accumulated platforms, up to December 26, 2017, have been identified as run-away incidents, and only 26 cases have caused attention. Furthermore, it is a very upsetting status quo for investors.

However, on December 20, 2017, the Supreme People's Procuratorate, the Ministry of Public Security issued the 'Regulations on standardizing public security to deal with financial crime cases and investigation measures.

The regulation made it clear that Public Security authorities must receive and record the cases related to financial crime report or accusation regardless of their jurisdiction and shall not decline the cases for this reason (Article 14). This new policy specifies the public security's responsibility for financial crime and provides investors a safeguard when the platform acts against them.

Nevertheless, the policy is of broad scope. When it comes to P2P lending, a more specific case report, and trial procedure should be established. As mentioned above, as online lending, the evidence used for a legal purpose is minimal.

### **5.1 Consumer Education**

Another regulatory vacuum that is of great importance but hardly mentioned is consumer education. Many cases could suggest a lack of consumer education in P2P lending in China. For example, on December 17, 2017, one of the capital custodies projects on Lufax became overdue, with 1400 million unpaid affecting 118 investors. Lufax is one of the most successful institutions that conducting P2P lending business. Furthermore, many investors simply regard Lufax as a pure P2P platform; however, P2P business is just one of the Internet finance businesses that Lufax conducted. Moreover, the overdue project is a capital custody project which had nothing to do with P2P lending.

Zhang and Chen (2017) identified herding behavior in China's P2P lending market. Herding behaviors and significant information asymmetry make consumer education more critical and necessary. Without proper guidance, investors may simply engage in P2P lending without knowing the risks and may even do not know how to protect themselves when they get cheated.

There is no formal website or institution that provides investors with the necessary investing guide in P2P lending. Future policy settings should specify a responsible party to give necessary consumer education to potential investors regularly. For example, the National Internet Finance Association of China could publish a review on the general development of P2P lending weekly, or the P2P platform itself should take this responsibility and provide an investing guide and remind them of the potential risk.

## **6. CONCLUSION**

Unlike the UK and the US, P2P lending in China is still at a competition stage due to the previous years' lack of regulations. The regulatory vacuums have led to the accumulation of systematic risk of the P2P industry. However, as an effective solution to address SMEs and individuals' financing difficulties, P2P

has its unreplaceable merits; thus, regulations need to be perfect to guide the healthy development of P2P lending.

Because P2P lending is at the crossroads of many sectors, such as the Internet and finance, a regulatory void is easy to shape and lead to problems including conflicting industry standards, market dominance, and unequal distribution, which are not conducive to successful industry growth. P2P lending is an advancement in Internet finance and discovery. The government must regulate P2P lending to encourage industry innovation, enhance the transparency of new financial products, protect both borrowers and lenders, offer adequate protection to all market players, and strictly prohibits fraud. If this issue of market control over P2P lending gets resolved successfully, and the formal legal status of P2P lending companies is achieved, in that case, this will help address the growing problems of the P2P lending industry. It will further provide experience and solutions to regulatory enforcement concerns in Internet finance and other fields.

In this chapter, the author thoroughly reviewed the regulation development in terms of P2P lending in China and analyzed the current policies' pertinence and effectiveness. The author concluded that the rapid growth rate of the P2P lending sectors has slowed down and tended to level off, but there remain some risky areas that the current policies have not covered. The chapter's theoretical contribution is to the implications of the latest development of regulatory changes and the established individual credit reference system. The chapter also discovered three new regulatory vacuums, i.e., platform exit, a case report of financial crime, and consumer education, thus shed light on the future approach towards perfecting the regulatory framework.

However, the chapter does have its limitations. Due to the limited time of the policies issued, it is hard to obtain sufficient data and analyze its fundamental influence in a more quantified way. Future studies in this area could focus on how the new individual credit reference system helps reduce the information asymmetry in P2P lending and how P2P lending could gradually move back to an information intermediary nature without harming the investors (Bholat & Atz, 2016).

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

- Barberis, J., & Arner, D. W. (2016). FinTech in China: From Shadow Banking to P2P Lending. In *Banking Beyond Banks and Money*. New Economic Windows (pp. 69-96). Springer.
- Bebchuk, L., & Fried, J. (2009). *Pay without performance: The unfulfilled promise of executive compensation*. Harvard University Press.
- Bholat, D., & Atz, U. (2016). *Peer-to-Peer lending and Financial Innovation in the United Kingdom* (Working paper No. 598). Bank of England. Retrieved from <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/peer-to-peer-lending-and-financial-innovation-in-the-uk.pdf?la=en&has=h=731A6951C1EEFF82BEBC281516E464139D996743>
- Brennan, M., & Kraus, A. (1987). Efficient Financing Under Asymmetric Information. *The Journal of Finance*, 42(5), 1225–1243. doi:10.1111/j.1540-6261.1987.tb04363.x
- Buckley, R., Arner, D., & Barberis, J. (2016). The Evolution of Fintech: A New Post-Crisis Paradigm? *Georgetown Journal of International Law*, 47, 1271–1319. doi:10.2139/ssrn.2676553
- Davis, K. T., & Murphy, J. (2016). Peer to Peer lending: structures, risks and regulation. *JASSA: The Finsia Journal of Applied Finance*, 2016, 3–37.
- Gao, Y., Sun, J., & Zhou, Q. (2017). Forward looking vs backward looking: An empirical study on the effectiveness of credit evaluation system in China's online P2P lending market. *China Finance Review International*, 7(2), 228–248. doi:10.1108/CFRI-07-2016-0089
- Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, 35(1), 220–265. doi:10.1080/07421222.2018.1440766
- Guofeng, D. (2017). Legal Regulation of Alienation Operation of P2P Net Loan Platforms. *Journal of Shanghai University of Finance and Economics*, 19(4), 105–117.
- Huang, Z., Deng, J., Xiong, M., Ren, Y., & Qiao, Y. (2014). Comparisons of P2P Regulatory Systems between USA, UK and China's P2P Regulatory Policies. *Financial Regulation Research*, 10, 4.
- Klaft, M. (2008a). Online peer-to-peer lending: A lenders' perspective. In H. R. Arabnia, & A. Bahrami (Eds.), *Proceedings of the International Conference on E-Learning, E-Business, Enterprise Information Systems, and E-Government* (pp. 371–375). London: CSREA Press
- Lin, Y., Canhua, K., & Long, W. (2015). Study on Internet Financial Supervision Game: A Case Study of the P2P Net Loan Mode. *Nankai Economic Studies*, 2015(5), 126–139.
- Lufax. (2014). *White paper: P2P Lending Market in China*. Retrieved from <http://blog.lendit.com/wp-content/uploads/2015/04/Lufax-white-paper-Chinese-P2P-Market.pdf>
- Luo, Y., Shen, J., & Liu, X. (2016). *New policy of P2P lending guides healthy development of the industry: A detailed review and research on P2P interim measures*. Beijing: Huatai Securities. Retrieved from <https://www.htsc.com.cn>

## **Regulatory Developments in Peer-to-Peer (P2P) Lending to Combat Frauds**

- Ma, B., Zhou, Z., & Hu, F. (2017). Pricing mechanisms in the online Peer-to-Peer lending market. *Electronic Commerce Research and Applications*, 26(6), 119–130. doi:10.1016/j.elerap.2017.10.006
- Magee, J. R. (2011). *Peer-to-Peer Lending in the United States: Surviving after Dodd-Frank* (Working Paper No. 9). North Carolina Banking Institute. Retrieved from <https://go.gale.com/ps/anonymou?id=GALE%7CA254244467&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=10967249&p=AONE&sw=w>
- Pi, H., & Xu, Z. (2016). *Summary report of Financial product for the year ended December 2015*. Ka-rachi: Fortune Securities. Retrieved from <https://www.fortunesecurities.com/>
- Qiu, J., Lin, Z., & Luo, B. (2012). Effects of borrower-defined conditions in the online peer-to-peer lending market. In M. J. Shaw, D. Zhang, & W. T. Yue (Eds.), *E-life: web-enabled convergence of commerce, work, and social life* (pp. 167–179). Springer. doi:10.1007/978-3-642-29873-8\_16
- Segal, M. (2015). Peer-to-Peer Lending: A Financing Alternative for Small Business. *Issue Brief*, 10, 1–14.
- Serrano-Cinca, C., Gutiérrez-Nieto, B., & López-Palacios, L. (2015). Determinants of default in P2P lending. *PLoS One*, 10(10), 1–22. doi:10.1371/journal.pone.0139427 PMID:26425854
- Shen, J. (2017). *A review and comment on Guidelines for Fund Depository of Online Lending Information Intermediary Institutions*. Beijing: Huatai Securities. Retrieved from <https://www.htsc.com.cn>
- Stiglitz, J. E., & Weiss, A. (1981). Credit rationing in markets with imperfect information. *The American Economic Review*, 71(3), 393–410.
- Suryono, R. R., Purwandari, B., & Budi, I. (2019). Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review. *Procedia Computer Science*, 161(15), 204–214. doi:10.1016/j.procs.2019.11.116
- Tengvall, M., & Claesson, G. (2015). *Peer-to-peer lending: the effects of institutional involvement social lending* (Master's thesis, Jönköping University). Retrieved from <https://www.diva-portal.org/smash/get/diva2:812631/FULLTEXT01.pdf>
- Thornton, G. (2014). *Alternative lending: a regulatory approach to peer-to-peer lending*. Academic Press.
- Tu, L. (2017). Commercial banks' involvement in P2P lending; present dilemma and response. *Financial Market*, 555, 56–59.
- Verstein, A. (2011). The Misregulation of Person-to-Person Lending. *University of California Davis Law Review*, 45(2), 445–530.
- Wang, J., & Huang, Y. (2017). Field Study Report on American Financial Technology. Institution of Digital Finance, Peking University & Shanghai Finance Institute.
- Wang, J. G., Xu, H., & Ma, J. (2015). *Financing the Underfinanced*. Springer. doi:10.1007/978-3-662-46525-7
- Wang, P., Zheng, H., Chen, D., & Ding, L. (2015). Exploring the critical factors influencing online lending intentions. *Financial Innovation*, 1(1), 1–11. doi:10.1186/40854-015-0010-9

- Wei, Q., & Zhang, Q. (2016). P2P Lending Risk Contagion Analysis Based on a Complex Network Model. *Discrete Dynamics in Nature and Society*, SI, 1-8. doi:10.1155/2016/5013954
- Wei, S. (2015). Internet lending in China: Status quo, potential risks and regulatory options. *Computer Law & Security Review*, 31(6), 793–809. doi:10.1016/j.clsr.2015.08.005
- Wei, T. (2015). *New development of credit reference: new era for P2P lending*. Boston: BOC International. Retrieved from <http://www.bocintl.com/en/>
- Weiss, G. N. F., Pelger, K., & Horsch, A. (2010). *Mitigating Adverse Selection in P2P Lending – Empirical Evidence from Prosper.com*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1650774](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1650774)
- Xie, P., Zou, C., & Liu, H. (2016). The fundamentals of internet finance and its policy implications in China. *China Economic Journal*, 9(3), 240–252. doi:10.1080/17538963.2016.1210366
- Yan, J., Yu, W. & Zhao, J. L. (2015). How signaling and search costs affect information asymmetry in P2P lending: the economics of big data. *Financial Innovation*, 1(1), 1-11.
- Yan, Y., Lv, Z., & Hu, B. (2018). Building investor trust in the P2P lending platform with a focus on Chinese P2P lending platforms. *Electronic Commerce Research*, 18(2), 203–224. doi:10.1007/10660-017-9255-x
- Yum, H., Lee, B., & Chae, M. (2012). From the Wisdom of Crowds to My Own Judgment in Microfinance Through Online peer-to-peer Lending Platforms. *Electronic Commerce Research and Applications*, 11(5), 469–483. doi:10.1016/j.elerap.2012.05.003
- Zhang, H. (2016). Regulation of information disclosure and the patterns of P2P lending in China. *China Economic Quarterly*, 16(1), 371–392.
- Zhang, K., & Chen, X. (2017). Herding in a P2P lending market: Rational inference OR irrational trust? *Electronic Commerce Research and Applications*, 23(3), 45–53. doi:10.1016/j.elerap.2017.04.001
- Zhang, Y., Wu, Y., Tian, M., & Qiao, Z. (2015). *Third market analysis: The development of P2P lending in the new third market*. Beijing: Minsheng Securities. Retrieved from <http://www.mszy.com>

## Section 3

# Frauds and Financial Reporting



# Chapter 11

## Combating Fraud Through Forensic Accounting: The Case of Islamic Inheritance in Nigeria

**Umar Habibu Umar**

*Universiti Brunei Darussalam, Brunei*

**Md Harashid Haron**

*Universiti Sains Malaysia, Malaysia*

**Junaidu Muhammad Kurawa**

*Bayero University, Nigeria*

### ABSTRACT

*This study examines the potential application of forensic accounting in detecting and preventing of fraudulent activities in the administration of Islamic inheritance in Kano State, Nigeria. Data were collected through semi-structured interviews with some selected experts who are aware of Islamic inheritance and forensic accounting. Thematic analysis was used. The study established the nature and forms of the fraudulent activities committed in the administration of Islamic inheritance, such as non-compliance with the provision of Islamic inheritance law, hiding some inherited estate, the non-usage of professional valuers and the advice of experts, misappropriation of inherited cash, mismanagement of inherited wealth, etc. The key fraudsters include the eldest heirs, the parents of heirs (particularly mothers), court officials, estate valuers, relatives and the trustees of the deceased. The respondents strongly believe that forensic accounting could be used as a reliable instrument to detect and prevent such forms of fraudulent activities.*

## **INTRODUCTION**

Islamic inheritance or succession is an essential branch of Islamic Jurisprudence, which deals with the distribution of the wealth of a Muslim deceased wealth among his/her heirs. It is one of the Islamic approaches to wealth redistribution in society (Umar *et al.*, 2020). It is a common among Muslims across the globe, irrespective of religious sects (Umar & Haron, 2021). Therefore, it becomes a platform that allows every Muslim almost to occupy two positions: an heir at one time and a deceased at another time (Umar & Kurawa, 2019). The importance of learning Islamic inheritance law is very profound, as it has been described as half knowledge by some traditions of the Noble Prophet Muhammad (*May peace be upon him*). These traditions were verified to be weak by some Muslim jurists (like Albani). Nonetheless, learning the knowledge is considered as a communal obligation, which means at least a few but a sufficient number of Muslims must know at all times (Al-Jibaly, 2005).

Moreover, Islamic inheritance entails the sharing of various forms of an estate, such as houses, farms, cows, cars, jewelry, investments, etc., among heirs after settling the liabilities of a deceased. These assets are exposed to different forms of fraudulent activities that jeopardize their welfare. Forensic accounting may serve as a veritable instrument for detecting and preventing fraudulent activities in the administration of Islamic inheritance. It is mostly performed when there is suspicion of fraudulent activities and other related irregularities in respect of wealth belonging to an individuals or organization for detection and deterrence. In an attempt to link forensic accounting to Islamic inheritance, Umar (2017) has clearly stated that forensic accounting could be applied to investigate the misappropriation or embezzlement of the wealth of heirs (orphans) by trustees or any person for presentation in a *Shari'ah* (Islamic law) Court. The detection and prevention of fraudulent activities in the administration of Islamic inheritance would invariably contribute to protecting of the wealth of heirs (orphans).

Two significant reasons were found to have shown the indispensable need to undertake this study. First, fraud becomes part and parcel of a harmful threat that influences the growth and development of any country (Abdulrahman, 2019). In particular, Nigeria has been ranked among the most corrupt nations in the world by Transparency International (TI) as a result of the various forms of corrupt practices and other related offenses committed in both private and public sectors. Despite religious injunctions, Islamic inheritance administration is also exposed to the various forms of fraudulent activities. Visiting *Shari'ah* Courts in Kano state could easily enable one to notice many cases of maladministration in Islamic inheritance. In other words, regardless of the Islamic teaching to desist from any act of misappropriating the wealth of heirs and orphans, the administration of Islamic inheritance in Kano state is not free of fraud. This illegal act becomes rampant in Kano state, Nigeria. Consequently, many heirs of influential and rich persons were turned to beggars. Annoyingly, most of such cases brought before the courts of law found relatives and trustees to heirs and orphans guilty of the offense red-handed. Second, almost all the previous studies (Enofe *et al.*, 2015; Okoye & Ndah, 2019; Ogundana *et al.*, 2018; Suryanto & Ridwansyah, 2016; Fathi *et al.*, 2017; Othman *et al.*, 2015; Ogiriki & Appah, 2018; Okoye & Gbegi, 2013; Gbegi & Adebisi, 2014; Joseph *et al.*, 2016; Olaoye & Olanipekun, 2018; Eze & Okoye, 2019; Amake & Ikhatua, 2016; Ogiriki & Appah, 2018; Joseph *et al.*, 2016; Olaoye & Olanipekun, 2018; Eze & Okoye, 2019) established that forensic accounting could serve as a veritable instrument to detect and prevent fraudulent activities. Unfortunately, none of these studies established its potential application in preventing and detecting fraudulent activities in the administration of Islamic inheritance. In other words, even though forensic accounting is a topical issue, to the best of our knowledge this is the first study to have empirically investigated its potential in the detection and prevention of fraudulent activities in the

administration of Islamic inheritance. It is strongly believed that the application of forensic accounting in the administration of Islamic inheritance could detect and prevent fraudulent activities.

In view of the above background, this study aims at establishing the potential of applying forensic accounting to detect and prevent fraudulent activities in the administration of Islamic inheritance in Kano State, Nigeria. This state was selected as a case study because it is the most populated state in Nigeria dominated by Muslims (95%) (Mustafa *et al.*, 2020) with about 20 million people. The remainder of the chapter is structured as follows. Section two reviews the relevant literature, including the conceptual, empirical and theoretical framework. Section three provides the methodology used to achieve the aim of the study. Section four deals with findings and discussion of the study. Lastly, section 5 five presents a conclusion and recommendations.

## **LITERATURE REVIEW**

### **The Protection of Inherited Wealth in Islam**

Islam provides special protection to inherited wealth for the welfare of heirs, particularly orphans. The protection of Islamic inherited wealth and its utilization for sustainable orphan welfare is mentioned in the Noble *Qur'an* and the *Sunnah/hadith* (the practice, saying and silent approval) of the Prophet Muhammad (*May peace be upon him*). The wealth of heirs, particularly if they are minors, is usually under the custody of their trustees/guardians. The trustee to an orphan could be a person mentioned in the will of a deceased or a close relative to heirs. They are required to be very careful in the custody of the wealth as if it belongs to their minor children. On this issue, Allah (*Subhanahu wa Taala*) says:

*And let those (executors and guardians) have the same fear in their minds as they would have for their own if they had left weak offspring behind. So let them fear Allah and speak the right words (Quran 4:9).*

The above verse describes the pains that people (as guardians) will feel if the wealth they left for their weak children is misappropriated or neglected. Hence, they are mandated to take care of the wealth they are entrusted with as if it belongs to their minor children. Allah (*Subhanahu wa Taala*) also shows in the Noble *Qur'an* the measures taken by Prophet Musa (AS) and Khidr (AS) to protect the wealth of orphans against misappropriation:

*Moreover, as for the wall, it belonged to two orphans in the towns; and there was under it a treasure belonging to them, and their father was a righteous man, and your Lord intended that they should attain their age of full strength and take out their treasure as a mercy from your lord ... (Quran 18: 82).*

Similarly, the following is a *hadith* (tradition) of the Noble Prophet Muhammad (*May peace be upon him*) from which the need to put in place both spiritual and physical measures to prevent misappropriating the inherited wealth could be learned:

*Anas ibn Malik narrated that a man said, "Messenger of Allah! Shall I tie it and rely [upon Allah] or leave it loose and rely [upon Allah]?" He said: "Tie it and rely [upon Allah]" (Jami' al-Tirmidhi).*

According to Umar and Kurawa (2019), the above *hadith* shows that Muslims are required to act physically and pray to Allah (*Subhanahu wa Taala*). Concerning this study, all the necessary physical and necessary measures should be designed and put in place by guardians to protect the entrusted wealth against any form of fraudulent activities in the interest of orphans and then pray to Allah (*Subhanahu wa Taala*) for protection. More so, Islam prohibits the exchange of orphans' suitable property for bad ones, as it is a great sin (*Quran* 4:2). People who eat up the property of orphans are like eating up only fire into their bellies (*Quran* 4:10). However, a poor trustee is allowed to take a just and reasonable amount (according to his labor) (*Quran* 6:10). This implies that a rich trustee is entitled to no remuneration.

It is worth noting that the Islamic concern for the protection of inherited wealth is just for the sake of the heirs' sustainable welfare. This is accordance with the tradition whereby the Prophet Muhammad (*May peace be upon him*) decreed that not more than one-third of one's estate should be bequeathed to prevent one's heirs from living in poverty after his/her death (Sahih Bukhari). In other words, this tradition disapproves giving out a bequest that exceeds one-third of the property to distribute among heirs in order to maximize their allocations as much as possible and enable them to comfortably afford their livings comfortably.

Moreover, it is recommended that inherited wealth be kept idle but invested in a profitable and *Shari'ah*-compliant business, either *musharakah*, *mudarabah* or both (Umar & Haron, 2021). They believe that the share given to each heir if not invested (or part of it) will be finished one day and become beggars. Similarly, Umar and Kurawa (2019) viewed that when a Muslim deceased left a business, it should not be liquidated but his heirs admitted into it as partners (shareholders in the case of a company). This would enable them to be earning income from the business as long as it remains a going concern. Similarly, Umar (2019) suggested for the integration of a family *waqf* into an inheritable going concern business in such a way as to ensure that the founder/owner of the business bequeathed a certain percentage of equity of the business for his exempted heirs. In this case, provided that the business continues to exist and earn a profit, both heirs and those exempted would get a share of profit from it (Umar *et al.*, 2020; Hassan & Noor, 2020). Besides, a weak narration called upon the guardians of orphan wealth to invest it in a business in order to avoid it being exhausted by *zakat*. Despite the weakness of this narration, some companions of the Prophet Muhammad (*May peace be upon him*), such as Aisha, Umar ibn Khattab and Abdullahi ibn Umar (*May Allah be please with them*), believed that *zakat* is chargeable on orphans' wealth (Jami' al-Tirmidhi).

Islam also provides the condition and time to handover wealth to orphans by trustees. They are required to surrender it to them in the presence of witnesses when the orphans reach the age of marriage and are capable of making sound judgments (*Quran* 4:6).

In summary, it has been clearly pointed out the Islamic need for the protection of the wealth of heirs (orphans) entrusted to guardians. It has also been pointed out that the wealth should not remain idle but maximized through the investment in a *Shari'ah*-compliant business.

## Linking Forensic Accounting to Islamic Inheritance

Forensic simply means "suitable for use in a court of law" (Okoye & Gbegi, 2013). Forensic accounting involves the use of accounting principles, theories and disciplines in order to resolve a legal dispute (Gray, 2008). It is a specialized branch of accounting that virtually combines not only other branches of accounting (financial accounting, auditing, cost and management accounting, taxation and finance)

but also other related disciplines, particularly law (Umar, 2017). More comprehensively, Ramaswamy (2007, pp. 33) defined it as:

*Accounting analysis that uncovers possible fraud that is suitable for presentation in court. Such analysis will form the basis for discussion, debate and dispute resolution.” A forensic accountant uses his knowledge of accounting, law, investigative auditing and criminology to uncover fraud, find evidence and present such evidence in court if required to do so.*

Briefly, forensic accounting entails the use of accounting, auditing and investigative skills to provide a report suitable for presentation in a court.

Further, according to ACFE (2020), various types of services could be performed by forensic accountants, such as financial data analysis, computer application design, testifying as an expert witness, tracing illicit funds, damage assessment, locating hidden assets, business valuation and damage assessment, bankruptcy fraud investigation, embezzlement investigation, etc. (Zolkafli, Nazri, Omar, 2021). Correspondingly, according to IFA (2020), forensic accountants could be engaged to render services, such as litigation support, economic damages computations, business/employee fraud investigations, the discovery of hidden assets, matrimonial disputes, business interruptions/business failures, professional negligence, etc. Hence, considering the nature of the inherited estate, the following (but not exhaustive) forensic accounting services could be applied in the administration of Islamic inheritance:

- Discovery of a hidden estate left by a deceased
- Authentication of the bequests of a deceased
- Investigation of fraud in the valuation of an estate
- Valuation and distribution of the equity of an inherited business
- Presentation of expert witness relating to Islamic inheritance in courts
- Investigation of a murder case
- Investigation of the legitimacy of heirs
- Investigation of unknown heirship claimants
- Investigation of embezzlement
- Fraud detection and prevention in the custodianship of the estate of orphans

The above examples show the applicability of forensic accounting in detecting and preventing all the forms of fraudulent activities in the administration of Islamic inheritance.

It is worth noting that forensic accounting is a multi-skills practice, as the knowledge and skills of the various disciplines need to be integrated to discharge it effectively and efficiently. In specific, forensic accountants have to possess adequate knowledge and skills of accounting, auditing, finance, law, criminology, report writing, psychology, etc., in order to discharge their duties efficiently and effectively. More importantly, in Islamic inheritance forensic accountants are required to have sufficient knowledge of Islamic Jurisprudence.

Moreover, forensic accounting professional practice, like other professions, has institutions/associations that produce qualified personnel to render services efficiently and effectively. Notable organizations that promote and support forensic accounting activities include the Association of Certified Fraud Examiners, American College of Forensic Examiners, Association of Certified Fraud Specialists; National Litigation Support Services Association; National Association of Certified Valuation Analysts, American Institute

of Certified Public Accountants; and the Institute of Business Appraisers (Gray, 2008). In Nigeria, the Institute of Forensic Accountants of Nigeria (IFA), otherwise known as the Chartered Institute of Forensic Accountants of Nigeria (CIFAN), also exists. However, no single institution is primarily established to render forensic accounting services for the detection and prevention of fraudulent activities in the administration of Islamic inheritance. Hence, there is a need to have such an institution to train, regulate and encourage the application of forensic accounting in the administration of Islamic inheritance as inheritance distribution becomes almost a daily practice in all Islamic societies.

### **Review of Empirical Studies**

Forensic accounting has been for long a topical issue across the globe. Therefore, a lot of studies were conducted to establish whether it could serve as an instrument to combat fraud and other related offenses in organizations, private and public. In the private sector, Enofe *et al.* (2015) evaluated the relevance of forensic audits in detecting fraud in Nigerian corporate organizations by generating data through administration questionnaires. The study found that fraud in business entities could be detected and prevented significantly through the use of forensic audits frequently. Okoye and Ndah (2019) conducted a study to find whether the practice of forensic accounting could prevent fraud in the manufacturing sector in Nigeria. Data were collected by using questionnaires distributed to the staff of the sector concerned. The study found that forensic accounting could significantly prevent the occurrence of fraud in the manufacturing sector. Ogundana *et al.* (2018) embarked on a study to find the role of forensic accountants in the prevention and detection of fraud in the Nigerian banking industry. Primary data were generated through the administration of questionnaires to the staff of some selected banks. One of the key findings was that forensic accounting has a significant effect on the prevention and detection of fraud in the industry.

Moreover, relevant studies exist in the Islamic banking industry. For example, some researchers examined the impact of *Shari'ah* financial accounting standards (Suryanto and Ridwansyah, 2016; Alam, 2021), the independence of the *Shari'ah* Supervisory Board (Rafay & Farid, 2018) and Auditor Competency *Shari'ah* (Ahmad & Abdul-Rahman, 2020) on the prevention of fraud. In Indonesian Islamic banks, questionnaires were administered to a saturated sample of 48 respondents comprising Islamic bank auditors and the Islamic supervisory Board (Suryanto and Ridwansyah, 2016). It was found that the *Shari'ah* financial accounting standards, the independence of the *Shari'ah* Supervisory Board and Auditor Competency *Shari'ah* were collectively found to have significantly influenced the prevention of fraud in the Islamic banks. But individually, Islamic financial accounting standards have a significant impact on the prevention of fraud in Islamic banks. But the independence of the *Shari'ah* Supervisory Board was found to have an insignificant impact on fraud prevention. In addition, the competency of the Islamic auditor was found to have a partial significant impact on fraud prevention in the banks. Fathi *et al.* (2017) investigated the relationship between employee attributes (gender, age, position and religiosity) and the asset misappropriation of Islamic bank assets in Malaysia. The study adopted the fraud triangle model and administered questionnaires to 109 employees of Islamic banks in Malaysia. It found gender, age, position and religiosity to have significantly influenced employees to misappropriate the assets of the Islamic banks. Hence, the study called on the management to provide ways of preventing fraud in the banks.

However, most of the relevant studies in developing countries used the public sector as their case study. Like in Malaysia, Othman *et al.* (2015) administered questionnaires to some selected accountants and internal auditors in the public service with a view to finding ways of detecting and preventing fraud

and corruption in the public sector of the country. The study established operational audit, enhanced audit committees, rotation of staff, improvement in internal controls, implementing fraud reporting policy, the provision of fraud hotlines and the application of forensic accounting as instruments for the effective detection and prevention of fraudulent activities in the Malaysian public service. Similarly, in Nigeria, Okoye and Gbegi (2013) sought to establish whether forensic accounting could serve as an instrument for fraud detection and prevention in some selected public organizations in Kogi State. The major data were generated through the administration of questionnaires to a sample of 370 staff drawn from five ministries in the state out of which 350 were returned. In addition, some of the respondents were interviewed. One of the key findings of the study showed that forensic accounts could play a vital role in the detection and prevention of fraud in public sector organizations.

Gbegi and Adebisi (2014) examined the role of forensic accounting skills and techniques in fraud investigation in Nigeria. Questionnaires were given to a sample of 129 staff of anti-corruption agencies in the country. It was established that forensic accounting skills and techniques contribute significantly to discovering and reducing fraud in the Nigerian public sector. Amake and Ikhatua (2016) sought to establish whether forensic accounting could detect fraud in the Public Sector of Nigeria. A sample of 100 respondents was selected from the auditors and accountants of four ministries in Edo State, Nigeria. It was found that fraud could be detected and prevented effectively in the Nigerian public sector through the application of forensic accounting. A significant association was also found between forensic accounting and litigation support services in Nigerian courts.

Moreover, Ogiriki and Appah (2018) used questionnaires to establish the impact of forensic accounting and auditing techniques on fraudulent activities in the Nigerian public sector. The study found these techniques to have significant effects on fraud detection, investigation and prevention in the Nigerian public sector. Joseph *et al.* (2016) investigated the contribution of forensic accounting in the detection and prevention of fraud in Nigeria. Primary data were generated through the administration to a sample of 92 professional accountants in the Nigerian public sector. The results revealed that forensic accounting has a significant role in the detection and prevention of fraud. Also, Olaoye and Olanipekun (2018) assessed the relationship between forensic accounting and corporate governance in Ekiti State, Nigeria. The data were generated through the administration of questionnaires to 100 forensic accountants and practitioners in the state. The study found that forensic accounting could significantly enhance corporate governance practice in the state through the improvement of management accountability, internal control system and financial reporting system. More recently, Eze and Okoye (2019) conducted a study to assess the relationship between forensic accounting and fraud detection and prevention in the public sector in Imo state, Nigeria. Through the administration of questionnaires, it was found that forensic accounting can significantly detect and prevent fraud in the state public sector. Abdulrahman (2019) also applied content analysis to assess the role of forensic accounting in the prevention of fraud in the Nigerian public sector. The study established a significant positive relationship between forensic accounting techniques and fraud prevention in the sector.

Briefly, the empirical studies so far reviewed showed that forensic accounting is a strong and veritable instrument to reduce all the forms of fraudulent activities in both private and public sectors. Specifically, the effective application of forensic accounting in Nigeria, particularly in the government sector, will definitely reduce fraudulent activities to the barest minimum.

## **Theoretical Framework**

Based on the objective of this study, the most elegant theory relevant to this study is the fraud triangle theory. This theory has been widely accepted and used by industry and academics across the globe to explain why fraudulent activities are committed (Akkeren, 2018). The Association of Certified Fraud Examiners (ACFE) and the American Institute of Certified Practicing Accountants (AICPA) are among its strong proponents (Akkeren, 2018). Another relevant theory is the diamond fraud theory, an extension to the fraud triangle theory also found to be relevant. The idea of what makes people commit fraud was put forward by Cressey in 1953 (Christian *et al.*, 2019). Cressey was a criminologist who began the study to establish the reasons for committing fraud by people through interviews with 250 criminals within 5 months (Abdullahi & Mansor, 2015). Therefore, the fraud triangle theory emerged from the literature of sociology and was subsequently adopted to explain the reasons for committing fraudulent activities (Akkeren, 2018). It is called “triangle” because three factors were identified to cause fraud, which is exactly the same as the number of the sides of a triangle. According to ACFE (n.d.), the fraud triangle is the best and most widely accepted theory explaining the reasons for committing fraud by people. Cressey identified three elements that make people engage in fraudulent activities as follows:

1. **Pressure:** This is what stimulates a person to commit fraud. It is the factor that leads to unethical behavior that serves as an incentive to commit fraud. Pressure can be financial or non-financial, but financial pressure is believed to be the major reason that makes one commit fraud (Abdullahi & Mansor, 2015). Similarly, it motivates someone to commit fraud as a result of financial problems that could not be solved through legitimate ways and then becomes a motivator to such a person to use illegal ways (ACFE, n.d.). Examples of pressures that make people to commit fraud include an unduly lavish lifestyle, an increase in family size, losses suffered as a result of a natural and artificial disaster, excessive dependent relatives, etc. Specifically, in Islamic inheritance, the poor relatives of a wealthy deceased person may motivate them to hide some assets before distribution, particularly when they are exempted from inheritance. In addition, many guardians/trustees were found guilty of substantial misappropriating heirs (orphans) assets due to poverty and selfishness.
2. **Opportunity:** This is a chance that one has to commit fraud. The existence of a pressure to commit fraud alone will not lead someone to commit it unless there is a way to do so without being found, such as poor internal control, poor training, poor supervision, lack of prosecuting fraudsters, ineffective anti-fraud programs, etc., (ACFE, n.d.). Similarly, according to Abdullahi and Mansor (2015), an opportunity may occur as a result of the existence of ineffective control or governance, which is popularly known as internal control weaknesses in the accounting environment. Islamic inheritance is more vulnerable to fraud than public and private organizations. This is because mostly guardians are not required to account for the estate of heirs under their custody periodically, say, at least once in a year. In addition, weak or no internal control exists to prevent such fraudulent activities from happening.
3. **Realization:** This is the formulation of morally acceptable ideas by fraudsters before committing fraud upon which they defend themselves when they are caught (Abdullahi & Mansor, 2015). ACFE (n.d.) states some of the terms used by fraudsters to rationalize their fraudulent activities as follows, “everyone else does it”, “it was not a bribe but part of conducting business”, “bribery is a part of the culture in the country”, etc. In the case of Islamic inheritance, during distribution, the relatives of the deceased may take something from the inherited estate unreasonably by depending



themselves that Allah (*Subhanahu wa Taala*) said, when the relatives and the poor are present at the time of division, gives them out of the property (Quran 8:10). In another way, trustees may be spending orphans' wealth unjustly because they are allowed to take something from it if they are poor (Quran 6:10).

Although the fraud triangle contributes significantly to the explanations of the factors that contribute to the commitment of fraudulent activities, it has been criticized for some limitations. ACFE (n.d.) pointed out three limitations of this theory. First, though it guides in explaining the nature of occupational fraud, it fails to explain the nature of occupational offenders. Second, the theory is nearly half a century old and there has been a considerable social change in the interim. This renders it outdated to some extent as new forms of fraudulent activities continuously emerge, like cybercrime and other white-collar crimes. Third, some experts called for the extension of the theory by introducing the fourth factor. Hence, the diamond theory emerged to address some of the limitations of the fraud triangle theory. Wolfe and Hermanson (2004) developed this theory by publishing a paper in the CPA journal. This theory is not completely new but an extension of the fraud triangle theory. The founders believed that even if pressure, opportunity and realization exist, the fraudster must have the capability to commit fraud. In other words, corporate fraud becomes impossible unless there are people who can commit fraud. Fraud perpetrators must have the necessary skills and abilities to engage in fraudulent activities (Abdullahi & Mansor, 2015). Christian *et al.* (2019) also believed that a lot of corporate frauds that are generally large in number would not have occurred without the helpful hand of a particular person with a specific capability in the company. In Nigeria, trustees/guardians and other relatives are capable of misappropriating inherited estate right before distribution to the time they are formally entrusted with such wealth. In fact, some trustees may unjustly spend the whole estate entrusted to them before the heirs become mature. It is worth noting that the major contribution of Wolfe and Hermanson to the theory of fraud theory is the introduction of "capability", which transformed Cressey's triangle-shaped (three factors) theory to a diamond-shaped (four factors) theory.

In summary, based on the above discussion, it is understandable that pressure, opportunity, realization and capability are the factors leading to committing the various forms of fraudulent activities in the administration of Islamic inheritance.

## **METHODOLOGY**

This study used semi-structured interviews to achieve its objective, as it is a pioneer and exploratory in nature. This was applied by previous qualitative studies (Nor & Hashim, 2015; Thaker, 2018, Umar *et al.*, 2019, Umar, 2020). This method allows the respondents a degree of freedom to explain their thoughts and bring to light the areas of their particular interest as well as permit certain responses to be asked in greater depth and, in particular, bring out and resolve apparent contradictions (Horton *et al.*, 2004). Similarly, according to Nor and Hashim (2015), interviews enable respondents to express their opinions on a particular subject as well as allow some areas to be explored in detail. The participants were experts, comprising qualified professional accountants and lawyers with working experience.

In selecting the respondents, a purposive sampling technique was applied. It is the sampling technique that is commonly used in qualitative research (Gentles *et al.*, 2015). According to Umar (2020), it allows the researcher to ensure that experienced and qualified participants (respondents) are chosen who

## Combating Fraud Through Forensic Accounting

are free to answer research questions competently. The next issue is the sample size of the study, which is very essential in the provision of adequate and reliable findings in line with study objectives (Umar *et al.*, 2019). Unfortunately, the appropriate sample size of qualitative research remains inconclusive. However, the data saturation technique was used to select the sample size. The concept of data saturation originated from grounded theory studies, which means continuously bringing additional participants into a study until the data set is complete by getting data replication or redundancy (Marshall *et al.*, 2013). Thus, a sample of five respondents was used, as it has been realized that any additional sample would lead to data redundancy.

Table 1. Profile of the participants

No.	Position	Code
1.	Professional Accountant	A1
2.	Legal Practitioner	A2
3.	Professional Accountant	A3
4.	Legal Practitioner	A4
5.	Professional Accountant	A5

Table 1 presents the profile of five respondents comprising three Muslim professional accountants and two Muslim legal practitioners, who have at least basic knowledge of Islamic inheritance. They were asked to narrate what they notice happening on the subject matter of the study in Kano, State Nigeria, as they not only reside in the state but are also indigenes of the state.

Moreover, in line with previous studies (Thaker, 2018; Umar *et al.*, 2019; Umar, 2020), the data collected during the interviews were transcribed into field notes and analyzed by using thematic analysis. According to Nowell *et al.* (2017), thematic analysis is a qualitative research method that has been commonly applied across a range of epistemologies and research questions. It involves identifying, analyzing and reporting patterns (themes) within data and minimally organizes and describes data sets in detail (Braun & Clarke, 2006). The following six phases for conducting a trustworthy thematic analysis were followed:

- Familiarizing yourself with your data
- Generating initial codes
- Searching for themes
- Reviewing themes
- Defining and naming themes
- Producing the report (Nowell *et al.*, 2017, p.4).

## FINDINGS AND DISCUSSION

The findings and discussion are based on the seven categorical themes presented in Table 2.

Table 2. Categorical themes and interview questions

No.	Categorical Themes	Interview Questions
1.	Fraudulent activities in the administration of Islamic inheritance and the fraudsters	Do you notice fraudulent activities in the administration of Islamic inheritance? If yes, who are the fraudsters?
2.	The nature and forms of fraudulent activities in the administration of Islamic inheritance	Could you describe the nature and forms of fraudulent activities in the administration of Islamic inheritance?
3.	The causes of fraudulent activities in the administration of Islamic inheritance	What factors do you think are the causes of fraudulent activities in the administration of Islamic inheritance?
4.	The relevance of forensic accounting in combating fraudulent activities in the administration of Islamic inheritance	Do you agree that forensic accounting is relevant in combating fraudulent activities in the administration of Islamic inheritance?
5.	The usefulness of forensic accounting reports to Nigerian <i>Shari'ah</i> Courts in deciding fraudulent activities cases in the administration of Islamic inheritance	Do you believe that Nigerian <i>Shari'ah</i> Courts would find forensic accounting reports very useful in deciding fraudulent activities in the administration of Islamic inheritance?
6.	Measures for detecting and preventing fraudulent activities in the administration of Islamic inheritance	What measures should be taken to detect fraudulent activities in the administration of Islamic inheritance?
7.	Knowledge and disciplines to integrate for discharging forensic accounting in the administration of Islamic inheritance	What knowledge and disciplines do you think should be integrated to discharge forensic accounting services in the administration of Islamic inheritance efficiently and effectively?

## Fraudulent Activities in the Administration of Islamic Inheritance and the Fraudsters

The respondents were asked whether they noticed the occurrence of fraudulent activities in the administration of Islamic inheritance. They all agreed that the administration of Islamic inheritance was exposed to fraudulent activities and other irregularities. In particular, an excerpt from A4 response is as follows:

*Fraudulent activities and other irregularities exist not in the system of Islamic inheritance (being a divine law) but in its administrations...*

In addition, based on their responses the following were identified as the key fraudsters, such as heirs (particularly the eldest), parents to heirs (particularly mothers), court officials (judges, registrars, clerks and bailiffs), trustees/guardians, relative to heirs, business partners to the deceased, valuers and other experts, among others. Briefly, this clearly shows the extent to which the administration of Islamic inheritance in the state is exposed to fraudulent activities by all the persons that have direct or indirect access to inherited wealth.

## The Nature and Forms of Fraudulent Activities in the Administration of Islamic Inheritance

The respondents were also asked to describe the nature and forms of fraudulent activities committed in the administration of Islamic inheritance. All five of them provide details of the various forms of fraudulent activities. Based on their responses, these fraudulent activities could be grouped into six (though some are intersected).

## **Combating Fraud Through Forensic Accounting**

First, one of the notable forms of fraudulent activities is non-strict compliance with the principles of Islamic inheritance law. A4 describes it as follows:

*A key fraudulent activity is non-observance of the basic principles or pre-requisites of Islamic inheritance, such as death, the existence of heirs, settlement of liabilities and wills of the deceased. In addition, in many cases, the debts and the will of a deceased were deliberately refused to be settled by heirs.... Information or facts were also misrepresented or falsified to include illegitimate heirs or exclude rightful heirs through the fabrication of certain documents... (A4)*

Second, hiding some inherited estate. Some important excerpts from two respondents are as follows:

*Before sharing the estate, some business associates, relatives to the deceased, etc., hidden/carted away some valuable estate left by the deceased... (A1)*

*Some heirs (particularly the eldest and mature ones) and relatives/trustees to heirs do not disclose some estate left by the deceased. Business partners may also refuse to surrender the actual capital contribution belonging to the deceased. (A4)*

Third, revaluation of the inherited estate, particularly landed property, is exposed to various fraudulent activities. Some of their responses to this issue are as follows:

*The use of non-expert advice in the revaluation of properties... (A2)*

*Professional/expert services are not engaged, particularly in the revaluation of properties, such as houses, motor vans, plots, etc., which may lead to their under /overvaluations. (A3)*

*An heir who has a target to possess a particular estate like a house may give bribes to valuers and court officials to revalue it at say N 20 million instead of N 35 million. (A4)*

*An heir who has a target to possess a certain property may connive with court officials and valuers to undervalue the assets. On the other hand, because of rivalry among heirs some wealthy ones may require the valuers to overvalue a particular property (particularly land property located in a strategic place) to make it difficult for some deserving but poor heirs to possess. Such a wealthy heir is ready to take it at whatever price solely because of enmity. This enmity mostly occurs between heirs who have the same father but different mothers ... (A5)*

Fourth, inherited cash is the most exposed estate to fraudulent activities. A4 said that mostly when a person dies his bank balances are usually transferred to the court's account before distribution. The following are the key excerpts on this issue:

*Some court workers/representatives and even judges give order to the bankers of the deceased to transfer his/her money to the court account they have access to. They can withdraw the money to engage in business for their benefits without the consent of heirs. Alternatively, they may save the money into fixed*

*deposits in order to earn interest. Hence, they deliberately delay the distribution for some months like six within which they expect to earn income or profits ... (A3)*

*In many instances, court officials that have a direct or an indirect access to the account into which inherited cash is deposited withdraw money from such an account for their personal use or business without the knowledge of heirs. Some court officials withdraw the money to deposit it into a fixed deposit account to earn interest .... They may later return the money into the court account before the distribution. This makes them delay the distribution .... Moreover, sometimes the cash allocations of minor heirs are left in the court's account. This gives them another opportunity to misappropriate it. These illegal practices when discovered led to the termination of the appointments of many judges in Kano state by the government. (A4)*

*When someone dies, heirs are required to apply for the letter of administration from the court of law. After completing the form, they are required to publish it in a reputable newspaper before distribution. Some heirs use this opportunity (with or without court officials) to apply for the letter of administration and publish it in the newspapers without informing their co-heirs. They then apply to the bank of the deceased to release the money for distribution among theirs by transferring it into their personal accounts or court accounts. This allows them to withdraw the amount they like ... (A5)*

Fifth, the misappropriation of the wealth of minor or insane heirs (orphans). Two respondents said the following:

*Nowadays, many trustees (who are mostly related to the deceased) of minor heirs were found guilty of unjustly eating the estate they were entrusted with ... (A1)*

*A lot of trustees/guardians to whom the inherited estate of minor or insane heirs is entrusted do not fear Allah, as they squander the wealth within a few years and jeopardize the welfare of the heirs ... More sadly, some mothers who insisted to act as custodians of the wealth inherited by their minor children were established to have completely or significantly spent it before they grow up. This tradition and culture expose the children of many wealthy deceased persons into extreme poverty ... (A5)*

Sixth, the collection of illegal court fees by court officials. On this issue, three respondents said the following:

*The court officials used a certain clause that is not provided in any provision of the law to collect a certain percentage of the distributable estate, say, 5%, which is not paid into any government account but given to them. Sometimes, the heirs have no option rather than to negotiate with them to a certain amount or reduce the percentage to, say, 2%. This amount is huge if the deceased is at least a millionaire. (A3)*

*The collection of illegal fees by court officials from litigants (heirs) in the name of filing fees but actually for their personal interests; this occurs before distribution, during the distribution and after distribution. Some court officials charge it as a percentage of the distributable estate. The reality is that according to the Kano State Shari'ah Court Civil Procedure, the maximum filing fees for a case of inheritance are N 100. (A4)*

## **Combating Fraud Through Forensic Accounting**

*Court officials, particularly registrars, collect a certain percentage of the distributable estate ... Sometimes they deliberately delay the distribution until the amount is fully paid. (A5)*

Briefly, the above are six examples of various forms and nature of fraudulent activities in the administration of Islamic inheritance.

## **The Causes of Fraudulent Activities in the Administration of Islamic Inheritance**

The views of the respondents were sought on the causes of fraudulent activities in the administration of Islamic inheritance. They responded as follows:

*Lack of Islamic knowledge and fear of Allah (Subhanahu wa Taala) in managing the wealth of heirs (orphans) as ordained by Allah, lack of standard government regulations in relation to inheritance management, lack of keeping proper and complete records of one's estate and other business dealings ... (A1)*

*... lack of fear of Allah (Subhanahu wa Taala), ignorance of the principle of Islamic inheritance, incompetency of administrators and trustees, lack of integrity, selfishness and lack of control/restriction to the inherited property. (A2)*

*The causes of fraudulent activities in Islamic inheritance include lack of fear of Allah (Subhanahu wa Taala), lack of integrity, lack of using professional valuers and other experts' advice, etc. (A3)*

*Lack of fear of Allah (Subhanahu wa Taala), poverty, greediness, tradition and culture of the people in the society ... (A5)*

Moreover, A4 provides more comprehensive causes of fraudulent activities as follows:

- Lack of fear of Allah (*Subhanahu wa Taala*)
- Non-observance of the existing laws governing the distribution of Islamic inheritance
- Lack of enforcement of laws from the part of the regulatory agencies
- Lack of knowledge of laws and rules of courts of law from the litigants (heirs). If they know nobody would defraud them.
- Dishonesty of litigants (heirs), court officials and experts
- Hostility/enmity between heirs, more especially between the ones that have no the same mothers. In this case, some heirs may attempt to get undue advantages at the expense of their co-heirs; and
- Lack of preparation and keeping proper and complete records.

To sum up, the respondents pointed out the key causes of maladministration in Islamic inheritance. Lack of fear of Allah (*Subhanahu wa Taala*) and knowledge of Islamic inheritance law are almost the drivers of the other causes of fraudulent activities, such as lack of integrity, dishonesty, selfishness, non-usage of professional valuers and expert advice, enmity among heirs, etc. People that really fear Allah (*Subhanahu wa Taala*) would never involve themselves in any form of fraud in the administration of Islamic inheritance as it is totally condemned by Allah (*Subhanahu wa Taala*) and the Prophet Muhammad (*May peace be upon him*). More so, two key issues related to accounting are the lack of keeping

proper and complete records by a deceased and lack of restriction to access inherited wealth give room for maladministration. Recently, it happened in Kano state that a deceased who purchased about 170 commercial vehicles and secretly handed them over to drivers for commercial transportation. Unfortunately, he failed to keep proper and complete records (including valid documents) of ownership to such motors, letters of agreement with the drivers and their personal details (including their addresses). He also informed none of his family members. When he died, not up to 30 drivers feared Allah (*Subhanahu wa Taala*) and returned the motors to his heirs. Though later the heirs were able to know the drivers, unfortunately, they had no valid documents to present before the court to claim most of them. Related to this issue, A4 said that mostly even for those that claim to have complete records and evidence of their business transactions, they maintain the one-party document, as they cannot present any document of the agreement signed by the other party with whom they entered into the contract or any other commercial transaction. In addition, lack of restriction to access the inherited estate of an heir (orphan) after distribution, particularly by the relatives, contributes significantly to maladministration.

### **The Relevance of Forensic Accounting in the Combating Fraudulent Activities**

In consideration of the various forms of fraudulent activities that occur in the administration of Islamic inheritance, the views of the respondents were sought on whether forensic accounting could serve as a tool for combating fraudulent activities in the administration of Islamic inheritance. All the respondents believed that it could be used as a strong instrument to fight fraudulent activities in Islamic inheritance. The mentioned the following responses:

*I believe that the application of forensic accounting would stop the various forms of fraud in the administration of Islamic inheritance. (A1)*

*Of course, the forensic accounting could be used to checkmate all the fraudulent activities in the Islamic inheritance administration. (A2)*

*It would reduce the fraudulent activities in the administration of Islamic inheritance to the barest minimal. (A3)*

*In my opinion, forensic accounting is the best tool to use to curtail fraudulent activities in the administration of Islamic inheritance in Kano state ... (A4)*

*Yes, the application of forensic accounting would surely reduce the fraudulent activities in the administration of Islamic inheritance to the tolerable level. (A5)*

Briefly, the above responses established that forensic accounting could be applied to control all the forms of fraudulent activities in the administration of Islamic inheritance. This is in line with the findings of the earlier studies that established forensic accounting as a veritable instrument to combat fraud and other irregularities in both private and public sectors (Othman *et al.*, 2015; Joseph *et al.*, 2016; Ogiriki & Appah, 2018; Ogundana *et al.*, 2018; Olaoye & Olanipekun, 2018; Okoye & Ndah, 2019; Ogiriki & Appah, 2018; Eze & Okoye, 2019).

## **The Usefulness of Forensic Accounting to Nigerian Shari'ah Courts**

The respondents were asked about the usefulness of forensic accounting to *Shari'ah* Courts in deciding the cases of maladministration in Islamic inheritance. All five of them simply answered “yes”. This implies that Nigerian *Shari'ah* Courts would find forensic accounting very useful in deciding the cases involving fraudulent activities in the administration of Islamic inheritance. The fact is that the term “forensic” is simply described as “suitable for use in a court of law” (Okoye & Gbegi, 2013). It is applied for the resolution of a legal dispute in a court of law (Gray, 2008). In specific, forensic accounting reports could be applied to resolve all forms of fraud, irregularities and other disputes in the administration of Islamic inheritance brought before *Shari'ah* Courts.

## **Measures for the Detection and Prevention of the Fraudulent Activities**

The respondents were asked to provide the measures to take to detect and prevent fraudulent activities in the administration of Islamic inheritance. They provided the measures which they think are worth applicable in the detection and prevention of such illegal activities. The following are their responses:

*Effective punishment of fraudsters, educating the wider society on the Islamic inheritance law and its administration [...]. The use of expert and professional advice, etc. (A1)*

*Using competent valuers and expert advice for technical decisions, limited access to the inherited estate (before and after the distribution), ratification of informal inheritance distribution in the court, accountability and transparency in the distribution and custodianship of the inherited estate, preparation of proceedings of the distribution of the inherited estate, sanctions fraudsters, etc., ... (A2)*

*... supervision of the administration of Islamic inheritance by experts, limitation of access to the properties unless by authorized persons only, the use of professional valuers and expert advice in the administration, provision of the stewardship for the custodianship of the inherited estate, designing internal control measures to prevent misappropriation of the inherited assets and effective punishment of fraudsters. (A3)*

*Integrating forensic accounting into the administration of Islamic inheritance, periodic inspection of courts proceedings and court records, the appointment of trustworthy and competent persons as judicial officers, strict observance of disciplinary measures against any court official found guilty of committing fraud and prosecution of other fraudsters (e.g. experts/valuers, heirs, trustees, etc.), banning all cash payments and replace them with electronic ones in the courts, organizing public enlightenment programs to educate the general public on Shari'ah laws and rules (especially with regards to appropriate and current filing fees), development of the uniform database for the registration of ownership by all persons (particularly the land property), the use of certified experts when it comes to the matters of professional advice, etc., ... (A4)*

*The establishment of a supervisory agency to oversee the activities of the courts in the administration of Islamic inheritance, the use of professional valuers/experts (particularly in the case of landed property), keeping proper and complete records of the distributions (including the locations of valuable estates*



*as well as the names and addresses of the experts and other consultants), restrictions to access to the wealth of heirs, etc., ... (A5)*

## **Knowledge and Disciplines to Integrate for Discharging Forensic Accounting**

The respondents were asked to provide the relevant knowledge and disciplines needed to integrate to discharge the forensic accounting services in the administration of Islamic inheritance effectively and efficiently. The individual responses are as follows:

*Accounting, Islamic/Civil law, Engineering and it's allied, etc., ... (A1)*

*Islamic jurisprudence, accounting, Law, Estate valuation, Criminology, etc. (A2)*

*Accounting, estate valuers, law, criminology, etc. (A3)*

*Accounting, law, Shari'ah, criminology, estate valuation skills ... In my opinion, there is no discipline that has no application in forensic accounting either directly or indirectly. However, some disciplines are more relevant than others. (A4)*

*Accounting, law, Shari'ah, etc. (A5)*

Based on the above responses, the key and common knowledge and disciplines that need to be integrated include accounting, Islamic jurisprudence, and law and estate valuation. The application of forensic accounting in the administration of Islamic inheritance makes it a very complex issue because knowledge and various disciplines need to be applied, as believed by A4. For example, medical skills could be applied to resolve the complications in the inheritance involving the fetus, the hermaphrodite, the simultaneous death of persons, etc. In addition, criminology could be applied in the administration of Islamic inheritance where a particular heir is suspected to have been involved in the murder of the deceased. This is because a murderer does not inherit from the victim in Islam.

## **CONCLUSION**

Islamic inheritance entails allocating and transferring the estate left by a Muslim deceased to the successors after liabilities and bequests are settled. Such estate may comprise landed property, cash, motors, clothes, books, foodstuffs, etc. These are exposed to various forms of fraudulent activities that consequently undermine the welfare of heirs. Hence, this study investigated forensic accounting's potential application to detect and prevent fraudulent activities in the administration of Islamic inheritance in Kano state, Nigeria. Primary data were generated through semi-structured interviews with selected experts. The study found the parents of heirs (particularly mothers), the eldest heirs, court officials, estate valuers, business partners, relatives and trustees to the deceased, etc., committing fraudulent activities in one form or the other. The respondents were of the view that the application of forensic accounting in the administration of Islamic inheritance would detect and prevent such illegal practices. Forensic accounting has also been established as a beneficial instrument to *Shari'ah* Courts in making resolutions

for cases involving defrauding heirs and disputes. The study also provided different measures to prevent and detect fraudulent activities in the administration of Islamic inheritance to the barest minimum.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## **REFERENCES**

- Abdullahi, R., & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory. understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 5(4), 38–45.
- Abdulrahman, S. (2019). Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper. *International Journal of Accounting & Finance Review*, 4(2), 13–21. doi:10.46281/ijaf.v4i2.389
- Ahmad, N. F. G., & Abdul-Rahman, A. (2020). Shari'ah Governance and Audit Assurance in Islamic Banks. In A. Rafay (Ed.), *Growth and Emerging Prospects of International Islamic Banking* (pp. 278–297). IGI Global. doi:10.4018/978-1-7998-1611-9.ch015
- Akkeren, J. V. (2018). Fraud triangle: Cressey's fraud triangle and alternative fraud theories. In D. C. Poff & A. C. Michalos (Eds.), *Encyclopedia of business and professional ethics* (pp. 1–3). Springer. doi:10.1007/978-3-319-23514-1\_216-1
- Al-Jibaly, M. (2005). *Inheritance Regulations & Exhortations* (2nd ed.). Al-Madinah al-Munawwarah: Al-Kitab & Sunnah Publishing.

Alam, M. D., Tabash, M. I., Hassan, M. F., Hossain, N., & Javed, A. (2021). *Shariah Governance Systems of Islamic Banks in Bangladesh: A Comparison with Global Governance Practices*. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Amake, C. C., & Ikhatua, O. J. (2016). Forensic accounting and fraud detection in Nigerian public sector. *Igbinedion University Journal of Accounting*, 2, 148–173.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. doi:10.1191/1478088706qp063oa

Christian, N., Basri, Y. Z., & Arafah, W. (2019). Analysis of fraud triangle, fraud diamond and fraud pentagon theory to detecting corporate fraud in Indonesia. *International Journal of Business Management and Technology*, 3(4), 73–78.

Enofe, A. O., Omagbon, P., & Ehigiator, F. I. (2015). Forensic Audit and Corporate Fraud. *IIARD International Journal of Economics and Business Management*, 1(8), 55–64.

Eze, E., & Okoye, E. (2019). Forensic accounting and fraud detection and prevention in Imo State Public Sector. *Accounting and Taxation Review*, 3(1), 12–26.

Fathi, W. N. W., Ghani, E. K., Said, J., & Puspitasari, E. (2017). Potential employee fraud Scape in Islamic banks: The fraud triangle perspective. *Global Journal of Al-Thaqafah*, 7(2), 79–93. doi:10.7187/GJAT122017-3

Gbegi, D. O., & Adebisi, J. F. (2014). Forensic accounting skills and techniques in fraud investigation in the Nigerian public sector. *Mediterranean Journal of Social Sciences*, 5(3), 248–252. doi:10.5901/mjss.2014.v5n3p243

Gentles, S. J., Charles, C., Ploeg, J., & McKibbin, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report*, 20(11), 1772–1789.

Gray, D. (2008). Forensic accounting and auditing: Compared and contrasted to traditional accounting and auditing. *American Journal of Business Education*, 1(2), 116–126. doi:10.19030/ajbe.v1i2.4630

Hassan, R., & Noor, F. M. (2020). Islamic Good Governance for Waqf Institutions: A Proposed Framework. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 424–439). IGI Global. doi:10.4018/978-1-7998-0218-1.ch023

Horton, J., Macve, R., & Struyven, G. (2004). Qualitative research: experiences in using semi structured interviews. In C. Humphrey & B. Lee (Eds.), *The real life guide to accounting research: A behind-the-scenes view of Using qualitative research methods* (pp. 339–357). Elsevier. doi:10.1016/B978-008043972-3/50022-0

Joseph, F. A., Okike, B. M., & Yoko, V. E. (2016). The Impact of forensic accounting in fraud detection and prevention: Evidence from Nigerian public sector. *International Journal of Business Marketing and Management*, 1(55), 34–41.

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in IS research. *Journal of Computer Information Systems*, 54(1), 11–22. doi:10.1080/08874417.2013.11645667

## **Combating Fraud Through Forensic Accounting**

- Mustafa, D., Baita, A. J., & Adhama, H. D. (2020). Quantitative economic evaluation of zakah-poverty nexus in Kano state, Nigeria. *International Journal of Islamic Economics and Finance*, 3(1), 21–50. doi:10.18196/ijief.2120
- Nor, S. M., & Hashim, N. A. (2015). CSR and sustainability of Islamic banking: The bankers view. *Jurnal Pengurusan*, 45, 73–81. doi:10.17576/pengurusan-2015-45-07
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. doi:10.1177/1609406917733847
- Ogiriki, T., & Appah, E. (2018). Forensic accounting & auditing techniques on public sector fraud in Nigeria. *International Journal of African and Asian Studies*, 47, 7–18.
- Ogundana, O., Okere, W., Ogunleye, O., & Oladapo, I. (2018). Forensic accounting and fraud prevention and detection in Nigerian banking industry. *COJ Reviews & Research*, 1(1), 1-8. doi:10.31031/COJRR.2018.01.000504
- Okoye, E., & Ndah, E. N. (2019). Forensic accounting and fraud prevention in manufacturing companies in Nigeria. *International Journal of Innovative Finance and Economics Research*, 7(1), 107–116.
- Okoye, E. I., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and Prevention in the Public Sector. (A Study of Selected Ministries in Kogi State). *International Journal of Academic Research in Business & Social Sciences*, 3(3), 1–19.
- Olaoye, C. O., & Olanipekun, C. T. (2018). Impact of forensic accounting and investigation on corporate governance in Ekiti State. *Journal of Accounting. Business and Finance Research*, 4(1), 28–36. doi:10.20448/2002.41.28.36
- Othman, R., Aris, N. A., Mardziah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector: Accountants' and internal auditors' perceptions. *Procedia Economics and Finance*, 28, 59–67. doi:10.1016/S2212-5671(15)01082-5
- Rafay, A., & Farid, S. (2018). Shariah Supervisory Board Report (SSBR) in Islamic Banks: An experimental study of Investors' perception and behaviour. *International Journal of Islamic and Middle Eastern Finance and Management*, 11(2), 274–296. doi:10.1108/IMEFM-07-2017-0180
- Ramaswamy, V. (2007). New frontiers: Training forensic accountants within the accounting Program. *Journal of College Teaching and Learning*, 4(9), 3–38. doi:10.19030/tlc.v4i9.1545
- Suryanto, T., & Ridwansyah, R. (2016). The Shariah financial accounting standards: How they prevent fraud in Islamic banking. *European Research Studies*, XIX(4), 140–157. doi:10.35808/ersj/587
- Thaker, M. A. M. (2018). A qualitative inquiry into cash waqf model as a source of financing for micro enterprises. *ISRA International Journal of Islamic Finance*, 10(1), 19–35. doi:10.1108/IJIF-07-2017-0013
- Umar, U. H. (2017). The relevance of accounting profession in Islamic inheritance. *Bayero International Journal of Accounting Research*, 11(1), 414–430.

- Umar, U. H. (2019). Integrating family *waqf* into an inheritable going concern business: an instrument for the sustainable welfare of exempted heirs. In K. M. Ali, M. K. Hassan, & A. E. S. Ali (Eds.), *Revitalization of Waqf for Socio-Economic Development* (Vol. 2, pp. 87–87). Springer. doi:10.1007/978-3-030-18449-0\_4
- Umar, U. H. (2020). The business financial inclusion benefits from an Islamic point of view: A qualitative inquiry. *Islamic Economic Studies*, 28(1), 83–100. doi:10.1108/IES-09-2019-0030
- Umar, U. H., Ado, M. B., & Ayuba, H. (2019). Is religion (interest) an impediment to Nigeria's financial inclusion targets by the Year 2020? A qualitative inquiry. *Qualitative Research in Financial Markets*, 12(3), 283–300. <https://DOI.org/10.1108/QRFM-01-2019-0010>
- Umar, U. H., & Haron, M. H. (2021). (Accepted). The Islamic need for investing inherited wealth and accounting treatments. *The Journal of Muamalat and Islamic Finance Research*.
- Umar, U. H., Kademi, T. T., & Haron, M. H. (2020). Integrating waqf and business: Ensuring business sustainability for the welfare of heirs and non-heirs. *International Journal of Economic. Management and Accounting*, 28(1), 191–213.
- Umar, U. H., & Kurawa, J. M. (2019). Business succession from an Islamic accounting perspective. *ISRA International Journal of Islamic Finance*, 11(2), 267–281. <https://DOI.org/10.1108/IJIF-06-2018-0059>
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 38–42.
- Zolkafli, S., Nazri, S. N. F. S. M., & Omar, N. (2021). Factors Influencing the Outcome of Money Laundering Investigations. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

## **ADDITIONAL READINGS**

- Abdul Rahman, R., & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia: Social and Behavioral Sciences*, 145, 97–102. doi:10.1016/j.sbspro.2014.06.015
- Al-Hilali, M. T. & Khan, M. M. (n.d.). *Translation of the Meanings of the Noble Qur'ān in the English Language*. Madinah: King Fahd Complex for the Printing of the Noble Qur'an.
- Alabdullah, T. T. Y., Alfadhl, M. M. A., Yahya, S., & Rabi, A. M. A. (2014). The Role of Forensic Accounting in Reducing Financial Corruption: A Study in Iraq. *International Journal of Business and Management*, 9(1), 26–34.
- Association of Certified Fraud Examiners (ACFE). (2020). *Forensic Accountant*. Retrieved from <https://www.acfe.com/forensic-accountant.aspx>
- Association of Certified Fraud Examiners (ACFE). (n.d.). *Fighting fraud in the government*. Retrieved from <https://www.acfe.com/gf/>

### ***Combating Fraud Through Forensic Accounting***

Institute of Forensic Accountants. (2020). *Benefits of Joining IFA – Nigeria*. Retrieved from <https://ifa.org.ng/>

Khaliyl, A. (2007). *English Translation of Jami At-Tirmidhi*. Maktaba Dar-us-Salam Publishers.

O’Neil, J. M., & Egan, J. (1992). Men’s and women’s gender role journeys: Metaphor for healing, transition, and transformation. In B. R. Wainrib (Ed.), *Gender issues across the life cycle* (pp. 107–123). Springer.

Osho, A. E. (2017). Impact of forensic accounting on university financial system in Nigeria. *European Scientific Journal*, 13(31), 571–590. doi:10.19044/esj.2017.v13n31p571

Umar, U. H., & Mohammed, S. (2017). *The nexus between Islamic inheritance and financial accounting: An expository discourse*. Paper presented at the 2nd International Research Conference on Economics Business and Social Sciences, Jointly Organized by Center for Sustainability Research and Consultancy, Pakistan, School of Economics, Finance and Banking, University Utara Malaysia etc., held at Park Royal Hotel Penang, Malaysia, July 11-12, 2017.

## Chapter 12

# Forensic Audit Practices to Reduce Financial Frauds

Elif Yücel

Bursa Uludag University, Turkey

### ABSTRACT

*International markets are highly competitive these days due to the globalization of the industry. Companies might manipulate this competition to gain some advantages. Also, technology has been the main force behind business growth in the past decade. The widespread use of technology and globalization also increased financial crimes. Accordingly, the auditing profession has entered into the process of institutionalization and embedded itself within institutions due to the enhanced complexity of frauds, corruption, and manipulations. One of the developments that have been happened in the field of auditing is the emergence of the “forensic auditing” profession. This chapter discusses the conceptual framework of the forensic audit and its essential role in preventing frauds and corruption.*

### INTRODUCTION

Currently, the auditors have to work as detectives to investigate the reliability of evidence and the true-ness of financial statements with an inquisitive approach (Ramzan *et al.*, 2020). The auditing scandals that occurred at the beginning of the 21<sup>st</sup> century revealed the auditing profession’s deficiencies. All conventional auditing practices have been reviewed, and it is revealed that forensic audit can meet all financial statement users’ needs.

A forensic audit is a group of practices that enable accounting and auditing knowledge and research skills in the detection and solution of legal problems. It is also a science that uses auditing with various methods and techniques as a tool for identifying and developing evidence related to fraud (Houck *et al.*, 2006). In the literature, forensic auditing and forensic accounting concepts are used interchangeably. Forensic audit includes the implementation of capabilities for private investigation and examination in audit, finance, and quantitative methods in order to utilize them to collect all probative elements, analyze and evaluate them and share them, make them more understandable and share with the public in forensic

DOI: 10.4018/978-1-7998-5567-5.ch012

## ***Forensic Audit Practices to Reduce Financial Frauds***

processes or for the solution of other various disputes (Seddon and Pass, 2009; Rezaee & Lander, 1996; Crumbley & Apostolou, 2002; Kaya, 2005; Watters *et al.*, 2007).

In the context of accountancy and law, forensic auditing can be used in numerous areas, including analysis for fraud and corruption such as forgery of documents, computer fraud, credit card fraud, software piracy, tax fraud, embezzlement, and manipulation of financial information. It also evaluates and determines the actual loss of earnings in cases where disputes occur between partners due to bankruptcy, merger, demerger, and acquisition lawsuits (Bell, 2008; Clark & Diliberto, 1996; Rafay, 2021).

The main priority of the forensic auditor is to detect fraud, corruption, and manipulation. Thus, forensic auditors' practices and techniques to detect financial crimes will be discussed in the section. Concerning the reliability of the collected evidence, forensic document examination, as to the areas of risk in cheating, concentrating on these areas, applying various cheat detection methods, and effective use of technology in the process have been determined for a successful forensic auditing service. Also, these red flags used to detect fraud and manipulations will be highlighted throughout this chapter.

## **BACKGROUND**

Although it is prevalent nowadays, forensic auditing is not a new discipline. It is a known fact that in 3000 B.C., people in Egypt, whom we may call the pioneers of the accounting profession, used their specialty to audit fraud in stocks (D'Ath, 2008). The first documented forensic auditing case took place in Canada in 1817 when an expert accounting was assigned to audit the insolvent's properties and was summoned to court as a witness for evaluating Meyer's insolvent properties v. Sefton case (Crumbley, 2001). From the early 1980s, due to the change of needs in the auditing profession with an altered economic environment in many developed countries, forensic auditing has begun to improve (D'ath, 2008). In the same period, Joe Wells founded the Association of Certified Fraud Examiners (ACFE), which trains expert fraud auditors and carries out fraud detection practices. In the 1990s, AICPA made significant progress in their field of application by founding the "Forensic and Litigation Services Committee" with Peter Frank, one of Price Waterhouse's partners. The American College of Forensic Examiners International (ACFEI) was founded in 1992, and awareness of forensic auditing activities increased. The most significant milestone in forensic auditing's professional development came in 2002 with adopting the Sarbanes Oxley (SOX) Act following scandals in global companies. Another necessary evolvement is publishing the report titled "Incorporating Forensic Procedures in an Audit Environment," which emphasized the effect of forensic auditing techniques on the whole audit process by AICPA's Litigation and Dispute Resolution Services Subcommittee in 2003 (Minniti, 2011). As a result of these regulations, it was pointed out that several services provided by auditing firms fell within forensic services; hence they should be provided by a forensic auditor. Therefore, the importance placed on forensic auditing rose to a superior level, and most auditing firms extended their practices to include forensic auditing applications.

Forensic auditing based on predicting crimes by examining the numbers of the profession is a very comprehensive process. Forensic auditing, performed by employees and managers investigating fraud and corruption, disagreements in decisions taken in the business and determination of disputes, calculation of the size of financial losses in the enterprise, examination of behaviors contrary to professional rules, disputes between shareholders resolution, detection of technology-related losses (Paranjape & Sheeth, 2011), the company evaluation of assets during mergers and acquisitions, against disputes mediation and arbitration, investigation of insurance crimes (Yildirim & Rafay, 2021), systematic of evidence conducting



criminal investigations (Kasum, 2009) to be presented as legal, and many activities, such as proposing technical arrangements and supporting the court process (Rezaee & Lander, 1996).

Forensic auditors who can play an essential role in preventing fraud, corruption, and manipulations, have gained considerable attention in the business community because of the rapidly increasing digital information in the 21st century. Today, especially cyber breaches such as the illegal transfer of funds or stealing confidential personal data, and insider threats as data manipulation or information technology sabotage are emerging as the fastest-growing fraud risks faced by forensic auditors. So forensic auditors make great use of both structured data such as accounting data and unstructured data together with modern data sources such as e-mail, voice recordings, free-text payment descriptions, and social media (Rezaee and Wang, 2019).

## **LITERATURE REVIEW**

When literature on forensic auditing practices is reviewed, it is clear that the bulk of the research is concerned with evaluating the competence of professional auditors (Rezaee *et al.*, 1992; Mohd & Mazni, 2007; Kasum, 2009; Gunasegaran *et al.*, 2010; Okunbor & Obaretin, 2010; Hao, 2010; Elias, 2014; Okoye & Ndah, 2019). In these studies, strategies determined for developing and disseminating professional practices emphasize forensic auditing services' necessity to eliminate these negativities. Rezaee *et al.* (1992) highlighted the importance and necessity of forensic auditing service in their work. They evaluated the strategies that should be determined to disseminate forensic auditing practices according to the existing laws and regulations. Also, Mohd and Mazni (2007) examined the forensic auditing profession's current situation in their country by taking practitioners' opinions about forensic auditing and its development in Malaysia. Kasum (2009) investigated that fraud and corruption negatively affect the economies of developing countries. To eliminate these negativities, she investigated the necessity of forensic auditing practices both in the private and public sectors and forestalled the use of forensic auditing. In their studies, Quaddus and Evans (2010) have created a model for increasing the utilization of such services by measuring forensic auditing services' requests to detect and prevent fraud and corruption of large-scale enterprises in Malaysia. In his study, Hao (2010) emphasized the forensic auditing profession's need by evaluating China's existing inspection deficiencies. Likewise, according to Elias (2014), forensic auditors play a vital role in minimizing and eliminating fraudulent financial activities and reducing financial crimes that can endanger the economy's soundness.

Some of the studies on forensic auditing practices in the literature are related to using these auditing activities (Gray, 2008; DiGabriele, 2009; Chukwunedu & Okoye, 2011). These included that forensic auditing services should be included in the audit process. Auditors will have more success in detecting fraud and corruption and may make a difference in their professions if they have certain forensic auditing features. Digabriel (2009) concluded that forensic auditing should be involved in the audit process. Without proper analytical qualities, auditors will not be effective and will not be able to practice forensic auditing. Chukwunedu and Okoye (2011) investigated independent auditors' effect on independent auditors' success in detecting fraud and corruption by using forensic auditing techniques in independent auditing activities by considering cost-benefit analysis. The research concluded that forensic auditing practices would increase success, and suggestions were made regarding integrating forensic auditing practices in training programs and independent audit studies. The paper by Gray (2008) emphasizes that the forensic auditing profession is a separate profession independent of the auditing profession.

Another critical study for developing forensic auditing policies is related to the types of technical equipment and attributes forensic auditors should have. Although most of these studies advocate parallel views on the skills and features that forensic auditors should have, each of them has been emphasized with different features or evaluated from a different perspective (Harris & Brown, 2000; Grippo & Ibex, 2003; Messmer, 2004; Ramaswamy, 2005; DiGabriele, 2009; Boys, 2008; AICPA, 2009). In their work, Grippo and Ibex (2003) focused more on the importance of forensic auditors' professional experience in related fields. Harris and Brown (2000) assessed more personal abilities, such as analytical thinking and communication skills, which the forensic auditors should have. In his study, Ramaswamy (2005) emphasized the necessity of accounting and financial information and financial analysis ability, which is the most important in the tray of fraud and corruption.

On the other hand, Boys (2008) determined the technical and general skills that forensic auditors should have and investigated the differences between these requirements and the competencies provided by the current accounting education, and questioned the deficiencies in forensic auditing education. Digabriele (2008) has investigated what features a forensic auditor should have from the perspective of academics, practitioners, and those who have benefited from forensic auditing services. AICPA conducted a similar study in 2009.

Some other studies in the literature are about forensic auditing practices and the importance of technology. Wadhwa and Pal (2012) have discussed forensic auditing techniques like Benford's Law, ratio analysis, etc., that can be applied to find fraud and manipulations. Also, Okoye and Ndah (2019) found that forensic auditing practices are sufficient to prevent manufacturing companies' fraud. According to Bhasin (2016), due to the rapid spread of cloud computing and smart technologies, analytical technology knowledge is necessary for fraud and corruption investigations within the scope of forensic control applications. Also, Pamungkas *et al.* (2018) emphasized that forensic control technology helps prevent fraud and corruption by evaluating fraud risk. Additionally, Rezaee and Wang (2019); examined the relevance of data analytics to forensic auditing practice and emphasized data analytics and forensic auditing should be integrated into the business curriculum in their study.

Some studies focused on the forensic investigation process (Manning, 2005; Singleton *et al.*, 2006; Hopwood *et al.*, 2008; Zimbelman & Albrecht, 2012). Manning (2005) emphasized that all forensic investigations have similarities, and each investigation consists of planning, execution, analysis, reporting, and prosecution stages. Singleton *et al.* (2006) state that the forensic auditor's financial skills and investigation mentality in the forensic audit process gain importance to collect sufficient evidence against unsolved problems. Likewise, Hopwood *et al.* (2008) highlighted that the investigation process should be carried out in a planned manner following the laws in line with meaningful goals. In this process, the forensic auditor's most crucial issue is to pay attention to be fair and impartial by basing the investigation on documents. According to Zimbelman & Albrecht (2012), forensic auditors use both documents and evidence obtained by investigating witnesses regarding suspected or known nonconformities in the forensic auditing process.

In light of the literature review, forensic auditors play a vastly comprehensive role in detecting fraud and corruption. The most commonly employed practices they use are as follows:

## **FORENSIC AUDITING PRACTICES**

### **Evaluation of Fraud Risk**

The primary purpose of forensic auditing activities is to prevent and detect fraud and corruption before they emerge. Therefore, it is necessary to measure and evaluate the fraud risk before starting audit activities. In the most general definition, fraud risk is the risk of abuse of assets and pretenses on financial statements enough to negatively influence the users' decisions (Güredin, 2007). Compliance with all the procedures and standards in the audit process is not always directly proportional to fraud detection (Ranallo, 2006). That is why fraud risk factors are primarily detected. The necessity for defining fraud risk factors and early detection of fraud also increases the need for forensic auditing.

Fraud risk evaluation, which is more critical in the planning of forensic auditing work, should cover a cumulative process that continues from the beginning of its studies to its evaluation (Colbert & Turner, 2000). With the evaluation of fraud risk, forensic auditors can ensure that the resources are used in the most effective way, an early warning system is created against possible risks, and measures are put into practice before fraud and corruption occur (Özbek, 2003). While evaluating the risk of fraud, it is necessary to consider the probability of realizing the forensic auditors' forensic risk factors and the extent of the damages that will occur when they occur (Singleton & Singleton, 2010). Therefore, the forensic auditors can concentrate their works in the riskiest areas and with less cost can provide higher benefits to businesses (Reinstein & McMillan, 2004). Since fraud risk assessment is based on highly subjective judgments, forensic auditors should be careful, especially when determining fraud risk factors. These factors, which are very difficult to determine, are classified according to each business's needs. They vary according to the business's ethical perceptions and the employees and the business's management gaps (Kenyon & Tilton, 2006). For this reason, forensic auditors must collect information about the enterprises from as many different sources as possible and analyze all the data obtained in order to determine the fraud risk factors most effectively (Ramos, 2003). The most prevalent fraud risk factors in business can be explained in a fraud triangle (Wilks & Zimbelman, 2002):

- *Pressure:* The fact that the enterprise's financial stability and profitability are under threat due to various external factors causes managers to resort to fraud and corruption. These external factors are high competition, continually changing environmental conditions, customer demands, minus cash flows, excessive growth, irregular profitability, and continually changing legal regulations. The expectations of third parties related to the business put pressure on the managers. In particular, high profitability expectations of investors and lenders can cause fraud and corruption. Apart from that, high-performance values and financial targets expected from management are also risk factors for fraud and corruption.
- *Opportunity:* The most crucial risk factor in enterprises is the lack of an effective internal control system. Failure to keep workers under surveillance always poses a risk for fraud and corruption. Also, the risk of cheating is higher in enterprises that can make purchases in different periods, amounts, and amounts due to the industry or country's conditions. Complex and variable organizational structures are always open to fraud and corruption.
- *Rationalization:* Rationalizations are risk factors that can occur when the slightest pressure or opportunity arises. Most companies are vulnerable to the phenomenon of fraud and corruption, where efficient coordination cannot be accomplished, or ethical standards cannot be passed to

workers. Moreover, vulnerability also increases where criminal penalties for fraud and corruption are inadequate, and no appropriate monitoring mechanisms are available.

## **Forensic Document Examination**

Documents are written tools that provide explicit or implicit notices to the receiver, and they are the most effective source of the forensic auditing process. However, documents are not always reliable sources. Their reality and accuracy should be determined beforehand. Forensic document examination is conducted in this respect. It involves analyzing, comparing, and examining evidential documents subject to disputes and the writing, signatures, marks, and signs on these documents.

All documents including writing, identity card, license, passport, banknote, photocopy, fax, print outs, blackmail letters, and negotiable instruments such as check, note, and bond should be altered or deleted, which raises issues of the authenticity of the documents if subjected to forensic examination. Suspicious indications for the existence of such situations are as follows (Cendrowski *et al.*, 2007):

- If the document is at a well-hidden or unusual place
- If the chronological order of the document does not have any order
- Repeated errors in date entry for documents
- Page qualities of multi-page documents or difference between their order
- Difference between the commonly used font type or size
- Different kind of stapling for multi-page documents
- Finding signs of deletion or alteration on documents
- Usage of a soft-tip pen and special inks that disappear in a few days
- Use of different pens on the same document
- Change of hand-writing characters on the same document
- Increase in small fonts
- No sign of piercing the documents for filing
- Rough and dull page surfaces
- Slight vertical and horizontal lines on documents like that of a copied paper
- Existence of unidentified notes

Hand-writing crimes are another subject of examination on their own. Personalized texts, signatures, symbols, or punctuation marks can be imitated by hand or prepared with special equipment. However, experts can distinguish false documents by analyzing the main control areas of points, hooks, curves, and lines. Two different people cannot write all four elements in the same way. Moreover, the forensic document examination expert considers inclination, typeface, range of words, length and alignment of letters, line spacing, personal text figures, and creativities. Hand-writing examinations mostly analyze slow pen movements, hand tremors, consistency in writing direction, a difference in signature character, and real ink usage (Cendrowski *et al.*, 2007).

Simple tools such as pens, text deleting fluid, carbon paper, scissors, color copier, scanner, or printer are ubiquitous for committing crimes like altering documents, generating false ones, copying, reproducing, and stealing. Various professionals like calligraphers, teachers, police officers, physicists, and doctors met the expert demand in the past for document examination. However, they became insufficient due to rapid technological advancements, and there emerged a need for expert individuals and institutions on

document examination. Today, forensic documents are conducted by the Branch of Forensic Document Examination within the Department of Specialized Physics under the Institute of Forensic Medicine. Criminal laboratories under the General Directorate of Security and General Command of Gendarmerie also undertake the same task (Birincioğlu, 2005).

## **Using Technology for Forensic Auditing**

It is a well-known fact that fraud and corruption are on the rise with advances in technology. Increasing the use of information technology and moving financial transactions to the computer has led to data security (Rafay, 2019). The scandals showed that auditors are inadequately skilled in data analytics, accounting software, and program designs. To detect fraud and corruption in the financial reports, it is necessary to understand computers and statistical programs that are among the requirements for forensic auditors today.

With the utilization of computers in accounting proceedings, the court process has also gained flexibility. The convenience of editing records at any time with the features of computers and executing an arbitrary recording system without complying with legal restrictions have made it easy to commit fraud and corruption on books and documents. Furthermore, the data can be transferred, stolen, deleted, or altered quickly due to the constant innovations in information technologies and the internet, which is among the most important means of communication of our age (Albrecht *et al.*, 2011). At this point, the forensic auditors need to know all necessary computer software and information technology, even if not being an expert in this area.

Committed to taking control of the company's accountants, exploiting the market price, making an imaginary transaction, concealing commercial operation knowledge, or violating it (Seetharaman *et al.*, 2004), are increasing day by day. Thus, measures are taken against fraudulent practices by technologically assisted systems, and strategies are discovered in time by those who conduct the fraud hence avoiding these safeguards. For that reason, every model or technique used to prevent fraud cannot have the initial effect after using it one time. These techniques, which are primarily used to detect and deter fraud and corruption, should continuously be updated with and upgraded new features against the rapidly advancing I.T. industry (Bolton & Hand, 2002). In this respect, forensic auditors should always cooperate with tech firms to develop newer and more comprehensive software.

The following applications are commonly used to detect computer-aided crimes:

- **Detecting Vulnerable Parts in the System:** The complexity of a company's information technologies demonstrates that the company is vulnerable to fraud and corruption. Because the system contains more vulnerabilities as it becomes complex. Consequently, forensic auditors should primarily detect these vulnerabilities in the system and start investigating these points. Relevant information and records must be examined to gather clues (Markman *et al.*, 2006).
- **Examination of Similar Crimes in the Past:** One of the most useful evidence to better understand the committed crime is past crimes. Similar crimes committed in the past may be examined to find out its source, technique, and technologies utilized in committing the crime, which may consequently lead to detecting the tools used in the current crime, and the comparison of timing may provide foresight for the time and place of the crime. The forensic auditors will directly reach the result when these three issues are clarified (Casey & Seglem, 2003).

## ***Forensic Audit Practices to Reduce Financial Frauds***

- **Analyzing the Used Technologies:** Source of the crime can be reached. If a financial loss is in question, where and how this loss is transferred can be determined by analyzing the properties and shortages of technological tools, which the business organization uses the most. Moreover, knowing which technologies are used enables determining the extent to which the electronic data are authentic and reliable (Malinowski, 2005).
- **Gathering Information and Evidence:** Forensic auditors can make the data healthier and more usable via implementations such as retrieving the deleted data by various computer techniques, eliminating the unnecessary data and files, analyzing the history of transactions in the computer, determining the locations of hidden or masked files. Then, the evidence is gathered, and a solution is sought by focusing on the central problem (Casey & Rose, 2003).
- **Determining the Source by Comparison:** Analyzing all of the evidence obtained during the research process enables forensic auditors to reach the evidence source efficiently. Reaching the crime source gets easier when parts, which are not meaningfully different from one other, are combined by carrying out this comparison via production place, methods of falsification, and location of the evidence (Casey & Seglem, 2003).

## **Interview and Interrogation for Forensic Auditing**

Interviewing and interrogation are two of the most beneficial evidence-gathering methods used to determine deception and corruption. Although these two notions are used together, there is a relatively fundamental difference between them. The interview aims to research revealing truth or obtaining information. Interrogation is more result-oriented and aims to acquire confession. The interviewing method is used more in forensic auditing implementations, and the interviews that are carried out may be turned into interrogations from time to time.

Interviewing with everyone, who is suspicious or thought to have information about the subject, provides justification of other evidence or obtaining clues required for new evidence. During the interview, the person's conscious and unconscious confessions significantly direct the research (Dee & Durtschi, 2010).

The forensic auditor needs to be cautious in the interviews and interrogations. Forensic auditors must not use illegal interrogation methods such as torture, threat, or deception. A person must be punished for a crime regardless of the consequences. Interviews and interrogation, while different in their aims, are much the same in the techniques used. Points, which forensic auditors have to take into consideration during interview and interrogation that must take approximately 30 minutes in general, are as follows:

- The forensic auditors become more effective and persuasive during interview and interrogation as long as he/she possess lots of information about the subject. Given such variables, the impression of solving the problem is formed from other information that is collected. Therefore, the individual prefers confession to hide the knowledge or taking part in the crime.
- Forensic auditors have to plan the interview and interrogation, to be conducted, with all details. Essential questions to be asked must be issued before interview and interrogation, and speeches must be directed to prevent wandering from the main subject.
- Forensic auditors must determine behavior during the interview and interrogation beforehand and abide by this behavior during the interview. There are different manners of behaving in legal cases, based on characteristics, mental status, the status of a person's witness, being interviewed,

and interrogated. If the interviewer has adequate time, they should collect as much information as possible about the individual being interviewed and their intentions (Dee & Durtschi, 2010).

- Correct selection of people, who are to be interviewed with or interrogated, has importance in time and cost management. Loss of time and money, caused by interviews that are carried out with people who are not related to the case, generally cause a lack of attention on people who must be interviewed with and interrogated.
- The appearance of forensic auditors during interviews and interrogation is also essential. Over-formal and over-sportive clothes must not be preferred in general. He/she must be simple, and accessories must not be used. The way of clothing must vary based on the person who is interviewed with or interrogated. For example, if an interview is conducted with a worker, wearing an over-expensive suit prevents obtaining a close connection (Cendrowski *et al.*, 2007).
- The expression, created by forensic auditors at the beginning of the interview and interrogation, is crucial for the process. Thus, forensic auditors must easily start their speeches with a soft voice tone and look polite and serious. Moreover, the person to be talked with must be definitely relieved before starting an interview or interrogation. Tea, coffee, or a similar beverage may be offered to the person for this purpose.
- Forensic auditors, who conduct interviews and interrogations, must be a good listener initially. It is required to let the person, who is interviewed with or interrogated speak, and he/she must not be interrupted. Also, various mimics, moves, or voices must be used to react to things that the person says other than listening steadily.
- Selection and physical conditions of the place where interview and interrogation are carried out are included in the forensic auditors' subjects. Forensic auditors shall prefer their own office rather than a particular interrogation room. Nevertheless, precautions must be taken against external factors, which may interrupt the talk, such as telephone, visitor, or an open window. No elements that may distract the person's attention, who is interviewed with or interrogated, or that may annoy him/her must be available in the place where interview and interrogation are carried out. Forensic auditors' offices must be plainly furnished, and the walls must be painted in more relaxing colors such as light blue or light green for this purpose. The way of sitting during interviews and interrogation is essential as well. The most particular sitting plan is how the forensic auditor and interrogated person sit on two opposite chairs. Also, a voice or video recorder must be available in the place where the interrogation is conducted, within the knowledge of the person who is interviewed with or interrogated (Sennewald & Tsukayama, 2006).
- Forensic auditors must not be interested only in the things that the person, who is interrogated, says during the interview and interrogation. The facial expression, mimics, body and eye movements, preferred words, change in voice tones, and general posture of the person interviewed with or interrogated are issues that must be monitored because people provide clues by their moves in general when they lie.
- Arguing with the person, who is interrogated, or objecting to what he/she says only damages the process of interrogation. No information can be obtained from a person who is interrogated with such a technique. An interrogation related to feelings must be developed for suspects who implement deception and corruption with feelings such as ambition, greed, jealousy, or anger, rather than that. For the purpose, clues must be obtained by asking questions related to the feelings of the person, who is interrogated, and which are not related to the main topic, such as "How do you

feel?”, “How can I help you?” “Whom may I call for you?” rather than critical questions such as “Why did you do this?”.

- Whether the person who is interrogated is lying or not must be taken into consideration. Lies generally appear in ways of denial, negligence, decreasing, exaggerating, or making up. In general, the person, who denies, answers all the questions with “I did not do it” frequently. The people, who tell the truth by decreasing, are in attempts to lightening their crimes by expressions such as; “yet, a short time ago, newly, some.” Exaggeration action appears when the person introduces himself/herself. For example, a person who is interrogated for debit, etc. crimes, exaggerates his/her honesty and wealth. The lie, which is the hardest to determine, is making up. Because there is a story, which is newly written, forensic auditors must take notes about each small detail and wait for the story to be changed with trap questions at this point (Cendrowski *et al.*, 2007).

## **DETECTION OF FRAUD AND CORRUPTION**

Companies demand forensic auditing services, usually in the court process after fraud and corruption occurs or when there are essential suspicions regarding the possibility of fraud and corruption. In this respect, the detection of fraud and corruption is vital for the profession of forensic auditing. With the growth of the markets, it has become increasingly difficult to identify fraud and corruptions due to the growing sophistication of transactions, the fact that fraud and corruptions are usually hidden in legal works, the use of technical innovations, and the more manageable and careful covering or falsification of facts and records. The first step of detecting fraud, which is one of the forensic auditing’s primary objectives, is to determine where to start the control. Understanding the factors causing frauds and determining the riskiest accounts and the priority areas to be examined in detail provides the most effective detection of frauds. At this stage, the forensic auditor’s suspicious and skeptical approach is critical. Also, the forensic auditors must evaluate all processes with professional skepticism while detecting fraud. It should be kept in mind that there may be deceptive practices in all books and financial statements, and all documents may be counterfeit. The situation mentioned here is not distrust but only an investigation (Kenyon & Tilton, 2006).

Various methods can use by forensic auditors to detect fraud in practice. Nevertheless, the most extensive global studies on occupational fraud have been prepared by the Association of Certified Fraud Examiners (ACFE) since 1996. According to these reports, the most commonly used fraud detection methods are given in Table 1.

As shown in Table 1, the most used detection method for all years has been determined as warnings and complaints, and the most important source of these warnings and complaints is the employees. These employees also help to execute a successful internal control system directly. However, due to their threats and fear, they often report the tricks they observe to the top management secretly. In this respect, the number of tricks detected with unknown warnings is also very high. The most reliable source of fraud detection information is customers. They can also monitor business activities such as employees, the company itself, and even become involved in these activities. Based on all these facts, a forensic auditor should first question the suspect. The requisite information is much easier to obtain from people who work for the company, primarily through conversations. At this stage, the forensic auditor should understand psychological query techniques because the slightest negative impression of the questioned person can change the course of the interview.



*Table 1. Percentage of Fraud Detection Methods (ACFE: 2010 – 2020)*

	2010	2012	2014	2016	2018	2020
Tips	40	42	43	39	40	43
Internal Audit	14	14	14	17	15	15
Management Review	15	15	16	13	13	12
By Accident	8	7	7	6	7	5
Account Reconciliation	6	7	7	6	5	4
External Audit	5	3	3	4	4	4

*Table 2. Percentage of Anti-Fraud Control Methods (ACFE: 2010 – 2020)*

	2010	2012	2014	2016	2018	2020
External Audit	81	80	82	82	80	83
Code of Conduct	75	78	77	82	80	81
Internal Audit	68	68	71	74	73	74
Management Certification of Financial Statements	68	69	70	72	72	73
Management Review	59	61	63	65	66	65
Hotline	51	54	54	60	63	64
Independent Audit Committee	58	60	63	63	61	62
Employee Support Programs	55	58	52	56	54	55
Anti-Fraud Policy	43	47	45	50	54	56
Fraud Training for Employees	44	47	48	52	53	55

Another research conducted by ACFE is anti-fraud control methods used by victim companies. As can be understood from the results in Table 2, companies which are the victim of fraud mostly trust audits conducted by independent parties. Also, many activities such as establishing ethical rules in the enterprise, ensuring the effectiveness of the internal audit activities, and supervising the management facilitate fraud detection (Khan *et al.*, 2020). Therefore, the forensic auditor must primarily focus on the enterprise's internal systems and begin auditing books, documents, and tables after detecting the enterprise's organizational and internal control system deficiencies.

Forensic auditors use many different techniques to detect fraud and corruption. The increase in financial statement scandals and companies' million-dollar losses has shown that fraud and corruption are too late to detect. The losses can only be detected by preventing, preventing, or deterring before fraud and corruption occur. When examined, it is seen that many of them occur after similar symptoms appear. Especially in enterprises with a weak management structure, these symptoms are more common. These indicators are called "red flags" in the literature.

## RED FLAGS

Even if they are not considered proof of fraud, these symptoms indicating the fraud is done in the financial statements are expressed as a “red flag” (Dzamba, 2004). Fraudulent situations often display a significant deviation, and red flags refer to situations that are unnatural or different from usual activities (DiNapoli, 2010). In the literature, there are many red flag classifications for detecting fraud and corruption. The most commonly accepted of these classifications was devised by the Federal Trade Commission (FTC) in Fair Accurate Credit Transactions Act (FACTA) implemented in 2003. FACTA classified red flags as follows:

- Warning and notices from consumer reporting agencies,
- Suspicious documents,
- Suspicious personnel identifying information,
- Unusual activities in accounts,
- Notices from customers, victims of identity theft, and law enforcement authorities.

The use of red flags in the forensic auditing process significantly increases the success of the investigations. The red flags most frequently used by forensic auditors in practice are as follows:

### Red Flags on Fraudulent Financial Reporting

- **Accounting and Document Abnormalities:** The balance of the reported income and sales accounts is very high, the sales discounts and sales returns accounts are very low, there are no or no provision accounts, excessive increases in trade receivables account, most of the reported income is not collected, original documents are not available, important bank accounts not disclosed, inconsistencies between revenues and sales and collection receipts or other supporting evidence (Albrecht *et al.*, 2011), inadequate disclosures in the balance sheet footnotes, periodic differences, created fictitious revenues and inappropriately valued assets (Singleton & Singleton, 2010), unexplained changes in the balance of the financial statements, regular change of bank accounts, excessively unrequited finding checks, deviations in cash accounts are high (DiNapoli, 2010), making large and high profitable transactions close to the end of the period, having insufficient equity structure, borrowing with excessive amounts and high interest, overdue increase in receivables.
- **Managerial Abnormalities:** Rapid growth, unusual profits, aggressive management style, obsessing the stock prices of the company, determining the micro-management style that means the top management is directed to do the work that the sub-units should do (Singleton & Singleton, 2010), finding significant lawsuits or reviews about the business, high amount of personal debtor and financial managers in difficulties, dishonest and morally qualified management staff, executing secret agreements with third parties, adopting a management policy with high staff turnover rate (DiNapoli, 2010), having a too complex business structure, high risk of the sector, frequent changes of the top management.

## **Red Flags on the Abuse of Assets**

- **Personnel Abnormalities:** Changes in the behavior of individuals, difficulty in looking into the eyes of people, increase in nervous behavior, irregular work schedule, sudden changes in lifestyle, unusual tendencies and suspicions, constant thoughtfulness, excessive boring behaviors, becoming wasteful (Singleton & Singleton, 2010), tendency to blame others, without giving information or permission dealing with subordinate jobs, reducing the severity of work, discounts offered by third parties to employees, decisions that are incomprehensible to procedures and frequent business trips.
- **Business Process Abnormalities:** Unusual relationships between crucial employees and suppliers or customers, confidentiality in relationships with third parties, and insufficient information flow to management, abnormalities in the recording of trading transactions, inconsistencies in the validation of sales, conflicts of interests between employees (Singleton & Singleton, 2010), the management or employee inconsistencies in income or analytical procedures working, ineffectiveness of the internal control system (Albrecht et al., 2011), increase in denunciations and complaints about the frauds performed, decrease or increase in stocks, missing or an excessive amount of cash in the safe, providing remarkable convenience to the customers or suppliers, making contracts for extended periods despite uncompetitive and unsuitable prices for the business.

## **FUTURE RESEARCH DIRECTIONS**

In this study, the methodology and practices of forensic audits are analyzed. The primary duty of the forensic auditor is to detect fraudulent activities. The result of this study highlights the red flags of possible fraud or corruption. Future research needs to examine the effectiveness of current red flags techniques from tax inspectors and auditors' perspectives.

## **CONCLUSION**

Forensic auditors' need to search for fraud and corruption appears to be a problem within the forensic auditor profession. Forensic auditors perform complex investigations and analyses to detect embezzlement and fraud. Forensic document examination, interview and interrogation techniques, technology usage, fraud risk evaluation, and red flags are the areas forensic auditor's emphasize.

Forensic audit activities must be used to prevent and detect fraud and corruption before it becomes evident. Therefore, fraud risk must be assessed prior to audit activities. In light of this, forensic auditors must collect information about the various enterprises to analyze all of the data obtained to determine which fraud risk factors are most significant. Nevertheless, it has been well demonstrated that corruption and fraud crimes tend to increase with technology progression. Therefore, computer knowledge and statistical program skills are a must for forensic auditors who must detect fraud and corruption in today's digital age.

Due to the increasing number of financial statement scandals and companies' million dollars in losses, it is often too late to prevent fraud and corruption. Losses can only be prevented, or deterred by investigating before fraud and corruption taking place. After a thorough investigation, it is seen that

## ***Forensic Audit Practices to Reduce Financial Frauds***

many frauds and corruptions manifested similar symptoms. These symptoms are commonly seen with weak organization, and these warning signs are called “red flags” in the literature.

Recently researchers have tried to stress the importance of using red flags early in the audit process. Red flags can act as a warning system for sensitive stakeholders who may be victims of fraudulent activity. Forensic auditors must use specific red flags when analyzing debts. Auditors use a variety of indicators to detect fraud and corruption.

Many businesses find their profitability decreasing due to internal and external issues. Under these circumstances, businesses must increase their stock prices and profitability in order to prosper. Some firms resort to financial statement tricks on the growth rates and profitability of their companies. Rapid changes compared with other companies in the sector indicate that the company could be in financial straights. Fraud and corruption are more common and evident in small or poorly managed companies. In businesses without an internal control system, wrong decisions are more likely to occur, and fraud in financial statements and assets loss will occur. Without corporate governance, fraud and corruption become the norm in society.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in her personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## **REFERENCES**

AICPA. (2009, July). The Evolution of the CFF Credential. *The Practicing CPA- The Newsletter of the AICPA Private Companies Practice Section*, 1-8.

Albrecht, W. S., Albrecht, C. C., Albrecht, C., & Zimbelman, M. F. (2011). *Fraud Examination* (3rd ed.). Cengage Learning.

Bell, S. (2008). *Encyclopedia of Forensic Science* (Revised Ed.). Facts on File Inc.

- Bhasin, M. L. (2016). Forensic Accounting in Asia: Perspectives and Prospects. *International Journal of Management and Social Sciences Research*, 5(7), 25–38.
- Birincioğlu, İ. (2005). Adli Belge İncelemesinin Tarihçesi, Yazının Anatomisi - Nöro- Fizyolojisi. İstanbul: Adli Belge İncelemesi Ed. Faruk Aşıcioğlu, Beta Yay.
- Bolton, R. J., Hand, D. J., Provost, F., Breiman, L., Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review. *Statistical Science*, 17(3), 235–255. doi:10.1214s/1042727940
- Boys, J. (2008). Forensic Accounting in New Zealand: Exploring the Gap Between Education and Practice. *AFAANZ Conference*.
- Casey, E., & Rose, C. W. (2003). Forensic Analysis. In E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology* (2nd ed.). Academic Press.
- Casey, E., & Seglem, K. (2003). Introduction. In E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology* (2nd ed.). Academic Press. doi:10.4324/9780203359105-6
- Cendrowski, H., Martin, J., & Petro, L. W. (2007). *The Handbook of Fraud Deterrence*. John Wiley & Sons.
- Chukwunedu, O. S., & Okoye, E. I. (2011). Forensic Accounting and Audit Expectation Gap – The Perception of Accounting Academics. *SSRN Working Papers*. doi:10.2139srn.1920865
- Clark, F., & Diliberto, K. (1996). *Investigating Computer Crime*. CRC Press. doi:10.1201/9781420048896
- Colbert, J. L., & Turner, B. S. (2000). Strategies for Dealing with Fraud. *The Journal of Corporate Accounting*, 11(4), 43–49. doi:10.1002/1097-0053(200005/06)11:4<43::AID-JCAF7>3.0.CO;2-Z
- Crumbley, D. L., & Apostolou, N. G. (2002). Forensic Accounting: A New Growth Area in Accounting. *The Ohio CPA Journal*, 61(3), 16–20.
- Crumbley, L. (2001). Forensic Accounting: Older Than You Think. *Journal of Forensic Accounting*, 2(2), 181–202.
- D'ath, J. (2008). Forensic Accounting Is Here to Stay. *Chartered Accountants Journal*, 87(3), 12–14.
- Dee, C. C., & Durtschi, C. (2010). Return of the Tallahassee BeanCounters: A Case in Forensic Accounting. *Issues in Accounting Education*, 25(2), 279–321. doi:10.2308/iace.2010.25.2.279
- DiGabriele, J. A. (2009). Implications of Regulatory Prescriptions and Audit Standards on The Evolution of Forensic Accounting in The Audit Process. *Journal of Applied Accounting Research*, 10(2), 109–121. doi:10.1108/09675420910984673
- DiNapoli, T. P. (2010). *Red Flags for Fraud*. State of New York Office of the State Comptroller.
- Dzamba, A. (2004). 36 Red Flags to Look for When Reviewing Financial Reporting Controls. *Financial Analysis. Planning & Reporting*, 4(8), 1–12.
- Elias, A. I. (2014). The Use of Forensic in Fraud Detection and Control. *International Journal of Research in Management*, 4(5), 61–71.

- Gray, D. (2008). Forensic Accounting and Auditing: Compared and Contrasted to Traditional Accounting and Auditing. *American Journal of Business Education*, 1(2), 115–126. doi:10.19030/ajbe.v1i2.4630
- Grippio, F. J., & Ibex, J. W. T. (2003). *Introduction to Forensic Accounting*. National Public Accountant.
- Gunasegaran, M., Quaddus, M., & Evans, R. (2010). Behavioral Intention to Use Forensic Accounting Services: A Critical Review of Theories and an Integrative Model. *Business Review (Federal Reserve Bank of Philadelphia)*, 15, 42–48.
- Güredin, E. (2007). *Denetim ve Güvence Hizmetleri: SMMM ve YMM'lere Yönelik İlkeler ve Teknikler*. İstanbul: 11. Baskı, Arıkan Yay.
- Hao, X. (2010). Analysis of the Necessity to Develop the Forensic Accounting in China. *International Journal of Business and Management*, 5(5), 185–187. doi:10.5539/ijbm.v5n5p185
- Harris, C. K., & Brown, A. M. (2000). The Qualities of a Forensic Accountant. *Pennsylvania CPA Journal*, 71(1), 2–3.
- Hopwood, W. S., Leiner, J. J., & Young, G. R. (2008). *Forensic Accounting*. McGraw Hill/Irwin.
- Houck, M. M., Kranacher, M. J., Morris, B., Riley, R. A., Robeitonson, J. J., & Wells, J. T. (2006). Forensic Accounting as an Investigative Tool: Developing a Model Curriculum for Fraud and Forensic Accounting. *The CPA Journal*, 76(8), 68–70.
- Kasum, A. S. (2009). The Relevance of Forensic Accounting to Financial Crimes in Private and Public Sectors of Third World Economies: A Study from Nigeria. *The 1st International Conference on Governance Fraud Ethics and Social Responsibility*, 1-12.
- Kaya, U. (2005). Muhasebe Mesleğinde Adli Muhasebe Uzmanlığı ve Türkiye Açısından Gerekliliği. *Muhasebe Bilim Dünyası Dergisi*, 7(1), 49–64.
- Kenyon, W., & Tilton, P. D. (2006). Potential Red Flags and Fraud Detection Techniques. In *A Guide to Forensic Accounting Investigation*. John Wiley & Sons.
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Malinowski, C. (2005). The Digital Investigative Unit: Staffing. In A. Thomas (Ed.), *Training, and Issues, Forensic Computer Crime Investigation*. CRC Press. doi:10.1201/9781420028379.ch2
- Manning, G. A. (2005). *Financial Investigation and Forensic Accounting*. Taylor and Francis.
- Markman, M. S., Bucrek, J. E., Levko, A., Lechner, S. P., Haller, M. W., Dennis, R. W., Clayton, M. M., Dineen, J. C., & Schaffer, G. (2006). Other Dimensions of Forensic Accounting. In *A Guide to Forensic Accounting Investigation*. John Wiley & Sons.
- Minniti, R. K. (2011). *Introduction to Forensic Accounting*. Retrieved from <http://www.imavalleyofthesun.org>
- Mohd, S. I., & Mazni, A. (2007). An Overview of Forensic Accounting in Malaysia. *International Conference on Business and Information*.

- Okoye, E., & Ndah, E. N. (2019). Forensic Accounting and Fraud Prevention in Manufacturing Companies in Nigeria. *International Journal of Innovative Finance and Economics Research*, 7(1), 107–116.
- Okunbor, J. A., & Obaretin, O. (2010). Effectiveness of the Application of Forensic Accounting Services in Nigerian Corporate Organisations. *AAU Journal of Management Sciences*, 1(1), 171–184.
- Özbek, Ç. (2003). İç Denetimde Yeni Uygulamalar. 7. *Türkiye İç Denetim Sempozyumu*.
- Özkul, F. U., & Pektekin, P. (2009). Muhasebe Yolsuzluklarını Tespitinde Adli Muhasebecinin Rolü ve Veri Madenciliği Tekniklerinin Kullanılması. *Muhasebe ve Bilim Dünyası Dergisi*, 11(4), 57–87.
- Pamungkas, I. D., Ghazali, I., & Achmad, T. (2018). A pilot Study of Corporate Governance and Accounting Fraud: The fraud Diamond Model. *The Journal of Business and Retail Management Research*, 12(2), 253–261. doi:10.24052/JBRMR/V12IS02/APSOCGAAFTFDM
- Paranjape, M., & Sheeth, R. (2011). A study of creative accounting and forensic accounting as inter-linked trends in accounting. *International Journal For Business. Strategy and Management*, 1(1), 1–8.
- Rafay, A. (Ed.). (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Ramaswamy, V. (2005). Corporate Governance and the Forensic Accountant. *The CPA Journal*, 70(3), 68–70.
- Ramos, M. (2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 95(1), 28–36.
- Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.
- Ranallo, L. F. (2006). *Forensic Investigations and Financial Audits: Compare and Contrast. In A Guide to Forensic Accounting Investigation*. John Wiley & Sons.
- Reinstein, A., & McMillan, J. J. (2004). The Enron Debacle: More Than A Perfect Storm. *Critical Perspectives on Accounting*, 15(6-7), 955–970. doi:10.1016/j.cpa.2003.08.006
- Rezaee, Z., & Lander, G. H. (1996). Integrating Forensic Accounting into the Accounting Curriculum. *Accounting Education*, 1(2), 147–163.
- Rezaee, Z., Lander, G. H., & Reinstein, A. (1992, August 20–25). Forensic Accounting: Challenges and Opportunities. *The Ohio CPA Journal*.
- Rezaee, Z., & Wang, J. (2019). Relevance of Big Data to Forensic Accounting Practice and Education. *Managerial Auditing Journal*, 34(3), 268–288. doi:10.1108/MAJ-08-2017-1633
- Seddon, A. E., & Pass, A. D. (2009). *Forensic Sciences*. Salem Press.
- Seetharaman, A., Senthilvelmurugan, M., & Periyannayagam, R. (2004). Anatomy of Computer Accounting Frauds. *Managerial Auditing Journal*, 19(8), 1055–1072. doi:10.1108/02686900410557953

### ***Forensic Audit Practices to Reduce Financial Frauds***

Sennewald, C. A., & Tsukayama, J. K. (2006). *The Process of Investigation: Concepts and Strategies for Investigators in the Private Sector*. Butterworth-Heinemann Press.

Singleton, T. W., Bologna, G. J., Lindquist, R. J., & Singleton, A. J. (2006). *Fraud Auditing and Forensic Accounting*. Wiley.

Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing and Forensic Accounting* (4th ed.). John Wiley & Sons. doi:10.1002/9781118269183

Wadhwa, L., & Pal, V. (2012). Forensic Accounting and Fraud Examination in India. *International Journal of Applied Engineering Research: IJAER*, 7(11), 1–4.

Watters, M., Casey, K. M., Humphrey, J., & Linn, G. (2007). CPA Firms Offering of Forensic Services Surprisingly Consistent Over Time: Are CPA's Missing Out on A Forensic Accounting Gold Rush. *Academy of Accounting and Financial Studies Journal*, 11(2), 89–95.

Wilks, T. J., & Zimbelman, M. F. (2002). The Effects of a Fraud-Triangle Decomposition of Fraud Risk Assessments on Auditors' Sensitivity to Incentive and Opportunity Cues. *Proceedings of the 15th University of Illinois Symposium on Auditing Research*.

Yildirim, Y., & Rafay, A. (2021). Anti-Money Laundering in Insurance Sector: The Turkish Case. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Zimbelman, M. F., & Albrecht, C. C. (2012). *Forensic Accounting* (4th ed.). South Western Cengage Learning.



## Chapter 13

# Forensic Audit for Financial Frauds in Banks: The Case of Bangladesh

Md. Nur Alam Siddik

 <https://orcid.org/0000-0001-8406-3903>

Begum Rokeya University, Rangpur, Bangladesh

### ABSTRACT

*Traditional auditing has failed to control the jeopardy of increased financial frauds. Gradually, forensic auditing has been employed by organizations to control such frauds. Nonetheless, there is a dearth of studies examining the effects of forensic auditing on financial frauds. In particular, the impact of forensic auditing on financial frauds in Bangladesh is not examined. This study attempts to fill this gap. Using survey data of 182 respondents, this study applied logistic regression analysis. Findings indicate that forensic auditing has significant positive effects on the detection and prevention of financial fraud occurrences in the banking sector of Bangladesh. Findings also indicate that forensic auditing is competent to diminish financial frauds. Therefore, it is recommended to adopt forensic auditing in the banking sector of Bangladesh.*

### INTRODUCTION

Increased scenario of fraudulent practices in organizations and government agencies across the world have brought the forensic auditing to the limelight. Well known examples of frauds in the corporate world are Enron, Arthur Anderson and WorldCom. Tackling frauds is a complex task because of the varieties of frauds, committers, and the way of perpetration and conventional auditing has become futile in its preemptive role in this purpose. Generally, a conventional auditor is not liable for fraud identification, prevention, and reduction, except when placed on inquiry (Ramzan, *et al.*, 2020) In other words, the scope of work of a conventional auditor is primarily limited. This means that diverse methods of tackling frauds are needed by taking into consideration the types of frauds, committers, the mode of

DOI: 10.4018/978-1-7998-5567-5.ch013

perpetration, and the duties of external auditors as enshrined in the governing laws. In response to these, forensic auditing came to the fore.

Forensic auditing is seeming to have developed in answer to particular emerging fraud allied circumstances and the growing intricacy of financial fraud necessitates that forensic auditing should be applied and added to the tools required to carry the efficacious enquiry and trial of those persons or groups engaged in illicit activities (Nwosu, 2015). Deb (2018) described forensic audit as the use of financial expertise and inspective ability surrounded by the perspective of rule of evidence to inspect unsettled disputes. Forensic audit is seen as summarizing and acclimatizing inspective auditing, criminology, lawsuit services, and financial talents to detection of fraud. According to Izedomin and Mgbame (2011), a forensic auditor is one who, in addition to conveying a factual and unbiased opinion on the company's financial statements, goes beyond the scheduled audit to do a colossal enquiry into the facts in question, cultivates spontaneous intents and is eager to enquire query with the purpose of excavation deep into the examination imminent. Therefore, a forensic auditor is clinched to be one who owns expertise in financial inquiry procedures in order to disentangle fraud committed earlier.

Presently the outsized number of financial frauds in the corporate world of Bangladesh has become a great concern to the country (Alam *et al.* 2021). One after another, financial frauds at vast scales are taking place in the country beginning from stock market crash twice in 1996 and again in 2010, institutional frauds like Hallmark, Bismillah Group, and a good number gigantic scandals exposed in bank sector such as BASIC bank, Janata bank, Agrani bank, Sonali Bank etc.<sup>1</sup>. The incapacity of the law execution agents to magnificently track down committers of fraud has made it bothersome. Forensic audit may be one of the most effective and capable way to identify, lessen and inhibit such financial frauds. Thus, though new in Bangladesh till today, organizations and policymakers have recognized the urgent and utmost need for the forensic auditing to tackle and reduce fraudulent financial practices. Present research aims to observe the effects of forensic auditing on reducing financial frauds cases in banks operating in developing economies like Bangladesh.

## **Objectives of the Study**

The main objective of the present scholarship is to inspect whether forensic audit practice can reduce financial frauds, while the particular objectives of the study are as follows:

1. Determine the effect of forensic audit on financial fraud detection.
2. Ascertain the effect of forensic audit on financial fraud prevention
3. Find out whether forensic audit can reduce financial fraud.

## **Research Hypotheses**

The following hypotheses are articulated to test our model:

$H_{01}$ : Forensic audit have no effect on financial fraud detection

$H_{02}$ : Forensic audit have no effect on financial fraud prevention

$H_{03}$ : Forensic audit have no effect on financial fraud reduction

## **Significance of the Study**

With outcomes of the present study, the regulatory authority may commend the affirmative role of forensic auditing and practice of forensic audit evidence in the resolution of alleged criminals in law court cases. Foreign and domestic investors might not only feel contented to increase the number of investments but also sustain their existing investments in Bangladeshi banks. With the assertion that fraudulent events might be detected earlier, given stable political condition and effective and fair juridical system, stakeholders may start learning to trust the system. This research adds to the body of existing knowledge on the issue of forensic auditing and its effects on financial frauds which will help other scholars and practitioners to diagnosis the issue. Banks' management would be able to understand and identify the most vulnerable areas to fraud, detect them in advance and accordingly undertake some measures to lessen the chance of financial frauds occurring.

## **BACKGROUND**

### **Concept of Forensic Audit**

Forensic auditing is a process which consists of collecting, authenticating, handling, investigating of, and reporting on data so as to get realities and proof in a pre-specified setting in the issues of legal, financial disputes, and recommending preemptive guidance. The prime goal of forensic auditing is detection of frauds, contrasting the old-fashioned auditing that efforts on examination of internal control method, miscalculation detection and preclusion (Khan, *et al.*, 2020; Albrecht *et al.*, 2001).

Forensic auditing often described as a specific and specialized arena of accounting that deals with the outcome from authentic or foreseen disputes or court case. Silverstone and Sheetz (2007) explained that forensic auditing is a method of construing, reviewing and offering multifaceted financial concerns evidently, concisely and factually every so often in a law court as a professional. According to Peter *et al.* (2014) forensic auditors are proficient auditors, accountants, and detectives of permissible and financial papers and appointed to examine probable doubt of fraudulent doings within an organization; or are appointed by an organization who may just think to avert deceitful doings from happening. Nwosu (2015) stated forensic auditing as tripartite exercise of employing accounting, auditing and inspective skills to support in lawful substances.

Eyisi and Ezuwore (2014) itemized the purposes of forensic auditing to comprise of but not restricted to: developing management accountability; expanding corporate governance and the legal audit task; advancing financial reporting method; assist in discovering financial fraud; support in firming up auditors impartiality; providing added promise for audit committees; supporting financial statement auditors to take more responsibility for fraud identification; giving the audit committees superior instruments to assess the excellence of the financial statement audit by the exterior auditor. The above objectives according to them could be said to have solider effects on corporate governance, since the forensic auditor is likely to go afar from traditional audit as to examine fraud and inspect deeper applying more classy scientific diagnostic tools and software packages to detect fraudulent activities.

## **Concept of Financial Fraud**

Financial fraud has been stated differently in different literatures, but no single definition is sufficient enough. Financial frauds vary widely among organizations based on nature, character and operational procedures in general. Salehi and Azary (2008) described fraud as the planned falsification, camouflage or oversight of the actual fact for the aim to cheating or manipulation to the financial loss of a person or an institution as for example a bank, which contains fund embezzlement, burglary or any effort to steal or illegitimately acquire or abuse of asset. Nwaeze (2008) stated that fraud is an act of illegal doing which perpetrated in various arrangements and typically insiders from the institution and outsiders join together to effectively execute the act. Looking from a global perspective, Okoye and Gbegi (2013) argued that fraud is a global delinquent, and no country is insusceptible though developing countries are the most suffer. From a legitimate standpoint, fraud itself is a generic term which holds diverse meaning, which human inventiveness can invent, that are routed to by one individual or a group of individuals to get an advantage over another individual or a group of individuals by false deceptions.

Different scholars classified frauds differently on different dimension. Singleton *et al.* (2006) classified fraud according to occupational and non-occupational events, while Othman *et al.* (2015) views fraud a deceitful event occurred in public or private sector. Lendemen (2003) grouped fraud as corporate or non-corporate frauds, such as management fraud, insider dealing, and investment frauds. Skalak *et al.* (2012) provided an important category of fraud based on the industry in which the fraud committed. According to the authors bank fraud refers to any acts planned to complete or completed with the intention to deceiving a financial institution. As for example, if the fraud was committed in banking industry it is a bank fraud which typically is financial fraud (Gupta and Biswas, 2021). Among the frauds occurred in banks some of which are noteworthy to mention: cad traders, deceitful loans, fake papers, mugging of identity, fake and changed cheques, filched cheques, debit or credit card fraud, promoter cheque duplication and scanning of card information, illicit financing, money laundering (Rafay, 2021). Present study endeavors to observe the influences of forensic audit on financial frauds of banking industry as such we define financial frauds as any financial fraud occurred in banks.

## **LITERATURE REVIEW**

### **Theoretical Underpinnings**

Among many theories of fraud detection, prevention and reduction, this research is moored on some useful and practicable theories namely policeman theory, fraud triangle theory, fraud diamond theory and White-collar crime theory. These theories are discussed as follows:

*The Policeman theory:* The Policeman theory postulates that the forensic auditor is a policeman whose primary duty is to detect and prevent frauds so as to diminish the total cases of reported incidences corporate frauds (Hayes *et al.*, 2014). In other words, this theory asserts that the forensic auditor is liable for examining, ascertaining and preventing fraud.

*Fraud Triangle Theory:* The Fraud Triangle theory is initiated upon the proposition which (Cressey, 1953) states that certainly some factors are responsible for any fraud to occur and these factors craft an enhancing environment for such occurrence of fraudulent doings and these certain factors are pressure, opportunity and rationalization which structure the triangle. Cressey (1953) further argued that when

trust violators consider themselves as having a financial difficulty which he or she cannot share with others and has understanding or mindfulness that such difficulty can be clandestinely solved by defilement of the situation of financial faith. In addition, they are intelligent to relate to their individual manner in that articulations which allow them to modify their outsets as reliable personnel with their outsets of themselves as handlers of the assigned funds or assets.

*The Fraud Diamond Theory (FDT):* FDT was proposed by Wolfe and Hermanson in 2004 as an extension of the fraud triangle theory. Wolfe and Hermanson (2004) presented the fraud diamond theory where they added fourth factor ‘capability’ to the three-element theory of ‘fraud triangle’ of pressure, opportunity and rationalization. This theory considers that the existence of pressure, opportunity and rationalization alone is not sufficient to occur fraud except the person or personnel has the capability to commit that fraud. Capacity is defined as the possession of pertinent qualities or abilities and capability to turn such chance to a realm. Therefore, capacity means knowing of the internal control system and its gaps that could be abused in preparation and execution of the fraudulent activity. Wolf and Hermanson (2004) assumed that many frauds will not happen without the right person with right capabilities carry out the whole process of a fraudulent activity. Authors observed and identified four observation traits for committing fraud as: (i) commanding rank in the institution; (ii) capacity to recognize and feat the accounting and internal control systems of the institution; (iii) sureness that no one would be able to identify them, or if alleged, they will be able to get out of it smoothly and easily; and (iv) competency to cope with the strain generated within and otherwise be a moral being when he or she commits fraudulent activities. Handoko and Selly (2020) applied factors of fraud diamond in detection of financial frauds and found effective.

With the added component offered in the fraud diamond theory influencing persons’ choice to involve in fraud, the institutions and auditors require to know well personnel’ characters and skills in order to evaluate the jeopardy of fraud activities. Furthermore, modern and updated security systems for checks should be affected and supervised to preemptively reduce risks and losses resultant from fraudulent happenings in the workstation. It is, therefore, valid to note that for the capability of those who engaged in fraudulent activities to be detected and prevented, the necessity for skillful, trained and knowledgeable specialists like the forensic auditor becomes sacrosanct.

*White collar crime theory:* Attributed to Ross (1907) who first developed the notion of white-collar offenses and came up with the term ‘criminaloid’ to denote to the individual who offends in society but does not fit the depiction of the usual offender. Further developed by Sutherland (1945), this theory postulates that white collar offenses are committed by an individual who holds a decent and high status in a particular profession, and they do it intentionally, very carefully and in a well-planned way. These white-collar offenders do not consider themselves as law breakers. White collar crimes comprise of but not limited to bribery, embezzlement, money laundering, and cybercrime. Therefore, owing to the rank or position of those who involved in these atrocities, a skilled and proficient sleuth such as the forensic auditor is highly recommended to anticipate the happening of such frauds.

## **Existing Empirical Studies**

Ogiriki and Appah (2018) empirically studied the impacts of forensic accounting and auditing practices on fraud detection, examination and inhibition. Using survey data conducted in Nigeria, authors found that forensic auditing significantly helps in fraud detection, investigation and prevention. Alao (2016) inspected the effect of forensic auditing on financial frauds. The study adopted a purposive sampling

technique and administered a structured questionnaire. Author conducted logistic regressions and found that forensic audit has substantial influence on financial fraud control and that forensic audit report considerably improves court settlement on financial frauds in Nigeria. Modugu and Anyaduba (2013) observed a significant affirmative connection of forensic accounting with fraud reduction.

Njanike *et al.* (2009) studied the efficacy of forensic auditing in identifying, probing, and inhibiting frauds occurred in banks operating in Zimbabwe. The survey study applied structured questionnaires, individual interviews, and documented review methods to get data from multi-occupational respondents including banks and audit firms. Authors found that forensic auditing undergo many challenges, among them the deficiency of material means, technical expertise, intervention from managerial body, and imprecise appreciation of the profession. Based on findings, authors argued that the forensic auditors must be equipped significantly and officially to increase their efficiency and thus suggested that the forensic auditors should form an organized body that works for their welfare and standardize the actions just like any other line of work.

Bassey (2018) studied the influence of forensic accounting on the fraud managing system in microfinance institutions. Based on survey data the study conducted ordinary least square method for analysis. Findings indicate noteworthy negative impacts of forensic accounting on frauds. In other words, it was found that active commitment of forensic examination and lawsuit provision lessens fraud in sample microfinance banks. The study urged that micro finance banks should adopt more and rigorous forensic accounting systems for observing and inspecting alleged wrongdoers in fraud cases. In another study, Abdulrahman (2019) examined application of forensic accounting on Nigerian public sector and found that forensic accounting was able to detect and prevent frauds. Using 50 respondents' response, Okoye and Ndah (2019) found that practice of forensic accounting in manufacturing companies is significantly positively related with fraud detection and prevention.

Bressler (2012) studied the awareness of attorney and judges in the law court as to what might augment understanding of the significance of forensic accountants in fraud enquiry. Employing conceptual study author found argued that forensic accountants plays a vital role in detecting frauds and as such should be given more proper training on rules of evidence, accounting information system, examination of financial data, on modern updated software and communication skills.

In the context of an emerging economy, namely Brazil, Imoniana *et al.* (2013) attempted to analyze the features of forensic accounting amenities executed by accounting companies. Authors applied an experimental method to achieve their aims. Findings indicate that forensic auditors detect more frauds compared to traditional auditing and thus concluded that forensic audit should be adopted. In the context of Bangladesh, Islam *et al.* (2011) explained the growing status of forensic accounting as an encounter against exploitation, identification and preclusion of fraud in Bangladesh. Using 100 respondent's response, authors just stated the need for forensic accounting in Bangladesh but have not investigated the relationship between the issues which is an important research gap identified in this study.

Based on the literatures discussed above, it is evident that forensic auditing seems to be an efficient method to detect, prevent and reduce financial frauds. Nonetheless, studies on the nexus between forensic auditing and financial frauds is scarce. Particularly in the context of Bangladesh, no empirical studies focusing on the issue have been found. Therefore, this research aims to fill this research gap. This study attempts to scan the effects of forensic auditing on reducing financial frauds in banks operating in developing economies like Bangladesh. The contributions of this study are two-fold: first, it provides an important framework to the existing knowledge on the issue of forensic auditing and reduction of financial frauds. Second, it empirically explores and establish the association between forensic auditing

and financial frauds in the context of a developing economy, namely Bangladesh and thus extends an avenue for other developing nations to explore and adopt forensic auditing method.

## **METHODOLOGY OF THE STUDY**

To investigate whether forensic audit can reduce financial frauds in banks, a survey was conducted by means of structured questionnaire during September-November 2019. In order to confirm content validity, the survey instrument, questionnaire, was prepared and modified from prior related studies. Purposive sampling technique was applied to choose the sample. The questionnaires were distributed to a total of 200 prospective respondents, who are staffs and executives working at different scheduled banks operating in Bangladesh, out of which 182 responded (91% response rate). We employed logistic regression technique to observe the effects of forensic audit on financial frauds. We considered application of logistic regression model as significant for this scholarship because all dependent and independent variables are qualitative in nature and are able to be stated in binary form. In order to accomplish the objectives of the study replies of the respondents were coded in binary form; thus, it takes 1 for agreed while it takes 0 for disagreed opinion.

### **Operationalization of the Variables**

For estimation purpose, the logistic regression model is given as;

$$L_i = \text{Log} \frac{p_i}{1 - p_i} = Y_i \quad (1)$$

Where

$$Y_i = \beta_0 + \beta_1 X_i + \varepsilon_i \quad (2)$$

So, the logistic regression model for above mentioned three hypotheses are as follows:

For 1<sup>st</sup> hypothesis: Forensic audit have no effect on financial fraud detection:

$$Y = \beta_0 + \beta_1 X_1 + \varepsilon \quad (3)$$

$$FFD = \beta_0 + \beta_1 FA + \varepsilon \quad (4)$$

Where *FFD* represents the financial fraud detection which is the dependent variable for the 1st hypothesis. *FA* indicates the independent variable, which is forensic auditing.  $\beta_0$  is the intercept and  $\beta_1$  is slope of the regression.  $\varepsilon$  is the error term. For this hypothesis, respondents were asked to give their opinion

(agree or disagree) as follows: 'Forensic auditing can be used to detect financial frauds in Bangladeshi commercial banks'.

For 2<sup>nd</sup> hypothesis: Forensic audit have no effect on financial fraud prevention:

$$FFP = \beta_0 + \beta_1 FA + \varepsilon \quad (5)$$

Where *FFP* represents the financial fraud prevention which is the dependent variable for the 2<sup>nd</sup> hypothesis. *FA* indicates the independent variable, which is forensic auditing.  $\beta_0$  is the intercept and  $\beta_1$  is slope of the regression.  $\varepsilon$  is the error term. For this hypothesis, respondents were asked to give their opinion (agree or disagree) as follows: 'Forensic auditing can be used to prevent financial frauds in Bangladeshi commercial banks'.

For 3<sup>rd</sup> hypothesis: Forensic audit have no effect on financial fraud reduction:

$$FFR = \beta_0 + \beta_1 FA + \varepsilon \quad (6)$$

Where *FFR* represents the financial fraud reduction which is the dependent variable for the 3<sup>rd</sup> hypothesis. *FA* indicates the independent variable, which is forensic auditing.  $\beta_0$  is the intercept and  $\beta_1$  is slope of the regression.  $\varepsilon$  is the error term. For this hypothesis, respondents were asked to give their opinion (agree or disagree) as follows: 'Forensic auditing can be used to reduce financial frauds in Bangladeshi commercial banks'.

In addition to the questions mentioned above, respondents were also asked to give their opinion on the corporate governance level, presence of external auditing, participation on Basel accord in their respective banks and thus included in our analysis. Abri *et al.* (2019) found positive effects of corporate governance on fraud controls. As such we expect positive role of corporate governance in detection, prevention and reduction of financial frauds. Dimitrijevic *et al.* (2020) found that external auditors work scope is very much narrowed with many limitations and as such they are not able to significantly control frauds in companies. Sharma (2008) argued and described that maintaining Basel accords reduce fraudulent activities in banks.

## **A Priori Expectation**

1<sup>st</sup> hypothesis: Forensic audit have no effect on financial fraud detection

For the 1<sup>st</sup> hypothesis, we expect that  $\beta_0, \beta_1$  would be greater than zero (0) which means that as the more the activities of forensic audit the more the detection of financial fraud is. Hence, there is an affirmative association of forensic audit with financial fraud detection.

2<sup>nd</sup> hypothesis: Forensic audit have no effect on financial fraud prevention

For the 2<sup>nd</sup> hypothesis, we expect  $\beta_0, \beta_1$  would be greater than zero (0) which means that the more the implementation of forensic audit the more the prevention of financial fraud is. Hence, there is an affirmative association of forensic audit with prevention of financial fraud.



3<sup>rd</sup> hypothesis: Forensic audit have no effect on financial fraud reduction

For the 3<sup>rd</sup> hypothesis, we expect a positive effect of forensic audit on financial fraud. Thus, the more the adoption of forensic auditing, the more the financial frauds reduction.

## **FINDINGS AND DISCUSSION**

### **Reliability Analysis**

The research instrument was evaluated for its reliability. We employed Cronbach's alpha to measure the reliability co-efficient. We found Cronbach's alpha value of 0.69. Results indicate that instrument is acceptable and reliable as suggested by suggested by DeVillis (1991). Thus, it means that the questionnaire designed for the research work is a good instrument to achieve the objectives.

### **Regression Results**

Results of three separate logistic regressions are shown in Table 1. In case of the first model, column 2 to column 4, where dependent variable is *FFD*, we found that forensic auditing, *FA*, has significant positive effects on detection of financial frauds. The model's pseudo  $R^2$  explained from 17.9% to 22.1% of the variation in financial fraud detection. Our estimated model confirmed the priori expectation of an affirmative rapport between the use of forensic audit and financial fraud detection. This is shown by the positive value (0.512) of the coefficient of forensic audit. The inference is that forensic audit has significant positive impacts on fraud detection; therefore, the more forensic audit is employed, the more the financial frauds would be detected. Thus, we reject the null hypothesis that forensic auditing has no effects on financial frauds detection. Our estimated results are consistent with the findings of (Alao, 2016; Enofe *et al.*, 2015; Inyada *et al.*, 2019).

In case of the second model, where dependent variable is *FFP*, results are presented in column 5 to column 7 of Table 1. In this case, consistent with the results of (Alao, 2016; Bassey, 2018; Enofe *et al.*, 2015; Inyada *et al.*, 2019), we observed that forensic auditing, *FA*, has significant positive impacts on prevention of financial frauds, *FFP*. The model's pseudo  $R^2$  explained from 13.8% to 19.7% of the variation in financial fraud prevention. Our estimated model confirmed the priori expectation of a positive link between the practice of forensic audit and financial fraud prevention. This is revealed by the affirmative value (0.652) of the coefficient of forensic audit. The inference is that forensic audit has positive influence on fraud prevention; therefore, the more forensic audit is engaged, the higher the level of prevention of financial frauds would be. Thus, we reject the null hypothesis that forensic auditing has no effects on financial frauds prevention.

Findings of the third model, where dependent variable is *FFR*, are exhibited from column 8 to column 10 in Table 1. In this case, we observed that forensic auditing, *FA*, has significant positive impacts on financial frauds, *FFR* which is similar to the results of (Enofe *et al.*, 2015). The model's pseudo  $R^2$  explained from 15.6% to 24.8% of the variation in financial fraud reduction. Our estimated model confirmed the priori expectation of a positive link between the use of forensic audit and financial fraud reduction. This is revealed by the positive value (0.822) of the coefficient of forensic audit. The inference is that forensic audit has positive influence on reduction of financial fraud; therefore, the more forensic

*Table 1. Logistic regression results*

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Variable	FFD			FFP			FFR		
	Coeff.	S.E	Sig.	Coeff.	S.E	Sig.	Coeff.	S.E	Sig.
<i>FA_FFD</i>	0.512	1.012	0.047**						
<i>FA_FFP</i>				0.652	0.813	0.007***			
<i>FA_FFR</i>							0.822	0.735	0.000***
<i>CG</i>	0.302	0.801	0.069*	0.413	0.783	0.035**	0.305	0.815	0.084*
<i>EA</i>	0.111	0.880	0.096*	0.011	0.986	0.145	0.002	0.964	0.178
<i>BA</i>	0.420	0.758	0.087*	0.398	0.753	0.048**	0.358	0.832	0.045**
-2 Log likelihood	68.158			65.593			70.585		
Cox & Snell <i>R</i> <sup>2</sup>	0.179			0.138			0.156		
Nagelkerke <i>R</i> <sup>2</sup>	0.221			0.197			0.248		

Source: Author's calculation.

Note: *CG* refers level of corporate governance, *EA* refers presence of external auditing and *BA* refers participation on Basel accord. \*\*\*, \*\*, \* denotes variable significant at 1%, 5% and 10% respectively.

audit is applied, the more the level of reduction of financial frauds would be. In other words, forensic auditing significantly reduces financial frauds in banks. Thus, we reject the null hypothesis that forensic auditing has no effects on financial frauds reduction.

We found that level of corporate governance, *CG*, plays significant positive role in detection, prevention and reduction of financial frauds which is similar to the findings of (Abri *et al.*, 2019; In'airat, 2015). Another finding is that external auditor, *EA*, can play affirmative role in detecting financial frauds though no significant impacts have been found on prevention and reduction of financial frauds. This is because of limited scope of work. Our findings are similar to the findings of (Dimitrijevic *et al.*, 2020). Consistent with the findings (Kiehlborn, 2007; Sharma, 2008) of we also found that practicing and maintaining Basel accords, *BA*, plays significant positive role in detection, prevention and reduction of financial frauds in Banks.

Based on the estimated results with logistic regression analysis and their discussion above, we conclude that forensic audit helps in financial fraud detection, prevention and reduction. In other words, increase in forensic audit services will detect occurrence of the financial frauds in advance and thus able to reduce financial frauds.

## CONCLUSION

The significance of forensic auditing cannot be undervalued because of global stubborn execution of fraud in organizations especially banks operating in developing economies. The continued failures of traditional auditing over eras have provoked a paradigm shift in auditing and accounting. This certainly has made scholars and management of organizations including banks to explore other methods of deal with and decreasing the threat of frauds. This study investigated the effects of forensic auditing on detec-

tion, prevention and reduction of financial frauds in the banking sector of Bangladesh. Using survey data, this study conducted logistic regression analysis to meet the objectives. The study reveals that forensic auditing can detect, prevent and reduce financial frauds. Thus, we conclude that forensic auditing plays a significant role in fraud detection, prevention and reduction of financial frauds and accordingly we recommend that banks in Bangladesh can use forensic auditing service in order to control the financial frauds that will help to avoid unexpected losses. Since the forensic auditing is still at infancy stage in Bangladesh, policymakers can create enabling environment to foster forensic auditing by introducing forensic auditing education and training programs at tertiary level of education which will in turn promote to produce more forensic auditors in Bangladesh.

## **FUTURE RESEARCH DIRECTIONS**

This study adds to the existing knowledge of literatures on the impacts of forensic auditing on detection, prevention and reduction of financial fraud cases in banks operating in Bangladesh. The study however gives room for further research, upon availability of data, especially from viewpoint of court adjudication, losses from financial frauds and from regulatory perspective so that organizations become motivated to adopt forensic auditing their organizations.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in his personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and fine-tuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## **REFERENCES**

Abdulrahman, S. (2019). Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper. *International Journal of Accounting & Finance Review*, 4(2), 13- 21.

- Abri, A.F., Arumugam, D., & Balasingam, S. (2019) Impact of the corporate governance on the financial statement fraud: A study focused on companies in Tanzania. *International Journal of Recent Technology and Engineering*, 7(5s), 336– 341.
- Alam, M. D., Tabash, M. I., Hassan, M. F., Hossain, N., & Javed, A. (2021). *Shariah Governance Systems of Islamic Banks in Bangladesh: A Comparison with Global Governance Practices*. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research*, 4(8), 1– 19.
- Albrecht, C. C., Albrecht, W. S., & Dunn, J. G. (2001). Can auditors detect fraud: A review of the research evidence. *Journal of Forensic Accounting*, 2(1), 1– 12.
- Bassey, E. B. (2018). Effect of forensic accounting on the management of fraud in microfinance institutions in Cross River State. *Journal of Economics and Finance*, 9(4), 79– 8.
- Bressler, L. (2012). The role of forensic accountants in fraud investigations: Importance of Attorney and Judge's perceptions. *Journal of Finance and Accountancy*, 9, 1– 9.
- Cressey, D. R. (1953). *Other people's money; a study of the social psychology of embezzlement*. Free Press.
- Deb, R. (2018). Financial audit or forensic audit? Government sector panorama. *Indian Journal of Corporate Governance*, 11(2), 135– 158.
- DeVillis, R. F. (1991). *Scale development: Theory and applications*. Sage.
- Dimitrijevic, D., Jovkovic, B., & Milutinovic, S. (2020). (in press). The scope and limitations of external audit in detecting frauds in company's operations. *Journal of Financial Crime, ahead-of-print*(ahead-of-print). Advance online publication. doi:10.1108/JFC-11-2019-0155
- Enofe, A. O., Omagbon, P., & Ehigiator, F. I. (2015). Forensic audit and corporate fraud. *International Journal of Economics and Business Management*, 1(7), 1– 10.
- Eyisi, A. S., & Ezuwore, C. N. (2014). The impact of forensic auditors in corporate governance. *Research Journal of Finance and Accounting*, 5(8), 31– 39.
- Gupta, R. P., & Biswas, B. (2021). Banking Scams in India: A Case Based Analysis. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Handoko, B. L., & Selly (2020). The effect of fraud diamond on detection of financial statement fraud. *International Journal of Advanced Science and Technology*, 29(3), 467– 475.
- Hayes, R., Wallage, P., & Gortemaker, H. (2014). *Principles of auditing: an introduction to international standards on auditing*. Pearson.
- Imoniana, J. O., Antunes, M. T. P., & Formigoni, H. (2013). The forensic accounting and corporate fraud. *JISTEM-Journal of Information Systems and Technology Management*, 10(1), 119–144.
- In'airat, M. (2015). The role of corporate governance in fraud reduction-A perception study in the Saudi Arabia business environment. *Journal of Accounting & Finance*, 15(2), 119– 128.

- Inyada, S. J., Olopade, D. O., & John, U. (2019). Effect of forensic audit on bank fraud in Nigeria. *American International Journal of Contemporary Research*, 9(2), 40–45.
- Islam, M. J., Rahman, M. H., & Hossan, M. T. (2011). Forensic accounting as a tool for detecting fraud and corruption: An empirical study in Bangladesh. *ASA University Review*, 5(2), 77–85.
- Izedomin, F. I., & Mgbame, C. O. (2011). Curbing financial frauds in Nigeria, a case for forensic accounting. *African Journal of Humanities and Society*, 1(12), 52–56.
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Kiehlborn, T. (2007). Risk management-challenge and opportunity. *Management International Review*, 47(4), 621–624.
- Lendemen, R. (2003). *Implications for Investigations and Forensic Auditor*. Boston Beacon Press.
- Modugu, K. P., & Anyaduba, J. O. (2013). Forensic accounting and financial fraud in Nigeria: An empirical approach. *International Journal of Business and Social Science*, 4(7), 281–289.
- Njanike, K., Dube, T., & Mashayanye, E. (2009). The effectiveness of forensic auditing in detecting, investigating, and preventing bank frauds. *Journal of Sustainable Development in Africa*, 10(4), 405–425.
- Nwaeze, C. (2008). Quality and internal control challenges in contemporary Nigeria banking. *Zenith Economic Quarterly*, 3(2), 23–28.
- Nwosu, M.E., (2015). Forensic auditing and financial accounting in Nigeria: An assessment. *International Journal of Economics and Management Studies*, 2(7), 6–11.
- Ogiriki, T., & Appah, E. (2018). Forensic accounting & auditing techniques on public sector fraud in Nigeria. *International Journal of African and Asian Studies*, 47, 7–16.
- Okoye, E., & Ndah, E. N. (2019). Forensic accounting and fraud prevention in manufacturing companies in Nigeria. *International Journal of Innovative Finance and Economics Research*, 7(1), 107–116.
- Okoye, E. I., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and prevention in the public sector. (A study of selected ministries in Kogi state). *International Journal of Academic Research in Business and Social Sciences*, 3(3), 1–19.
- Othman, R., Aris, N. A., Mardziah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector: Accountants' and internal auditors' perceptions. *Procedia Economics and Finance*, 28, 59–67.
- Peter, Z., Masoyi, A. D., Ernest, E. I., & Gabriel, A. O. (2014). Application of forensic auditing in reducing fraud cases in Nigeria money deposit banks. *Global Journal of Management and Business Research*, 14(3), 14–22.
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

- Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.
- Ross, E. A. (1907). *Sin and society: An analysis of latter-day iniquity*. Houghton Mifflin.
- Salehi, M., & Azary, Z. (2008). Fraud detection and audit expectation gap: Empirical evidence from Iranian bankers. *International Journal of Business and Management*, 3(10), 65–77.
- Sharma, M. (2008). *Management of financial institutions: with emphasis on bank and risk management*. PHI Learning Pvt. Ltd.
- Silverstone, H., & Sheetz, M. (2007). *Forensic accounting and fraud investigation for Non-Experts*. John Wiley & Sons.
- Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2006). *Fraud auditing and forensic accounting*. John Wiley & Sons.
- Skalak, S. L., Alas, M. A., & Sellitto, G. (2012). Fraud: an introduction. In T. W. Golden, S. L. Skalak, M. M. Clayton, & J. S. Pill (Eds.), *A guide to forensic accounting investigation* (pp. 1–23). John Wiley & Sons.
- Sutherland, E. H. (1945). Is "white collar crime" crime? *American Sociological Review*, 10(2), 132–139.
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.

## ENDNOTE

- <sup>1</sup> <https://www.thefinancialexpress.com.bd/views/forensic-accounting-a-method-for-timely-flag-raising-1548256777>

# Chapter 14

## Determinants of Forensic Accounting: The Case of Northwestern States of Nigeria

**Sagir Lawal**

*Nigeria Police Academy, Nigeria*

**Junaidu Muhammad Kurawa**

*Bayero University, Nigeria*

**Kabir Tahir Hamid**

*Bayero University, Nigeria*

### ABSTRACT

*This study examined the political and environmental factors as determinants to apply forensic accounting in the North-Western states of Nigeria. The study utilized primary data through the administration of questionnaires. Partial least squares (PLS) path modeling (using smart PLS3 statistical software) was employed for the main analysis. The findings of the study indicated that both political and environmental factors are positively related to applying forensic accounting in these states. The study recommended that all political office holders and other government personnel should, even with the change of government, use their powers to ensure the right way to move forward and the continuity of state policies to apply forensic accounting. State governments should also provide an enabling environment for the applicability of forensic accounting through the provision of the required infrastructure to carry out the forensic services smoothly.*

### INTRODUCTION

Financial misconducts are universal problems to which no nation is excluded. Today modern organized financial misconducts, such as employee theft, payroll fraud, corporate and insurance fraud (Yildirim & Rafay, 2021), embezzlement and bribery, among others, have grown wide and the emergence of computer

DOI: 10.4018/978-1-7998-5567-5.ch014

software coupled with the advent of internet facilities has worsened the problems (Asuquo, 2012). The detection and prevention of the problems can be overcome using forensic accounting, especially at the state government level, where accounting controls and internal audit departments are not adequate to prevent and detect such financial misconducts (Dada, 2014; Khan *et al.*, 2020).

Muthusamy *et al.* (2010) argued that the growth in fraudulent practices is attributable to the non-adoption of forensic accounting by organizations. Accordingly, the non-adoption was presumed to be influenced by contextual, organizational and individual factors (Bierstaker *et al.*, 2006; Muthusamy, 2011). The low utilization of forensic accounting has been seen as a major factor contributing to the acceleration of fraud across the globe (Muthusamy, 2011). In specific, the demand for forensic accounting services continuously grows because of the increase in fraud (Azman and Vaicondam, 2020). Increase in financial crimes and the demand for the detection, prevention and deterrence of fraud in Nigeria have motivated forensic accounting research (Kumshe *et al.*, 2018). For long, Nigeria has been ranked among the most corrupt countries in the world by the Transparency International (Ekpo *et al.*, 2016). More so, at the state and local government levels, perpetrators get away unpunished. This means that only a few cases are uncovered on time, investigated, and prosecuted. Consequently, many financial crimes and the individuals involved are left undetected and unpunished (Okoye & Gbegi, 2013). Such problems justified the need for forensic accounting. In the same vein, Bierstaker *et al.* (2006) reported that forensic accounting is the most effective fraud detection tool but has the least adoption rate by organizations.

Furthermore, the World Bank (2020) disclosed that the drastic fall in oil prices together with the consequences of COVID-19 was expected to expose the Nigerian economy into a severe economic recession as worse as that of the 1980s. Hence, for many years the Federal Government of Nigeria would heavily depend on borrowing to finance its budget deficit. For the purpose of the 2021 budget, Nigeria sought to borrow ₦4.28tr, which could make the country's debt servicing be over ₦13.5 trillion. Averagely Nigeria is expected to pay \$303,683 monthly for matured loans (Ibemere, 2020). This study argues that continue borrowing without taking measures to deter and detect fraudulent activities would not impact positively on the lives of Nigerians but take the country deeper into the debt trap. Consequently, this study seeks to establish some key determinants of applying forensic accounting with a view to minimizing the fraudulent activities in Nigeria to the barest minimum. The borrowings that expose the Nigerian economy to various economic problems could also be reduced if not stopped at all, as the country has all potential to compete with many developed countries in the world.

According to the World Bank, there is the need to enact a series of potentially politically unpopular reforms in order to avoid a prolonged recession (Munshi, 2020). The bank added that by its failure to make a strong policy response, Nigeria would repeat the experience of the 1980 shocks, which became an impediment to the country's development by decades. In fact, according to Alia and Branson (2011), the political system of a country is one of the essential factors that affect its financial reporting framework. In addition, to a greater extent accounting is a product of its environment (Zhang, 2005). Generally, in the accounting literature, environmental factors were established as key factors responsible for international accounting diversity (Alia and Branson, 2011). Therefore, environmental factors are believed to have a significant influence on a country's accounting and auditing system and practices (Abdallah, 2008).

Briefly, the purpose of this study is to investigate the perceived political and environmental factors determining the application of forensic accounting in the North-Western States of Nigeria which has not been previously studied to the best knowledge of the researcher. The United Nations indicated a high rate of the prevalence of bribery in the public offices of the following states of Nigeria: Jigawa (93.0%), Kaduna (93.8%), Kano (84.8%), Katsina (92.9%), Kebbi (94.0%), Sokoto (95.5%) and Zamfara (95.5%)



(UNODC, 2017). Also, most former Governors in the region have cases with Economic and Financial Crimes Commission (EFCC). These include that of Jigawa State, (1.35 billion Naira fraud) and his son (10 billion Naira money laundering case) former governor of Kebbi State (0.45 billion Naira fraud) former governor of Katsina State (76 billion Naira) among others. All these fraudulent activities occurred despite the internal audit functions at the state level, the external auditors available in the office of the Auditor General of each state and all the anti-graft agencies established by the Nigerian government.

To the best of the researchers' knowledge, this study becomes the first to examine the relationship between political and environmental factors and the applicability of forensic accounting at the state level in Nigeria. The study is expected to provide answers to the following research questions:

1. Do the political factors significantly determine the applicability of forensic accounting in north-western states of Nigeria?
2. Do the environmental factors significantly determine the applicability of forensic accounting in the northwestern states, Nigeria?

## **LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT**

The unrelenting series of embarrassing audit failures over the years, has prompted a paradigm shift in accounting. In the mid-20th Century, when the fight for fraud detection was at its height, a few observers like Gray and Mousalli (2006) predicted that in future there would be the acceptance of the general responsibility of auditors to perform tests to detect material defalcation and errors if they exist. These events led to the hiring of fraud detection experts called forensic accountants. Forensic accounting can accordingly be defined as the practice of rigorous data collection and analysis in the area of litigation support, consulting, expert witnessing and fraud examination (Hogan *et al.*, 2008). According to Howard and Sheetz (2006) forensic accounting is the process of interpreting, summarizing and presenting complex financial issues clearly, succinctly and factually often in a court of law by an expert.

The fear of fraud is the motivation for hiring the forensic accountant, who is expected to detect fraud where it exists (Gray & Mousalli, 2006). Forensic accounting, therefore, refers to the comprehensive view of fraud investigation and includes the interview process of related parties to a fraud and the act of serving as an expert witness, among others. Bhasin (2007) asserts that the primary orientation of forensic accounting is a critical analysis of the phenomenon, including the discovery of deception and its effects introduced into the accounting domain. Degbaro and Olofinsola (2007) contended that forensic investigation is about the determination and establishment of facts in support of legal cases. It means that the use of forensic techniques to detect and investigate crime and expose all its attending features and identify the culprits is its main focus. It involves the application of accounting concepts and techniques to legal problems (Gray 2008).

Forensic accounting is all-encompassing as a practical field that includes accounting fraud, forensic auditing, compliance, due diligence and risk assessment, detection of financial misrepresentation and financial statement fraud (Skousen and Wright, 2008). In the words of Owojori and Asaolu (2009), forensic accounting is different from old debit and credit accounting, as it provides an accounting analysis that is suitable to the organization, which will help to resolve the disputes that arise in the organization. It demands reporting where the fraud is established and the report is considered as evidence in the court of law or the administrative proceeding (Kasum, 2009). Forensic accounting is also defined as a sci-

## **Determinants of Forensic Accounting**

ence dealing with the application of accounting facts and concepts gathered through auditing methods, techniques and procedures to resolve legal problems, which required the integration of investigative accounting and auditing skills (Koh, *et al.*, 2009; Dhar and Sarkar, 2010).

In the view of Singleton and Singleton (2010), forensic accounting refers to the analysis, inspection, and investigation, auditing and questioning process to reach the truth and obtain an expert witness opinion. It also includes fraud examination, litigation support and consulting. Forensic Accounting is also called investigative accounting or fraud audit, which is a merger of forensic science and accounting. Similarly, Stanbury and Paley (2010) defined forensic accounting as the science of gathering and presenting information in a form that will be accepted by a court of jurisprudence against the perpetrators of economic crime.

It is also concerned with the use of the accounting discipline to help to determine the issues of facts in business litigation (Okunbor & Obaretin, 2010). Forensic accounting is a discipline that has its models and methodologies of investigative procedures that search for assurance, attestation and advisory perspective to produce legal evidence, tax evasion, bankruptcy, valuation studies and the violation of accounting regulation (Dhar & Sarkar, 2010). It can also be employed in a setting where there is a breakdown of ethical behaviour under a complacent board (Buckstein, 2012). Forensic accounting is a scientific accounting method of uncovering, resolving, analysis and presenting fraud matters in a manner that is acceptable in a court of law (Oyedokun, 2013). All this means that forensic accounting can be employed in a variety of situations (Singleton; & Flesher, 2003; Bhasin, 2007; Gray, 2008; Özkul & Pamukçu, 2012). Deducing from above, forensic accounting can, therefore, be employed in multiple situations, which include the investigation of fraud and fraudulent practices, white colour crimes, litigation support, expert witness, evidence gathering, arbitration, business valuation, loss of earnings, professional liability, insurance claims, general damages, employee theft/fraud, financial statement fraud and corporate governance challenges. Thus, forensic accounting is an umbrella term that has multiple ranges of activities, which can be considered as various subthemes under it.

The general view of some authors (Smith & Crumbley 2009; Coppola 2006; Howard and Sheetz, 2006; AICPA, 2008; Chariri, 2009; Dhar and Sakar, 2010; Buckstein 2012; Bhasin 2007) is that forensic accounting has two main branches which are: investigative accounting and litigation support. Other authors (Iwata 2003; Wells 2011; Grippo & Ibex, 2003; Coenen, 2005; Gray & Mousalli, 2006; Singleton & Singleton, 2010) consider it to be employable in a variety of cases that involve civil and criminal actions (fraud, bankruptcy, matrimonial disputes, insurance casualty claims, personal injury claims, professional negligence and/or malpractice) and, therefore, has multiple branches or sub-themes. According to Saha (2014), forensic accounting is an umbrella term which has several branches as a field of knowledge that comprises accounting, auditing, investigative skills more of a 'bloodhound' of accounting and plays the role of a "watchdog" and is used to sniff out fraud and illegal transactions in public organizations and other institutions suitable for legal review.

## **POLITICAL FACTORS AND FORENSIC ACCOUNTING**

Generally, political factors are among key factors that influence the internalization of accounting and auditing standards (Abdallah, 2008). Similarly, the political system is an important factor that influences the development of accounting practices (Tahat *et al.*, 2018). Pratiwi *et al.* (n.d) concluded that a number of political factors, such as colonialism and the quality of local regulators, international power

politics and Colonialism, were established to affect the adoption of international financial reporting standards. Nearly all developed countries have well established political systems characterized by almost all developed countries, which are based on high levels of democracy, freedom, political stability and the culture of accountability (Alia and Branson, 2011). They added that some or all of these factors are found in the political systems of developing countries.

Further, Nobes (1998) claims that political systems do not affect accounting in developed countries because they are probably sufficiently homogeneous in these countries, but they may change the accounting system in developing countries, particularly local legislations and tax laws in order to favor political affiliates and other category of people because of nepotism. Ball *et al.* (2003) find it likely that political factors influence financial reporting practices in East Asian countries.

In specific, though there is very scanty literature on the impact of political factors and forensic accounting, they have been established as key factors that affect the applicability of forensic accounting as a result of the abuse of office by politicians (Imam, 2013). This is because in developing countries political office holders do not continue with the policies of previous governments, particularly of the opposition party. This indicates that the political will of office holders can determine the applicability of forensic accounting at the state level in Nigeria.

Briefly, the regular change of governments at the state levels in Nigeria due to the four-year tenure can affect the application of forensic accounting because another government administration may not be willing to continue with applying forensic accounting, particularly if it is initiated by the previous opposition party. But in developed countries there is continuity of previous government's good policies even if they were initiated by previous administrations. Hence, it is hypothesized that:

**H<sub>01</sub>:** Political factors have a positive and significant effect on the applicability of forensic accounting

## **ENVIRONMENTAL FACTORS AND FORENSIC ACCOUNTING**

Accounting is a product of its environment (Zhang, 2005). Generally, in the accounting literature, environmental factors were established as key factors responsible for international accounting diversity (Alia and Branson, 2011). Therefore, environmental factors are believed to have a significant influence on a country's accounting and auditing system and practices (Abdallah, 2008).

In specific, as regard to environmental factors Ibrahim *et al.* (2018) argued that the environment provides resources and posed obstacles to organizational performance. In essence, the adoption of forensic accounting may be influenced by environmental characteristics such as the availability of resources. Consequently, environmental factors have a basis to be considered as among the key determinants of the applicability of forensic accounting at the state level. Therefore, it is hypothesized that:

**H<sub>02</sub>:** Environmental factors have a positive and significant effect on the applicability of forensic accounting.

## **METHODOLOGY**

The objective of the present research is to answer the research question and identify whether political and environmental factors significantly determine the applicability of forensic accounting in the northwestern

## Determinants of Forensic Accounting

zone of Nigeria. The survey method is selected for the purpose of this study in order to collect a sufficient amount of primary data. The use of questionnaires is the most widely used data collection technique in a survey. The population of the study consisted of all the Ministries in the northwestern States of Nigeria, which covered seven states, namely Jigawa, Kaduna, Kano, Katsina, Kebbi, Sokoto and Zamfara states, with 1,636 accountants, internal and external auditors on Grade Level 12 and above for the 2019 budget year estimate. The sample of the study was arrived at using the Taro the Yamane 1968 formula. The sample for each state was arrived at using a stratified sampling technique. All the items adapted in the questionnaire are answered using the five points Likert scale. The use of the five- point scale format is considered most appropriate because it has been found to enhance the reliability of measures and reduce social desirability bias that could lead to the contamination of substantive results. A similar scale has also been used in previous studies (Olukayode, 2018; Wilson, Francis and Emeka 2017; Evans 2017; Fyneface and Sunday 2017), among others. The data collected are analyzed using partial least squares (PLS) path modelling using the smart PLS3 statistical software. This study distributed 482 copies of a questionnaire, and a total of 412 copies were finally retrieved back. This led to obtaining a response rate of 85%. A reasonably better response rate was achieved, which is above the expected rate of response, and as a result of the researcher's persistence, for on the mark conclusion of the questionnaire. Furthermore, in the procedure of data cleaning and screening, sixteen copies of survey questionnaires were detached from the records set and regarded as not suitable to continue the analysis. Thus, overall, 396 copies of the questionnaire were accurate and used for a continuous analysis.

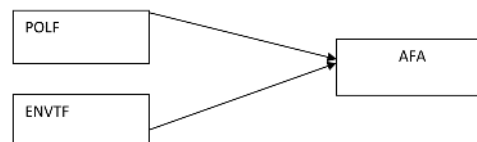
All the variables of the study were adapted from prior studies and measured with 5 point Likert scale, which ranges from 5= strongly agree to 1= strongly disagree. The applicability of forensic accounting (the dependent variable) was measured using 13 items namely detection and prevention of fraud, corruption, bribery, financial mismanagement, theft and reducing all financial misconducts (Imam, 2013; Sinha, 2021; Rafay, 2021). The political factor (the independent variable) was measured using 3 items namely; abuse of office and power, lack of continuity on the part of political office holders and lack of continuity on the part of fraud investigation agencies staff at the state level (Imam, 2013 and Eme, 2013). The environmental factor (another independent variable) was measured using 8 items namely availability of forensic experts, forensic laboratory, chemicals and reagents, computers, conducive air conditioning, meeting environmental regulations, climatic condition, and equipment and facilities as adapted from Ibrahim *et al.* (20016) and Ibrahim (2018).

Figure 1. Conceptual framework designed by the researchers

Key: AFA: Applicability of forensic Accounting

POLF: Political Factor

ENVTF: Environmental Factor



## Model Specification

$$AFA = \beta_0 + \beta_1 POLF + \beta_2 ENVTF \quad (1)$$

Where:

*AFA* = Applicability of forensic accounting

*POLF*= Political factors

*ENVTF*= Environmental factors

## RESULTS AND DISCUSSION

This study used the structural equation modelling (SEM) approach. There are three main reasons for using this approach. First, it is helpful to identify the predictive causal relationship (Baron & Kenny 1986). Second, it uses partial least squares (PLS) with confirmatory factor analysis (CFA) to test the hypotheses. Third, it has a friendly graphical interface, which helps users to create a moderating effect for the path model. This study uses Software SmartPLS 3.2 to analyze the data. It performs two steps to analyze data using the outer model (measurement model) by using the PLS algorithm. It also analyses the inner model i.e. the structural model through a bootstrap resampling technique.

Figure 2. Measurement Path

Source: PLS Result Output 2020

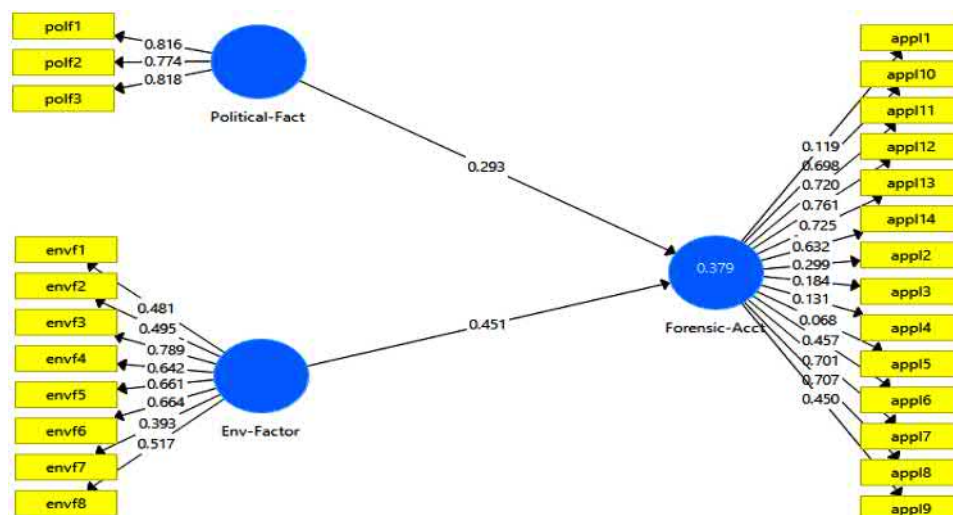


Figure 2 shows that the variable of the study, the oval blue cycle represents the independent variables (Political Factor and Environmental factor) and the dependent variable (Applicability of Forensic Accounting). The rectangles represent the items of the measure of the construct.

## ASSESSMENT OF MEASUREMENT MODE/OUTER LOADING

This subsection explains the measurement/outer loading of the model. It is part of the SEM model, which describes the relationships among the latent variables and their indicators (Becker *et al.* 2012). On the other hand, the outer model parameter estimates consist of the loadings (Ringle *et al.*, 2012). Figure 2 represents the path model.

*Figure 3. Path Model*

*Source: PLS Output Result 2020*

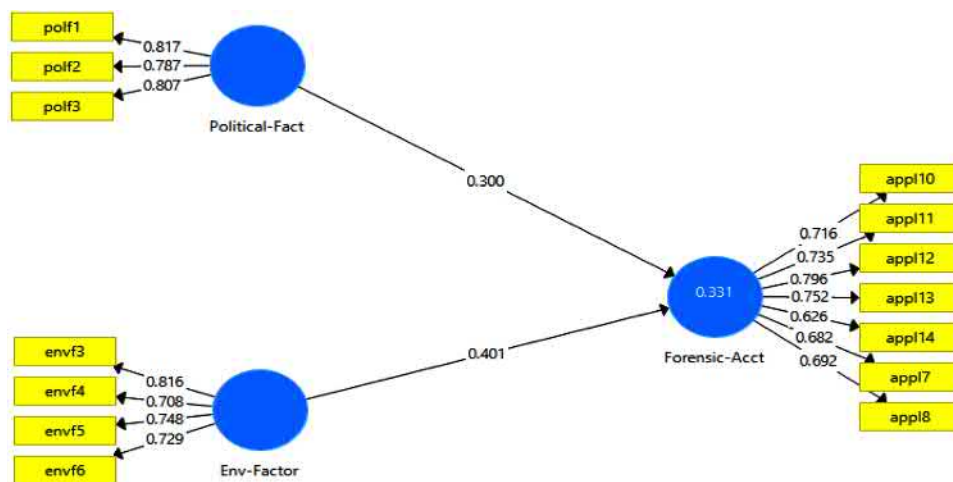


Figure 2 shows the loadings of respective indicators/items for the constructs and hence, it is reported by the reliability and validity, and discriminates validity.

## Reliability and Validity Tests

This study performs internal consistency composite reliability (CR) to ensure the accuracy of the designed first-order reflective constructs and factor loading to evaluate the reliability of each item (Nunnally 1994). It also executes the average variance extended (AVE) to evaluate the construct's validity. As illustrated in Table 1, factor-loading values for the all informative indicators were above 0.5. It achieves the desired value, which findings supported by several studies (Hair *et al.* 2012). The results of the constructs achieved desired composite reliability (CR)>0.7 and have gotten accepted AVE value >0.5 as presented in Table 1.

Table 1 shows the loadings of the respective items on their construct, and all the loadings are above 0.5. Also, the Table shows Cronbach's Alpha (CA) and composite reliability (CR), which is above the threshold of 0.7 and the Average Variance Extracted (AVE) is above the recommended value of 0.5. The study thus achieved the desired reliability of the constructs.

*Table 1. Constructs Reliability and Validity*

Constructs Reliability and Validity			Composite Reliability	Average Variance Extracted (AVE)
Items	Loadings	Cronbach's Alpha		
App_f10	0.716	0.749	0.838	0.565
App_f11	0.735			
App_f12	0.796			
App_f13	0.752			
App_f14	0.626			
App_f7	0.682			
App_f8	0.692			
Evn_f3	0.816	0.841	0.880	0.513
Evn_f4	0.708			
Evn_f5	0.748			
Evn_f6	0.729			
Pol_f1	0.817	0.729	0.846	0.646
Pol_f2	0.787			
Pol_f3	0.807			

Source: PLS Result Out 2020

## Discriminant Validity

The discriminant validity explains how each variable is distinct from each other in the study. The study report in Table 2 using Fornell and Lacker Criterion, Cross Loadings and Heterotraits-Monotraits Ratio.

Table 2 shows the discriminant validity using Fornell and Lacker criterion for the variable of the study. It indicates that the diagonal and bold figure show the square of the AVE and are above all the correlation of their respective loadings. Thus, the study satisfies this discriminant validity criterion and hence we shall check the next criterion.

*Table 2. Discriminants Validity*

Fornell and Lacker Criterion	Environment Factor	Forensic Application	Political Factor
Environment Factor	<b>0.751</b>		
Forensic Application	0.501	<b>0.716</b>	
Political Factor	0.335	0.434	<b>0.804</b>

Source: PLS Result Output 2020

In a similar view, the result of Table 3 shows the discriminants validity using the Heterotraits-Monotraits ratio. The threshold, as indicated by Henseler, *et al.* (2016), informed that none of the loadings should be above 0.9. Looking at the value, the highest is 0.582, which indicates that the discriminants validity using Heterotraits-Monotraits ratio is also achieved.

## ***Determinants of Forensic Accounting***

*Table 3. Discriminants Validity*

<b>Heterotraits-Monotraits Ratio</b>	<b>Environment Factor</b>	<b>Forensic Application</b>	<b>Political Factor</b>
Environment Factor			
Forensic Application	0.582		
Political Factor	0.475	0.536	

Source: PLS Result Output 2020

## **R Square**

The coefficient of determination ( $R^2$ ) illustrates the amount of variance in the endogenous constructs. It indicates that the threshold value of 0.25 (as weak), 0.5 (as moderate) and 0.7 (as substantial respectively). Thus, below is the R square value for the study.

Table 4 shows that the  $R^2$  value is 0.544. Therefore, it explains the 54% of the variation in the independent variables of the model.

*Table 4. Coefficient of Determination*

	<b>R Square</b>	<b>R Square Adjusted</b>
Forensic Application	0.544	0.328

Source: PLS Result Output 2020

## **Effect Size**

Effect size as a statistical concept to determine the strength of the relationship between two variables and explain a defined endogenous variable in terms of  $R^2$ . The larger the effect size means the stronger the effect. The guidelines indicates three effect sizes of the evaluation: 0.02 (small), 0.15 (medium) and 0.35 (large) impact on the endogenous constructs.

Tables 5 presents the results that environmental and political factors have a positive and a significant impact on the application of forensic accounting with a medium effect size of 0.213 and 0.120, respectively.

*Table 5. Effect Size*

<b>F Square Effect Size</b>	<b>Environmental Factor</b>	<b>Forensic Applicability</b>	<b>Political Factor</b>
Environmental Factor		0.213	
Forensic Applicability			
Political Factors		0.120	

Source: PLS Result Output 2020



## ASSESSMENT OF STRUCTURAL MODEL/INNER LOADING

This sub section explains about the assessment of the structural model. Also, it completes the SEM model, which describes the correlations among the latent variables that make up the SEM model (Chin, 2010).

Figure 4 shows the result of the bootstrapping of the direct relationship between the independent variables and the dependent variable of the study and the test of hypotheses. Below is the result of the test of hypotheses in Table 6.

Figure 4. Bootstrapping Result of Direct Relationship

Source: PLS Output Result 2020

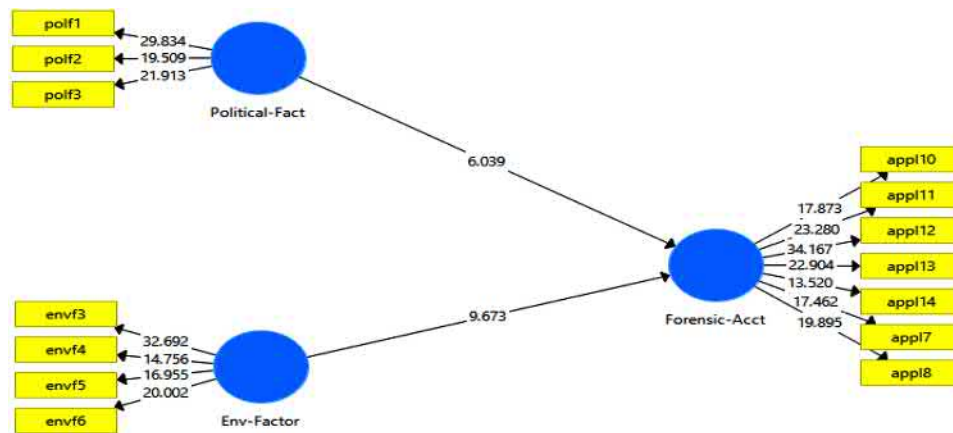


Table 6 shows the bootstrapping procedure for testing the hypotheses and evaluating the significance between constructs (Henseler *et al.* 2014). The Table further elucidates that all constructs in the model are with a critical value of 1.96 for the two-tailed test at the significant level  $p < 0.05$ . Therefore, it supports the following hypotheses:

Table 6. Test of Hypotheses

Hypotheses	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics ( O/STDEV )	P Values
Env_Factor ->Forensic_App	0.401	0.406	0.041	9.673	0.000
Pol_Factor ->Forensic_App	0.300	0.300	0.050	6.039	0.000

Source: PLS Result Output 2020

Table 6 summarizes the assessment of the relationship between the constructs (endogenous and exogenous). Results recapitulate that,

## ***Determinants of Forensic Accounting***

H<sub>01</sub>: Environmental factor has a positive and significant influence on applicability of forensic accounting ( $\beta = 0.401$ , t-value 9.673 and P-value = 0.000). Hence, this study was with the opinion that the application is largely influenced by environmental factors. These study findings are in support of the earlier findings of Ibrahim, Rose, and Mudzamir (2016) and Ibrahim (2018), who observed that the processes for the investigation of financial malpractices need environmentally friendly and infrastructural facilities for experts to carry out forensic accounting to detect and prevent fraud in government and the private sectors. Hence, environmental factors are positively related to the applicability of forensic accounting.

H<sub>02</sub>: Political factors have a positive and significant effect on applicability of forensic accounting ( $\beta = 0.300$ , t-value 6.039 and P value = 0.000). Hence, this study was with the opinion that the application of forensic accounting is largely influenced by transparency and accountability and political will from the top management of public organizations to use forensic accounting techniques in the prevention of fraud and other financial crimes. These study findings are in support of the earlier findings of Olukayode (2018), who mentioned that forensic accounting as the technique for investigating financial malpractices would be supported by political influence in the prosecution of perpetrators in courts. In addition, Joseph, Okike & Mathew (2016) and Imam (2013) observed that forensic accounting serves as a significant tool for the prevention of fraud in government and the private sector.

In contrast, results show that the environmental factor has a higher influence on the applicability of forensic accounting with ( $\beta = 0.401$ ), while the Political factor ( $\beta = 0.300$ ) has an effect on the applicability of forensic accounting. Applicability at the state level will definitely help in recovering looted funds as well as preventing future occurrence. This can be achieved through the use of financial forensics which is a modern tool used in tracing and investigating books/transactions that will lead to the discovery of financial fraud. It can also be achieved through the use of computer/digital forensics, which is used to uncover computer or digitally based frauds.

## **IMPORTANCE PERFORMANCE MATRIX (IPMA)**

The last step in assessing the structural model is to measure the importance-performance matrix (IPMA). Figures 5 and 6 illustrate the relationship between the constructs.

Figure 5 shows the level of the importance and the performance level of the respective variables. Political factor shows the level of importance approximately 0.27, that is, about 27% importance, while the environmental factor explains more than 41% level of importance in the model. This signifies that state and the federal authorities should pay more attention to the political factor, as it can affect the value of the applicability of forensic accounting in the various states under study. Similarly, Figure 6 shows the full level of performance to the main constructs, as the political factor assumes 74.55%. While the environmental factor shows the level of performance to be 76.12%.

Figure 5. Importance –Performance Map Analysis 1

Source: PLS Result Output 2020

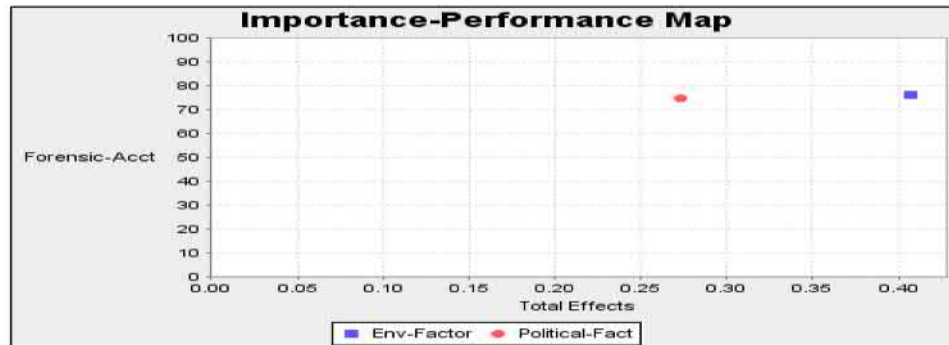
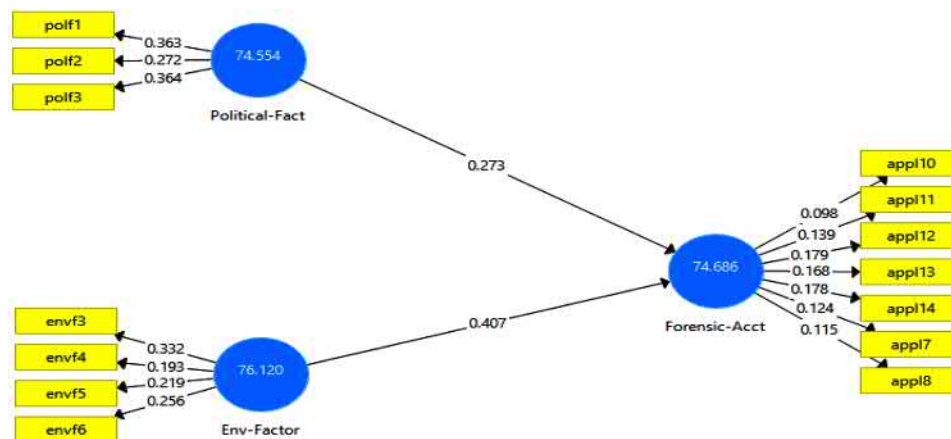


Figure 6. Importance –Performance Map Analysis 2

Source: PLS Result Output 2020



## DISCUSSION OF FINDINGS

The study found that political and environmental factors affect the application of forensic accounting in the study area. This indicates that today modern organized financial misconducts, such as employee theft, payroll fraud, states government budget and insurance fraud, embezzlement and bribery, among others, have grown wide and the emergence of computer software coupled with the advent of internet facilities has worsened the problem (Asuquo, 2012). The detection and prevention of the problems can be overcome using forensic accounting, especially at the state government level, where accounting controls and internal audit departments are not adequate to prevent and detect financial misconduct.

The paper sought to look at the effect of environmental and political factors on the application of forensic accounting in state government offices. This is on the score that previous studies have not focused on such an important issue. Accountants, auditors and finance personnel are confronted with complex financial decisions in running their state on a day-to-day basis (Ramzan, *et al.*, 2020). Thus, the effect of fraud indicated a high rate of the prevalence of bribery in the public offices of the northwestern States.

## ***Determinants of Forensic Accounting***

This is to cope with a directed effort to the finances of their respective state and local governments in a hardy, transparent and professional way on the applicability of forensic accounting. The study found a significant positive relationship between environmental and political factors on the applicability of forensic accounting. This implies that improvements in the environmental and political factors could spur an increase in applicability of forensic accounting in the study area. As indicated earlier, the volume and value of the knowledge available in applicability could create an advantage through proper decision making of public account. This likely supports the survey conducted by Chartered Global Management Accountant (2014) and suggests that the use of cloud-based solutions in accounting information system encourages professional accountants to know more about environmental and political factors on fraud detection.

## **CONCLUSION AND RECOMMENDATIONS**

The objective is to investigate whether political and environmental factors affect the applicability of forensic in Nigeria. Questionnaires were administered to accountants and auditors (internal and external) of various selected Ministries in the seven northwestern geo-political zones of Nigeria. The results of the study established the political and environmental factors as significantly affecting applicability of forensic accounting in the Northwestern geo-political zones of Nigeria. The findings of the study imply that largely the political will of top management of public organizations affect the use forensic accounting techniques in the prevention and detection of fraud and other financial crimes. Besides, making the environment conducive would contribute successfully to the applicability of forensic accounting. On the basis of findings, the study recommended that all political office holders and other government personnel should use their power to ensure the right and the continuity of the government policies and programs for forensic accounting applicability even with a change of government. State governments should also provide the enabling environment for applicability through the provision of needed and equipment, facilities and other resources necessary to carry out forensic services.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.

- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

Abdallah, W. M. (2008). The Economic and Political Factors and Their Impact on Accounting and Management in the Gulf Countries. In *Accounting, Finance, and Taxation in the Gulf Countries*. Palgrave Macmillan. doi:10.1057/9780230614543\_2

AICPA. (2008). *FVS practice aid 10-1 serving as an expert witness or consultant*. American Institute of Certified Public Accountant.

Alia, M., & Branson, J. (2011). The effect of environmental factors on accounting diversity. A literature review. SSRN *Digital Library*. Retrieved from <https://ssrn.com/abstract=1780479>

Archambault, J. J., & Archambault, M. E. (2003). A multinational test of determinants of corporate disclosure. *The International Journal of Accounting*, 38(2), 173–194. doi:10.1016/S0020-7063(03)00021-9

Asuquo, A. (2012). An empirical analysis of the impact of information technology on forensic accounting practice in Cross-River State Nigeria. *International Journal of Scientific & Technology Research*, 1(7), 25–33.

Azman, N. L. A., & Vaicondam, Y. (2020). Behavioral Intention in Forensic Accounting Services. *International Journal of Psychosocial Rehabilitation*, 24(2), 1837–1846. doi:10.37200/IJPR/V24I2/PR200485

Ball, R., Robin, A., & Wu, J. S. (2003). Incentives versus standards: Properties of accounting income in four East Asian countries. *Journal of Accounting and Economics*, 36(1-3), 235–270. doi:10.1016/j.jacceco.2003.10.003

Baron, R. M., & Kenny, D. A. (1986). Moderator Mediator Variables Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology*, 51(6), 1173–1182. doi:10.1037/0022-3514.51.6.1173 PMID:3806354

Becker, J. M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models. *Long Range Planning*, 45(5/6), 359–394. doi:10.1016/j.lrp.2012.10.001

Bhasin, M. (2007, January). Forensic accounting: A new paradigm for niche consulting. *The Chartered Accountant*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2703647](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703647)

Bierstaker, J. L., Brody, R., & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, 21(5), 520–535. doi:10.1108/02686900610667283

Buckstein, J. (2012). Forensic accounting: Far from a recent phenomenon Professional Development network. *Professional Development Network*. Retrieved from <https://docplayer.net/4231616-Forensic-accounting-part-1-far-from-a-recent-phenomenon.html>

## **Determinants of Forensic Accounting**

- Chariri, A. (2009). The relevance of forensic accounting in detecting financial fraud. *Bankers' Magazine*.
- Chin, W. W., Thatcher, J. B., Wright, R. T., & Steel, D. (2013). *Controlling for common method variance in PLS analysis: The measured latent marker variable approach*. Springer.
- Coenen, T. L. (2005, November 30). Forensic Accounting: A New Twist on the Bean Counting. *Wisconsin Law Journal*. Retrieved from <https://wislawjournal.com/2005/11/30/forensic-accounting-a-new-twist-on-bean-counting/>
- Coppola, D. R. (2006). Demystifying financial fraud: Forensic accountants gain in popularity. *Alaska Business Monthly*, 22(5), 79.
- Dada, S. O. (2014). Forensic accounting techniques: A means of successful eradication of corruption through fraud prevention, bribery prevention and embezzlement prevention in Nigeria. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 4(1), 176–186. doi:10.12816/0018900
- Degbaro, D., & Olofinsola, J. (2007). Forensic accountants and the litigation support engagement. *Nigerian Accountant*, 40(2), 49-52.
- Dhar, P., & Sarkar, A. (2010). Forensic accounting. An accountants vision. *Vidysagar University Journal of Commerce*, 15(3), 93-104.
- Ekpo, C. E., Chime, J., & Enor, J. N. (2016). The irony of Nigeria's fight against corruption: An appraisal of president Muhammadu Buhari's first eight months in office. *International Journal of History and Philosophical Research*, 4(1), 61–73.
- Eme, E. J. (2013). *An exploration of forensic accounting education and practice for fraud prevention and detection in Nigeria* (Unpublished PhD Thesis). University De Montfort, Leicester, UK.
- Evans, O. N. (2017). Forensic accounting and the combating of economic and financial crimes in Ghana. *European Scientific Journal*, 13(31), 379–393. doi:10.19044/esj.2017.v13n31p379
- Fyneface, N. A., & Sunday, O. O. (2017). Forensic accounting and fraudulent practices in the public sector. *International Journal of Arts and Humanities*, 6(2), 171–181.
- Gbegi, O. O., & Adebisi, J. F. (2013). The new fraud diamond model: How can it help forensic accountants in fraud investigation in Nigeria public sector? *Mediterranean Journal of Social Sciences*, 5(3), 243–252.
- Gray, D. (2008). Forensic accounting and auditing: Compared and contrasted to traditional accounting and auditing. *American Journal of Business Education*, 1(2), 115–126. doi:10.19030/ajbe.v1i2.4630
- Gray, O. R., & Mousalli, S. D. (2006). Forensic accounting and auditing united again: A historical perspective. *Journal of Business Issues*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1642100](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1642100)
- Grippio, F. J., & Ibex, T. (2003). Introduction to forensic accounting. *National Public Accountant*, 4, 4–8.
- Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The Use of Partial Least Squares Structural Equation Modelling in Strategic Management Research: A Review of Past Practices and Recommendations for Future Applications. *Long Range Planning*, 45(5-6), 320–340. doi:10.1016/j.lrp.2012.09.008

- Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modelling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. doi:10.1007/11747-014-0403-8
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). Testing Measurement Invariance of Composites Using Partial Least Squares. *International Marketing Review*, 33(3), 405–431. doi:10.1108/IMR-09-2014-0304
- Hogan, C. E., Rezaee, Z., Riley, R. A. Jr, & Velury, U. K. (2008). Financial statement fraud: Insights from the academic literature. *Auditing*, 27(2), 231–252. doi:10.2308/aud.2008.27.2.231
- Howard, S., & Sheetz, M. (2007). *Forensic accounting and fraud investigation for no experts*. Wiley.
- Ibemere, I. D. (2020). Next Level: 2021 budget serviced by Debt! *Dataphyte*. Retrieved from <https://www.dataphyte.com/economy/next-level-2021-budget-serviced-by-debt/>
- Ibrahim, U., Rose, S. S., & Mudzamir, M. B. (2016). Adoption of forensic accounting in fraud detection process by anti-corruption agency. *A Conceptual Frame Work*, 6(2), 139 – 148.
- Ibrahim. (2018). Adoption of forensic accounting in fraud detection process by Anti-corruption Agency: A conceptual framework. *International Journal of Management Research & Review*, 6(8), 139-148.
- Imam, A. (2013). *Forensic accounting model for Fraud prevention and detection in Nigeria public sector* (Unpublished PhD Thesis). Usman Danfodio University, Accounting, Sokoto, Nigeria.
- Imam, A., Kumshe, A. M., & Jajere, M. S. (2015). Applicability of forensic accounting services for financial fraud detection and prevention in the public sector of Nigeria. *International Journal of Information Technology and Business Management*, 4(1), 136–152.
- Iwata, E. (2003). Accounting Detectives in Demand. *USA Today*.
- Joseph, F. A., Okike, B. M., & Yoko, V. E. (2016). The Impact of Forensic Accounting in Fraud Detection and Prevention: Evidence from Nigerian Public Sector. *International Journal of Business Marketing and Management*, 1(5), 4–41.
- Kasum, A. S. (2009). The relevance of forensic accounting to financial crimes in private and public sectors of the third world economies: A study from Nigeria. *Journal of Accountancy*, 2(1), 23–40. doi:10.2139srn.1384242
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Koh, A. N., Arokiasamy, L., & Suat, C. L. A. (2009). Forensic accounting: Public acceptance towards occurrence of fraud detection. *International Journal of Business and Management*, 4(11), 145–149. doi:10.5539/ijbm.v4n11p145
- Kumshe, A. M., Umar, I., & Imam, A. (2018). Prospects of Forensic Accounting Education in Nigeria: A Review. *Journal of Resources & Economic Development*, 1(1), 74–84.
- Munshi, N. (2020, December 10). Nigerian economy at risk of ‘unravelling’, warns World Bank. *Financial Times*. Retrieved from <https://www.ft.com/content/14f600e9-2a7b-4a59-be67-f6485b256e99>

## **Determinants of Forensic Accounting**

- Muthusamy, G. (2011). *Behavioral intention to use forensic accounting services for the detection and prevention of fraud by large Malaysian companies* (Doctoral dissertation). Curtin University, Australia.
- Muthusamy, G., Quaddus, M., & Evans, R. (2010, June). Organizational intention to use forensic accounting services for fraud detection and prevention by large Malaysian companies. *Proceedings of the 2010 Oxford Business & Economic Conference (OBEC)*.
- Nobes, C. W. (1998). Toward a general model of reasons for international differences in financial reporting. *Abacus*, 34(2), 495–519. doi:10.1111/1467-6281.00028
- Nunnally, J. C. (1994). *Psychometric theory* (3<sup>rd</sup> ed.). Tata McGraw-Hill Education.
- Okoye, E., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and prevention in the public sector. A study of selected ministries in Kogi State. *International Journal of Academic Research in Business & Social Sciences*, 3(1), 1–1.
- Okunbor, J. A., & Obratin, O. (2010). Effectiveness of the application of forensic accounting services in Nigerian organizations. *Journal of Management Sciences*, 1(1), 171–184.
- Olukayode, S. A. (2018). Forensic accounting investigation techniques and successful prosecution of corruption cases in Nigeria. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 8(3), 37–44.
- Owojori, A. A., & Asaolu, T. O. (2009). The role of forensic accounting in solving the vexed problem of corporate world. *European Journal of Scientific Research*, 29(2), 183–187.
- Oyedokun, G. E. (2013). *Emergence of forensic accounting and the role in Nigeria economy*. In a lecture delivered at the Annual NUASA Week, 2012.
- Özkul, F. U., & Pamukçu, A. (2012). Fraud detection and forensic accounting. In *Emerging fraud* (pp. 19–41). Springer. doi:10.1007/978-3-642-20826-3\_2
- Pratiwi, N., Shalihatulhayah, A., & Mayasari, D. (n.d.). The Influence of Political Factors on IFRS Adoption. *The 3rd Uzbekistan-Indonesia International Joint Conference on Economic Development and Nation Character Building to Meet the Global Economic Challenges*.
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.
- Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's Comments: A Critical Look at the Use of PLS-SEM. *Management Information Systems Quarterly*, 36(1), iii–xiv. doi:10.2307/41410402
- Saha, C. A. (2014). A multidimensional approach to investigating frauds and scams: A study in the global and Indian context. *The Management Accountant India*, 49(9), 29–36.
- Singleton, T., & Flesher, D. L. (2003). A 25 years retrospective on the IIA's SAC project. *Managerial Auditing Journal*, 18(1), 39–53. doi:10.1108/02686900310454237



- Singleton, T. W., & Singleton, A. J. (2010). *Fraud auditing and forensic accounting*. Wiley. doi:10.1002/9781118269183
- Sinha, A. (2021). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Skousen, C. J., & Wright, C. J. (2008). Contemporaneous risk factors and the prediction of financial statement fraud. SSRN *Digital Library*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=938736](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=938736)
- Smith, G. S., & Crumbley, D. L. (2003). Defining a Forensic Audit. *The Journal of Digital Forensics, Security and Law*, 4(1), 61-80. Retrieved from <https://commons.erau.edu/jdfs/vol4/iss1/3/>
- Stanbury, J., & Paley-Menzies, C. (2010). Forensic futurama: Why forensic accounting is evolving. *AICPA Store*, 28.
- Tahat, Y., Omran, M. A., & AbuGhazaleh, N. M. (2018). Factors affecting the development of accounting practices in Jordan: An institutional perspective. *Asian Review of Accounting*, 26(4), 464–486. doi:10.1108/ARA-01-2017-0010
- UNODC. (2017). *Corruption in Nigeria, Bribery: public experience and response*. United Nations Office on Drugs and Crime. Retrieved from [https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Nigeria/Corruption\\_Nigeria\\_2017\\_07\\_31\\_web.pdf](https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Nigeria/Corruption_Nigeria_2017_07_31_web.pdf)
- Wells, J. T. (2011, October 1). The Fraud examiners. *Sleuthing Carrier bring CPA's Personal and Satisfaction, Journal of Accountancy*. Retrieved from <https://www.journalofaccountancy.com/issues/2003/oct/thefraudexaminers.html>
- Wilson, H. E., Francis, O., Emeka, E. E., & Loraver, T. N. (2017). Fraud and forensic accounting education: Prospects and challenges in Nigeria. *International Journal of Business and Management*, 12(7), 146–161. doi:10.5539/ijbm.v12n7p146
- World Bank. (2020, June 26). *Nigeria's Economy Faces Worst Recession in Four Decades*. World Bank Report. Retrieved from <https://www.worldbank.org/en/news/press-release/2020/06/25/nigerias-economy-faces-worst-recession-in-four-decades-says-new-world-bank-report>
- Yildirim, Y., & Rafay, A. (2021). Anti-Money Laundering in Insurance Sector: The Turkish Case. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Zhang, G. (2005). *Environmental Factors in China's Financial Accounting Development since 1949* (PhD Thesis). Erasmus University Rotterdam. Retrieved from <http://hdl.handle.net/1765/1888>

## **ADDITIONAL READINGS**

- Adegbe, F. F., & Fakile, A. S. (2012). Economic and Financial Crime in Nigeria: Forensic Accounting as Antidote. *British Journal of Arts and Social Sciences*, 6(1), 37–50.

## **Determinants of Forensic Accounting**

Anuolam, O. M., Onyema, E. T., & Okeke, U. (2016). Forensic accounting and financial crisis in Nigeria. *West African Journal of Industrial and Academic Research*, 17(1), 126–132.

Claire, A. C., & Jude, I. O. (2016). Forensic accounting and fraud detection in Nigerian public sector. *Igbinedion University Journal of Accounting*, 2, 148–173.

Efiong, E. J. (2012). Forensic accounting education: An exploration of level of awareness in developing economies-Nigeria as a case study. *International Journal of Business and Management*, 7(4), 26–34. doi:10.5539/ijbm.v7n4p26

Ehioghien, E. E. (2016). Forensic accounting and fraud management: Evidence from Nigeria. *Igbinedion University Journal of Accounting*, 2(1), 245–308.

Enofe, A. O., Okpako, P. O., & Atube, E. N. (2013). The Impact of Forensic Accounting on Fraud Detection. *European Journal of Business and Management*, 5(26), 61–72.

Ezeagba, C. E. (2014). The role of forensic accounting and quality assurance in financial reporting in selected commercial banks in Nigeria. *International Journal of Economic Development Research and Investment*, 5(2), 20–32.

Franklyn, O. I. (2013). Automated Auditing and fraud control in Nigeria. A case study of the economic and financial crimes commission (Unpublished Undergraduate Project). Caritas University, Nigeria.

Hassab, E. H., Epps, R. W., & Said, A. A. (2003). The impact of environmental factors on accounting development: An Egyptian longitudinal study. *Critical Perspectives on Accounting*, 14(3), 273–292. doi:10.1006/cpac.2002.0530

Irvine, H. J., & Lucas, N. (2006). *The rational and impact of the adoption of International Financial Reporting Standards: the case of the United Arab Emirates*. In *18th Conference on International Accounting Issues, Asian-Pacific*.

Kimberly, J. R., & Evanisko, M. J. (1981). Organizational innovation: The influence of individual, organizational and contextual factors on hospital adoption of technological and administrative innovations. *Academy of Management Journal*, 24(4), 689–713. PMID:10253688

Mohamed, E. K., & Lashine, S. H. (2003). Accounting knowledge and skills and the challenges of a global business environment. *Managerial Finance*, 29(7), 3–16. doi:10.1108/03074350310768319

Owolabi, S. A., Dada, S. O., & Olaoye, S. A. (2013). Application of forensic accounting in investigation and detection of embezzlement to combat corruption in Nigeria. *Unique Journal of Business Management Research*, 1(14), 65–70.

Rezace, Z., Crumbley, D. L., & Elmore, R. C. (2006). Forensic accounting education: A survey of academicians and practitioners. *Journal of Forensic Accounting*, 10(3), 48–59.

Roberts, C., Weetman, P., & Gordon, P. (2005). *International Financial Reporting, A comparative approach*. Prentice-Hall.

Saito, M., & Teresa, L. (2016). Global case studies in forensic accounting education: The case of audit failures. *Journal of Global Business Management*, 12(1), 176–183.


Section 4

# Investment Frauds

# Chapter 15

## Financial Scams Through Ponzi Schemes: The Case of CIS Countries

Alam I. Asadov

 <https://orcid.org/0000-0003-0805-6482>  
Prince Sultan University, Saudi Arabia

### ABSTRACT

*This chapter investigates the relationship between financial literacy, financial sector development, and Ponzi schemes in the commonwealth of independent states (CIS) countries. It begins with an overview of the early cases of Ponzi schemes in the CIS countries by examining circumstances which formed fertile ground for the schemes to develop during initial years of independence. The study then scrutinised the situation in the member states during the later years which revealed no improvements. A closer examination of the problem discovered that the main triggers are low level of financial literacy and scarce investment alternatives. The chapter suggests that unless the level of financial literacy is raised and the financial sector is developed, Ponzi schemes will continue to thrive in the region. It concludes by providing some policy recommendations to enhance financial literacy and financial sector development, as well as necessary steps to improve financial regulations.*

### INTRODUCTION

Following the collapse of the USSR, most of its former states are united in a union called the Commonwealth of Independent States (CIS). Even though each CIS country has chosen its own transition path which differs from the previous Soviet style command economy, the countries still share common economic history and heritage. These include low level of financial literacy among the public and under-developed financial industries. A large gap in the public's financial literacy level and their understanding of the market economy and financial markets existed since the early years of independence. This is true for all CIS countries particularly during the initial economic transition phase from a planned to a market economy. Nevertheless, during those early years, some quickly adopted to the new economic

DOI: 10.4018/978-1-7998-5567-5.ch015

reality and learned the rules of the game, while a vast majority of the population still depended on their old knowledge in economics and financials for survival. Thus, those with first-mover advantage became rich quickly, but at the cost of others who were financially illiterate and lacked business skills.

The Soviet Union also did not have a sophisticated financial system. It mainly relied on state owned commercial banks to primarily finance public enterprises, while financing for the other parts of the economy was either underdeveloped or non-existent. Commodities, forex or stock exchanges were not required given the absence of large private corporations which would raise funds through stocks or bonds; and the state controlled the commodities and foreign exchanges prices. The financial markets and institutions were mainly at very primitive stages or even lacking in most CIS countries in the early years of independence. It is disheartening to see that financial sector development has not progressed much in some of these countries, even after almost three decades of so-called 'economic transition' since their independence.

In the post-Soviet era, despite widespread financial illiteracy of the general public, there was a strong urge for new income sources in addition to the low salaries being earned, which formed a fertile ground for financial scams. Due to the lack of viable investment opportunities, Ponzi schemes were set up by some opportunists that had unfortunately led to many naive citizens of the CIS countries becoming victims (Aris, 2011; Koker, 2012; Witt, 1994). For example, one of the most infamous schemes which took place in early 1990s in the Russian Federation was the MMM Ponzi scheme. The scheme was promoted in many different ways by promising annual returns up to 2000%. It deceived the financially illiterate population of ex-Soviet Russia with an estimated 5 to 10 million 'investors' becoming victims. It was reported that most investors did suspect the fraudulent nature of the MMM scheme, but voluntarily took part in it with the hope of profiting quickly; and would withdraw their money before the scheme collapsed (Witt, 1994).

Citizens from the other countries of the CIS did not escape from such fraudulent schemes either. Countries such as Armenia, Georgia<sup>1</sup>, Kyrgyzstan, Uzbekistan and many others have experienced Ponzi schemes (Arminfo, 2013; EurasiaNet, 2016a, 2018; TI, 2012). If this was only a thing of the past, we would be relieved and satisfied with the lessons learned. Unfortunately, we are still witnessing such schemes until today. What is more worrying is that with the development of financial technology (fintech) and financial deregulation (DeFi), we can expect even more similar schemes taking place, particularly in dealing with cryptocurrencies and crypto assets (Hess & Soltes, 2018; Levenson, 2019; SEC, 2013a,b; Rafay, 2019).

The author sees financial illiteracy and underdeveloped financial infrastructure in the CIS countries as the main causes of the Ponzi scheme formation. Increasing financial education and developing the financial sector are viewed as possible cures for the problem. Unfortunately, despite years of financial illiteracy, most CIS countries still exclude financial education as part of their secondary education curriculums (Andreff, 2019; Filippova *et al.*, 2016; Koker, 2012). Most youths in these countries are still financially illiterate as their parents were. In view of this, the author suggests to improve financial education and to instil it into the education system as early as possible. Such measures would serve to eradicate financial illiteracy in the CIS countries to a certain degree, which could potentially reduce the frequency and extent of financial frauds. As witnessed in the developed countries, financial literacy plays an important role to educate the general public in making correct investment decisions (Younas & Rafay, 2021).

Citizens of developed countries are less prone to becoming victims of financial scams such as the Ponzi schemes due to wide availability of legitimate and sustainable investment alternatives. A more

developed financial industry can make available such alternatives to the general public, as information on the legitimacy of investment funds and use of resources are publicly provided. Such alternatives were and are still lacking in most CIS countries, with the gap being filled by Ponzi schemes and other similar financial scams. This leads us to suspect that development of the financial sector and increasing availability of different investment alternatives are important factors to reduce the level and frequency of Ponzi scheme formation in any country.

This chapter focuses on Ponzi schemes in the CIS countries due to two reasons - one being personal to the author; and the other is specific to the characteristics of the chosen countries. Firstly, the author has witnessed these cases, either by living thorough the events directly, or indirectly by observing them through daily news updates, having lived through most of the transition period in one of the CIS countries. Secondly, the CIS countries have witnessed significant changes both in the level of financial literacy and financial sector development after transiting from a command to a market economy within the past three decades.

The CIS countries chosen for the case study in this chapter provide the best examples to understand the factors relating to formation of Ponzi schemes. This chapter aims to analyse specific root causes of the scheme by studying some of its examples in the member countries. Consequently, some solutions for the problem will be investigated in the form of enhancing financial literacy, financial development, improvement in financial regulations and other actions that the governments can take to address the issue. General conclusion and some specific recommendations will follow. As a start, some background needs to be established to provide general understanding of Ponzi schemes and their formation in the CIS countries.

## **PONZI SCHEMES AND THEIR FORMATION IN CIS COUNTRIES**

### **What Are Ponzi Schemes and How Do They Work?**

The name originates from Charles Ponzi, an Italian immigrant who formed such a scheme during the early 1920s in the United States. He started the scheme as a genuine proposal to buy and hold foreign postal stamps. He would then resell them to the respective issuing country to make profits due to the higher currency exchange rate of the issuing country. Some of Ponzi's friends and family members got convinced by his business proposal and made large investments in the scheme. When the business proposal was not working as Ponzi expected, he started using some of the latter investments to pay the promised high dividends for the initial investors, which attracted more people to the scheme. However, it was too late when Ponzi realized that the scheme was unsustainable, and he had already accumulated a \$15 million debt during the first nine months of his venture. As an honest citizen, he started repaying the investors. Unfortunately, the business was \$4 million short to pay off all of its liabilities and had to be declared bankrupt. Charles Ponzi was later arrested and sentenced to some jail time (Frankel, 2012). Despite the fact that Ponzi started the scheme with good intentions, other schemes with a similar structure are named after him, even though the history of financial pyramids started during much earlier times.

In general, a Ponzi scheme works as follows: First, the scheme master starts by offering an investment proposal which promises very high returns with little or no risk. The investment is supposedly tied to a business venture or financial agreement which is portrayed as undoubtedly profitable in the scheme master's description. Once the scheme pays handsome dividends to the initial investors, it starts to gen-

erate large interest from new investors. The master uses the new funds to pay the promised high returns to the existing and new investors. This leads to even more investors joining the scheme. The scheme continues to expand in a similar manner until it either catches the attention of respective authorities, or until the scheme master realises that the pyramid has reached its point of culmination, and it is time to flee. Either way, the scheme can end abruptly, with only a few people on the top of the pyramid regaining their investment and even some gains, while most investors in the bottom of the pyramid who joined the scheme later would end up losing part or all of their investments (Frankel, 2012).

### **Some Background of Ponzi Scheme Formation in CIS Countries**

As mentioned earlier, lack of viable investment opportunities due to underdeveloped financial sectors, combined with lack of financial literacy among majority of the population served as a fertile ground for the formation of Ponzi schemes in most CIS countries. Since the start of early independence in 1991, the 12 CIS members were in the state of transition from the former Soviet style command economy to market economy as their new form of economic structure. While some chose a sudden or abrupt form of transition to market economy, others have chosen a more gradual method of transition. Irrespective of the transition choices made, the countries were more or less in a similar economic situation in the early 1990s.

The Russian Federation (i.e. Russia) was among the states which chose the “shock therapy” or “big bang” transition style that was mainly motivated by its first president, Boris Yeltsin and his pro laissez-faire cabinet. To expedite the process of transition, the state decided to issue privatisation vouchers in 1992 and started mass privatisation with this process. Every Russian citizen was given a free voucher worth 10,000 rubles (worth approximately \$25) with three options on how to utilise the voucher. They could either sell it for cash, invest in investment funds or directly invest in any public company undergoing privatisation. Many people decided to sell it for cash at a price equal to a fraction of its intrinsic value. Some chose to invest in investment funds which mostly turned out to be scams or Ponzi schemes. Only a few decided to invest them directly into any company undergoing privatisation given that the notion of private enterprise was relatively new and unknown to most of them (Tolstikova, 1999).

Such mass privatisation served to develop the Russian financial market and many new investment funds’ shares were traded freely, but with most destined for failure. Due to lack of restrictions for investment funds, there was a large tendency for some of the investment fund managers to choose an easier way of making money. Forming Ponzi schemes to take advantage of the financially illiterate public who possessed free cash in the form of vouchers was indeed a rare opportunity not to be missed. Most Ponzi schemes such as Tibet, Russki Dom, Selenga and Khopor did not grow too large and failed earlier on mainly due to lack of any bail-out promise by the government. Some others such as MMM have grown large both in terms of fund size and coverage of geographic area, which led to people being hopeful that it was too large to fail and that the government will bail them out even if they did (Bhattacharya, 2003). At that time, most Ponzi schemes were advertised to the masses as a common citizen’s way out of poverty. Due to some misconception, people believed that one can become rich quickly without putting much effort under the market economy. While some people realised the risks of investing in Ponzi schemes, they also assumed that such schemes had high profit potentials. This led to many believing that they would be able to pull out of the scheme before it collapses, but unfortunately this was not the case in reality (Tolstikova, 1999; Witt, 1994).

The MMM Ponzi scheme started in December 1992 and was promoted by one of its founders, Sergei Mavrodi, as a voucher investment fund called MMM-Invest which would collect privatisation vouchers for investment in the privatisation of public enterprises. Under this investment fund, a Ponzi scheme was found in February 1994 which gained fast popularity due to its promise of 20% to 60% monthly returns or up to 2000% annual returns for its deposits (Koker, 2012; Tolstikova, 1999). This ‘get rich quick’ scheme was widely advertised in Russian televisions which costed around 330 million rubles in March 1994 alone. As such, it was able to attract the interest of over 5 million Russians. However, the government grew suspicious of the investment fund’s rapid success and the Ministry of Finance issued a statement declaring MMM as an illegal investment firm circulating unregistered securities on 22 July 1994; and its founder Sergei Mavrodi was arrested by government prosecutors. The fund officially stopped functioning the next day. Mass protests were organised by thousands of investors in front of the MMM headquarters for several days that resulted in police intervention to disperse the crowd (Sloane, 1994). Mavrodi vowed that he will get MMM’s government bailout if he was released from prison and get elected as a member of the Russian Duma (Federal parliament). Under public pressure, he was released from jail and was elected to the Duma. This helped him to avoid criminal prosecution, but without any bailout taking place. A distinct feature of this and other similar scheme was “the initial non-discouragement by regulators and possibility of partial bailouts following any collapse” (Bhattacharya, 2003). Russians did learn their lessons at an early stage, but it is unfortunate that some are still falling into the trap of Ponzi schemes even until today, either due to lack of financial literacy and/or lack of viable investment alternatives (Aris, 2011; Kruglikov & Coalson, 2020).

Countries such as Belarus, Uzbekistan and Turkmenistan have chosen more gradual form of transition reforms. In these countries and others with similar reform strategies, no significant economic transition was witnessed in the early years of transition. Hence, no tangible change took place in the level of financial sector development as well as the population’s level of financial literacy (UNECE, 2003). Even though the magnitude and number of Ponzi schemes were not as large as the number of schemes witnessed in Russia, such schemes still emerged in some of the states in one form or another until today.

Other CIS countries which were more progressive reformers as compared to the above three, include countries such as Kazakhstan, Kyrgyzstan, Azerbaijan, Armenia and Georgia. These countries were also not also free from such financial scams. All of them had developed different levels of financial literacy and financial development as they transitioned towards becoming market economies. Ponzi schemes still existed in these countries from their independence until now. For instance, while construction-related Ponzi schemes flourished in Georgia in mid-2000s, the revival of MMM in the form of benevolent NGOs based on mutual cooperation was seen in early 2010s in Armenia. Some Central Asian members of CIS such as Uzbekistan and Kyrgyzstan which lagged further behind in terms of financial literacy and financial sector development have witnessed more recent cases of Ponzi schemes in the form of investment schemes and trade companies. Nevertheless, it does not mean that such schemes have disappeared in CIS countries with somewhat more developed financial sectors. Poor strata of population with relatively lower levels of financial literacy are becoming recent targets of Ponzi schemes in countries such as Russia (EurasiaNet, 2018; Kruglikov & Coalson, 2020).



## **Possible Causes of Ponzi Schemes in CIS Countries**

In the initial observation of the background of Ponzi scheme formation in the CIS countries, some common patterns are noticeable in most situations. The author suggests the following three hypotheses which will be considered in reviewing Ponzi schemes in other CIS countries:

**Hypothesis One:** Ponzi schemes are more frequently formed in an environment where the general public has lower level of financial literacy.

**Hypothesis Two:** Low level of financial literacy reduced awareness of authorities about financial frauds which led to increasing negative impact of the frauds on society.

**Hypothesis Three:** Underdeveloped financial sectors and unavailability of viable investment alternatives encouraged people to invest in Ponzi schemes.

An initial analysis of these hypotheses provides some preliminary results for the early years of independence in Russia, such as the case of the MMM Ponzi scheme. Firstly, there is no doubt in suggesting low level of literacy as a reason for the formation of Ponzi schemes, as observed from the MMM Ponzi scheme. It took place in early 1990s when Russia was in the initial stages of transition into a market economy and most people in the country were financially illiterate. Secondly, the respective government authorities are also to be blamed for allowing the MMM Ponzi scheme to grow to such a large scale. Their ignorance however could be partially explained by the low level of financial knowledge among public officials. Finally, relative scarcity of other investment alternatives was an additional factor that drew the general public to the scheme, despite some of them being aware of its dubious nature. It is obvious that all three hypotheses hold true in the MMM pyramid scheme of Russia. Next, the chapter will analyse the relative stance of financial literacy and financial sector development in the CIS countries, and investigate whether those could be the root causes of Ponzi scheme formation in these countries. Other cases of the Ponzi schemes will be further analysed, and the above suggested hypotheses would each be tested qualitatively.

## **REASONS BEHIND FORMATION OF PONZI SCHEMES IN CIS COUNTRIES**

### **Financial Literacy and Financial Development in CIS Countries**

As postulated in the previous sections, there are two assumptions on the main causes behind the formation of Ponzi schemes in the CIS countries, which are lack of financial literacy and underdevelopment of financial infrastructure. When it comes to the impact of financial literacy on formation of Ponzi schemes, a recent empirical study by Amoah (2018) using logistic regression on a large sample data from Ghana shows the importance of financial literacy to avoid people from becoming victims of such scams. More specifically, their findings show that as more investors understand the Ponzi schemes and their associated warning signs, the lower are the odds (0.9771) of them being victimised by Ponzi scheme operators. Also, the findings indicate that as more investors possess knowledge about different investments, the odds (0.7899) of Ponzi operators duping them are lower.

Most of the victims of Ponzi schemes in developed countries such as the United States had no clear purpose for being involved in the schemes, other than to obtain more income and wealth (Azim & Azam, 2016; Trahan *et al.*, 2005). On the other hand, an analysis of victims in developing countries indicated different underlying reasons for their involvement. For instance, when the profile of different Ponzi scheme victims was studied in China, there were many pressing reasons for them to invest in such schemes. These include preventing wealth deterioration, paying for housing, saving for children's education, saving for future pension or healthcare needs, and so on (Fei *et al.*, 2020). The victims of Ponzi schemes in the CIS countries most likely have similar goals which forced them to join such schemes, given similarities in their background due to economic and financial transitions. The shortage of viable investment alternatives for people in these countries could also be the reason for the success of Ponzi schemes there.

Within almost three decades of economic transition, financial development did not progress at a similar pace among all CIS states, where some countries witnessed very limited developments. Even for some member countries with relatively developed financial sectors, a part of the earlier developments in their finance industries was partially reversed in more recent years. For instance, from Table 1, the average ratio of domestic credit to private sector increased from 1995 to 2008, but the ratio slightly reduced for some countries with the CIS average, with a decrease from 35.1% to 32.8%. Part of it could be due to diversification of the financial sector and development of capital markets. Nevertheless, due to the unavailability of such data for all CIS countries, such conclusion cannot be made. The contrary was observed when data is available. Out of three countries which have data on capital markets, only one (i.e. Russian Federation) expanded its equity markets and the other two (i.e. Kazakhstan and Ukraine) experienced contractions within the same metric. Another explanation of such contraction in financial development could be the rise of shadow economies which is not unusual for economies in transition.

Some progress could also be observed in terms of financial literacy. According to the OECD (2018), results of a survey conducted in 2016 show that the average level of financial knowledge was found to be about 50% in seven of the surveyed CIS countries. However, the average score in this component ranged from as low as 37% for Kyrgyz Republic to reaching the highest at 61% for Belarus. If other components of financial literacy such as behaviour and attitude are included, the overall average rises to 56% (see Table 2). This is still low as compared to the financial literacy level in developed countries, especially the knowledge component of financial literacy. For a person to be considered as financially literate, the individual should be able to answer five or more of the seven financial knowledge questions correctly. Unfortunately, only 30% of the surveyed adults from the CIS countries were able to achieve this minimum target and about 48% of adults in G20 countries could obtain that minimum score in similar surveys conducted by the OECD. The average number of correct answers for the knowledge component of the financial literacy survey was 4.3 out of 7 (61%) for all participants in G20 countries, while the same was only 3.5 (50%) for the CIS countries. The fraction of adults who are considered financially literate was even more diverse, ranging from 10% in Tajikistan to 45% in the Russian Federation (See Figure 1).

As can be seen from the above analysis, both financial sector development and evolution of financial literacy vary largely among the CIS countries. According to the latest data from the World Bank, the ratio of private sector credit to GDP ranges from as low as 12.3% in Tajikistan to as high as 62.6% in Georgia. Similarly, financial market development is also diverse among the CIS countries. In using market capitalisation of listed companies (as % of GDP) as a proxy for such development, we see it ranging from 3.4% in Ukraine to 34.5% in Russia (See Table 1). The financial literacy divide gets even larger with almost 90% of those surveyed from Tajikistan not meeting financial knowledge standards, while the financial literacy level of Russians reaching almost as high as the average level of G20 coun-

tries with 45% meeting the minimum financial knowledge requirements. This given fact can imply that financial crimes such as Ponzi schemes could be a history for some CIS countries and a present time reality for others. Nevertheless, we cannot assume even distribution of financial literacy and financial sector development among the regions of more advanced CIS countries. Some may be lagging behind, such as in the impoverished and underdeveloped rural areas of Russia.

*Table 1. Financial development and macroeconomic indicators for CIS countries*

Indicator	Domestic Credit to Private Sector (% of GDP)			Market Capitalisation of Listed Companies (% of GDP)			GDP per Capita (current US\$)		
	1995	2008	2018	1995	2008	2018	1995	2008	2018
Armenia	7.3	17.4	55.5	-	1.5	-	456	4011	4220
Azerbaijan	-	-	20.8	-	-	-	397	5575	4740
Belarus	6.1	28.8	27.6	-	-	-	1371	6377	6330
Georgia <sup>^</sup>	6.1	33.3	62.6	-	2.6	-	578	3325	4723
Kazakhstan	7.1	50.1	25.9	-	23.5	20.6	1288	8514	9813
Kyrgyz Republic	12.5	13.8	23.4	-	1.8	-	364	966	1308
Moldova	6.7	36.5	23.2	-	-	-	594	2111	4234
Russian Federation	9.4	42	50.9	-	23.9	34.5	2666	11635	11371
Tajikistan	-	19.9	12.3	-	-	-	214	716	827
Turkmenistan	1.1	-	-	-	-	-	590	3904	6967
Ukraine	1.5	73.7	34.5	-	13.5	3.4	936	3887	3097
Uzbekistan	-	-	23.8	-	-	-	586	1082	1529
CIS average*	6.4	35.1	32.8	-	11.1	19.5	837	4342	4930

<sup>^</sup> Georgia is still added in the table even if it withdrew from the CIS effective 13 August 2008

\*Unweighted average

Source: Cojocaru *et al.* (2016), The World Bank (2020)

*Table 2. Components of financial literacy in selected CIS countries*

Country	Financial Literacy Component			Average
	Knowledge	Behaviour	Attitude	
Armenia	52%	60%	48%	54%
Azerbaijan	45%	55%	55%	52%
Belarus	61%	71%	55%	64%
Kazakhstan	58%	71%	52%	62%
Kyrgyz Republic	37%	60%	62%	53%
Russian Federation	59%	57%	58%	58%
Tajikistan	38%	62%	56%	52%
CIS average*	50%	62%	55%	56%

\*Unweighted average

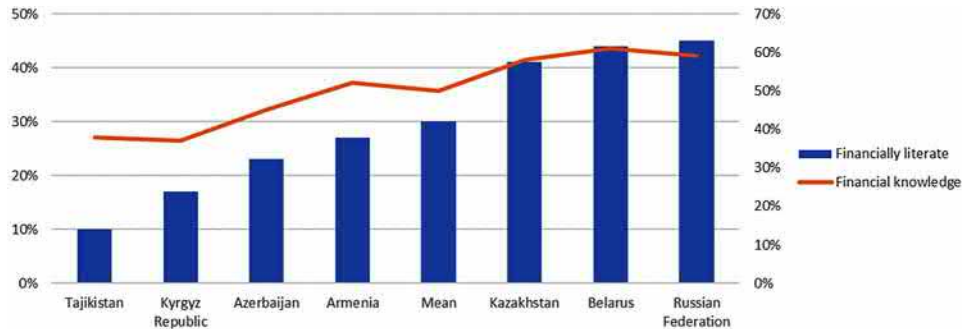
Source: *Levels of Financial Literacy in Eurasia*. OECD (2018)

## Financial Scams Through Ponzi Schemes

Figure 1. Financial knowledge and financially literate in participating CIS countries

Note: Values at left axis corresponds to financially literate while at right axis corresponds to financial knowledge

Source: Levels of Financial Literacy in Eurasia. OECD (2018)



All of these factors may contribute to the development of shadow economy. IMF (2009) has warned about increasing number of financial frauds being observed especially in countries with significant shallow financial systems. According to an empirical study of Ponzi scheme participation in Jamaica by Tennant (2011), the aura of exclusivity cultivated by Ponzi scheme masters with promises of significant gains are important factors that influence high levels of exposure to them. His findings also show that referrals from friends was another major factor adding to the credibility of the enigmatic claims being made for this informal investment alternative. Let us now scrutinise other cases of Ponzi schemes in the CIS countries and try to better understand the circumstances which resulted in their development. This can assist us to analyse whether the above studied factors may have contributed to the development of Ponzi schemes in these countries.

### The Case of Center Point Group of Georgia

The Ponzi schemes took different shapes in different countries of the CIS. For instance, in Georgia, construction-related Ponzi schemes became popular in late 2000s with the Center Point Group (CPG) Ponzi being the largest among them. CPG was a large construction conglomerate in Georgia consisting of 70 different companies. It was founded by three partners who also owned the smaller companies belonging to the Group. Two of the founders, Vakhtang Rcheulishvili and Rusudan Kervalishvili are the former MPs of the Georgian Parliament and the third partner is the wife of Vakhtang, Maia Rcheulishvili. The CPG Ponzi scheme attracted thousands of customers to buy unbuilt apartments and was said to have mishandled the construction payments estimated at \$310 million. As a result, about 6,200 families and 30,000 individuals lost their lifetime savings by investing in worthless incomplete apartments (TI Georgia, 2012).

The Ponzi scheme started in 2007 when CPG was using funds received from new customers to build the apartments promised to the earlier investors. The apartments were heavily advertised in all Georgian public television channels as a unique property purchasing opportunity with a flexible payment schedule offered by a renowned developer. This was an irresistible deal for many ordinary citizens who fell prey to the Ponzi scheme. The main nuance of the scheme was that none of the construction agreements were made between the customer and CPG. Instead, all agreements were signed between the customers and one of the small subsidiaries of CPG which had an initial capital of \$200 to \$300 and limited liability

(as compared to the parent company with millions of dollars in equity) (Patsuria, 2012). As with any Ponzi scheme, mishandling of money and drying up of sources of funds would lead to the collapse of the entire scheme. Many complaints were launched by the CPG customers in the civil courts, which required delivery of the promised apartments or compensation of losses. The courts responded by requesting the responsible companies to fulfil the demands of the customers, but to no avail. The dummy companies were already insolvent and CPG being the main perpetrator had no legal obligation to pay for their liabilities. Furthermore, close ties with the former government and the immunity status of the CPG founders shielded them from any personal liability for the losses inflicted on the customers, as the same ties assisted them in the formation of the scheme (TI Georgia, 2012)

Overall, there were some factors which contributed directly to the rise of construction-related Ponzi schemes in Georgia. These factors, according to Papava (2013) include large amount of foreign direct investments (FDIs) flowing into privatisations and acquisitions of real estates that far exceeded the sector's growth potentials, therefore causing a misbalance in the real estate industry. Low level of governmental controls over developments in the construction sector also made this a lucrative industry and a breeding ground for Ponzi schemes. Local banks which acquired cheap funding from the European financial markets for the purpose of construction financing further fuelled the expansion of construction-related Ponzi schemes. In summary, lack of financial and business competence of Georgian homebuyers as well as lack of investment alternatives for both consumers and banks resulted in the formation of large construction-related Ponzi schemes in the country during the late 2000s. While the founders of such schemes were opportunists taking advantage of the circumstance, part of the blame can also be placed on imprudent government officials who were ignorant of the situation.

## **The Ahmadboi Pyramid Scheme of Uzbekistan**

A more recent case is the financial pyramid scheme set up by Ahmad Tursunboev (a.k.a. Ahmadboi) in Uzbekistan. Ahmadboi along with his 30 associates formed a crude Ponzi scheme in the Chinaz district of the Tashkent region of the country which promised an annual investment return of 100%. The fund accepted all forms of investments ranging from cash, jewellery, cars to even houses. Around 40,000 to 80,000 naive investors participated in the scheme without realising that such a profitable enterprise was too good to be true (RFE/RL's Uzbek Service, 2018). At the time of his arrest in mid-June 2016, the scheme was in operation for about 5 years with full support from the local officials. The scheme ended with the arrest of the founder and the confiscation of money amounting to \$18.6 million at Ahmadboi's office. Titles for hundreds of cars and several houses were also found in his possession. It was also suspected that at the time of his arrest, Ahmadboi had already managed to transfer a significant sum of his money abroad (EurasiaNet, 2016b).

Ahmadboi's Ponzi scheme was said to have involved many in the country. Since the beginning of the investigation, some officials linked to the case, such as the Chief Prosecutor, Head of Police and even Governor of the Chinaz district out of which Ahmadboi operated his scheme lost their jobs. During prosecution, it was revealed that the perpetrator was careful enough to not provide any written commitments to the investors and even mentioned to some that the returns cannot be guaranteed in the case of his death or other unforeseen circumstances (EurasiaNet, 2016a). After almost two years of investigation, Ahmad Tursunboev was sentenced to 13 years in prison by the Tashkent regional court on 21 February 2018. At the same court session, the term of sentence was reduced by one-quarter under an amnesty

provision; and the service of the term was considered to begin from the day of his arrest in June 2016 (RFE/RL's Uzbek Service, 2018).

This infamous case exposed some weak sides of Uzbekistan's economy. For instance, the government failed to create a healthy investment environment with viable alternatives for personal investments. During the initial 25 years of its independence, Uzbekistan had a rather slow transition to a market-based economy under the ruling of its first President, Islam Karimov (EurasiaNet, 2016a). At that time, neither the capital markets nor any other financial institutions aside from state-owned commercial banks were developed. Ordinary citizens of the country had no exposure to real financial investments or acquired any financial literacy skills. This made them easy targets for fraudulent get-rich-quick pyramid schemes. Even high-ranking officials such as governors or prosecutors lacked the financial competence to realise that such schemes were similar to the fraudulent and non-sustainable ones set up by Ahmadboi.

### **The Sattylyk Pyramid Scheme Which Broke Kyrgyz Villagers**

Another sad story took place in 2017 in the neighbouring Kyrgyzstan, involving a Ponzi scheme which captured the region's surrounding villages around Issyk-Kul Lake. A Kazakhstan-based organisation called Sattylyk started operating a Ponzi scheme in Kyrgyzstan by pledging to bring villagers out of poverty. Such classic get-rich-quick scheme was too good of an offer to be turned down by the non-sceptical rural community. Sattylyk's scheme was rather simple. It promises an astonishing return of 300,000 som (\$4,400) within a couple of months to any investor who agrees to invest 34,000 som (around \$500) and to bring in several more investors. The initial seed money of \$500 provides an investor the right to a unit called "wallet." Those who were able to attract another 14 investors earned the title of "millionaire" and earned \$4,400 (equivalent of 1 million Kazakh Tenge) (EurasiaNet, 2018).

Once Sattylyk paid back part of the promised dividends to the initial investors, more investors started coming in with cash in hand. The investors were offered lucrative returns but most of the money was sent off to Kazakhstan rather than being placed in any investment. Similar to any classic Ponzi scheme, Sattylyk initially paid attractive returns to early investors which drew a larger crowd of investors. But as the number of new investors reduced, so did the compensation that was promised to the existing ones. Consequently, the pyramid scheme failed in September 2017. As a result, more than 300 complaints were filed about Sattylyk in 2018. Unfortunately, the Interior Ministry Department for the Issyk-Kul region claimed that their hands were tied since the company did not do anything illegal. The number of people affected by the scheme was estimated at 1,000 investors from villages along the lakeside (EurasiaNet, 2018).

Similar to the previous cases, lack of financial literacy among ordinary citizens and government officials was the main reason for the formation of schemes such as the Sattylyk in Kyrgyzstan. Despite being filed as a fraud case by the Ministry of Interior officials in January 2018, the company is still officially registered with the Justice Ministry as a limited liability partnership dealing with "wholesale of goods of a wide range" and operating until today (JMKR, 2020). According to the Director of Sattylyk, Zhannatkan Attokurova, the description of the firm is inaccurate and she defines the company as a charitable organisation with no forced participation (EurasiaNet, 2018). This clearly highlights a loophole in the justice system which allows companies to declare one activity as their main function, while in reality it is not the case. As in the earlier cases, shortage of investment opportunities for the rural people of Kyrgyzstan along with lack of financial knowledge made them vulnerable to Ponzi schemes.

## **Ponzi Schemes Are Still Thriving in CIS Countries**

One may assume that after the lessons learned from the 1990s, together with the relative development of the financial sector in the 2000s, financial pyramids would have disappeared or significantly subsided in Russia. On the contrary, Ponzi schemes remain in Russia and their numbers may have risen. According to Marat Safiulin, the Head of the Federal Public-State Foundation for the Protection of Investor and Shareholder Rights, a new financial pyramid emerges in Russia every 48 hours, based on 2016 estimates (Nikolova, 2017). The Russian Central Bank identified around 200 organisations suspected to be pyramid schemes in 2019, from only 168 a year before. These include a company called Sberkassa Alanii operating in early 2019, in the provincial capital of North Ossetia that was charged with fraud allegations due to the suspicion of stealing 288 million rubles (\$4.6 million) from prospective investors. In the same year, trial started in the Omsk region against a businessman called Dmitry Danilov on the suspicion of defrauding more than 100 people in a pyramid scheme for a total amount of 20 million rubles (\$317,000) (Kruglikov & Coalson, 2020). There are countless similar cases both in Russia and other CIS countries, indicating that not much reduction could be seen in the number of Ponzi schemes in the CIS in recent years.

It is a great concern that the schemes are able to change forms and adapt to changing times and cultures. They have become harder to be recognised by an untrained eye or by the regular laymen with no financial knowledge. There are several strategies generally employed by Ponzi schemes to conceal their true nature from unsuspected investors. Some could be using a modified name of a famous company or a well-known brand or referring to a well-known company that lacks credible source of information. Agreements with customers are also often made in a company office or in person to discourage customers from having more time to thoroughly review the documents or to consult others before making their final decisions. Customers therefore often do not understand that in-between the lines, the scheme management is able to free itself from any prepayment of principal or membership fee if the company fails to fulfil its promises (Filippova *et al.*, 2016).

Some Ponzi schemes can also imitate a multi-level marketing (MLM) arrangement which can be in the form of distributors for health and beauty or consumer products. The scheme can appear as an MLM but in reality, there are no legitimate products to sell or there are some dubious products with inflated price tags. Unlike MLM arrangements, Ponzi schemes focus on membership fees or quick disposals of the product bundles rather than real marketing of the company products (Koker, 2012). As soon as people realise that the products, they bought are worthless and there are not enough customers joining the pyramid, the scheme collapses. Ponzi schemes can also pose themselves as investment funds mainly in disguise of forex (foreign exchange) clubs. The forex clubs start with heavy advertising and promise handsome returns to their investors. Once money is invested in the clubs, investors that want to retrieve their principal along with the promised returns would be told that their money was lost due to miscalculations made by the clubs. At times, the original investment and real returns could be paid back to the investors by bigger and more famous clubs. However, these clubs engaged in profit smoothing by simply paying some returns to a majority of investors by stealing larger sums from other investors (Aris, 2011).

The above and many other varieties of Ponzi schemes are still actively deployed in the CIS countries. Unfortunately, we cannot only blame the scheme masters for the formation of such financial pyramids, as their customers and respective government institutions are also at fault. This is proven by numerous case examples which have also shown the validity of all three hypotheses put forward in the earlier section. The first hypothesis holds, and we could see how deficiency in financial literacy and business

knowledge was a major factor in the formation of Ponzi schemes in all of the studied cases. The indirect result from lack of financial knowledge was also observed among government officials, which paved the way for Ponzi schemes to operate smoothly either officially or otherwise. This fact supports the second hypothesis of the chapter. Underdeveloped financial sector was another major cause of increasing Ponzi schemes. In all of the studied cases, lack of investment alternatives also made financial pyramids appear as a mirage in a desert. Therefore, it can be assumed that unless a systematic approach is adopted to address these issues, the problem of Ponzi schemes will persist, and many more may suffer as a result.

## **HOW TO FIGHT PONZI SCHEMES: SOME POLICY RECOMMENDATIONS**

The chapter has provided some evidence that the main causes of Ponzi scheme formation are low level of financial literacy among the general population, relative ignorance of authorities about such schemes and lack of viable investment alternatives due to underdeveloped financial infrastructure. Firstly, improving financial literacy of the general public plays a vital role in reducing the negative impact of Ponzi schemes and other financial frauds. Therefore, the main solution against Ponzi scheme is undeniably to raise investors' financial literacy to prevent them from joining such schemes. People who are financially literate are generally better protected against financial risks and troubles. It makes them more responsible about their personal financial decisions which at the same time help them to improve their economic welfare through correct distribution of financial resources. Financially literate people also have better financial behaviour, which helps them in diversifying their financial investments as well as in making sound financial planning for the future. Financial safety of the general public is improved in societies with higher level of financial knowledge and at the same time contributes to economic sustainability (Filippova *et al.*, 2016; Mandell, 2009).

In addition to financial literacy, the level of financial developments is also important to prevent the formation of Ponzi schemes. Some economic research indicate close relationship between the two and income distribution. According to Lo Prete (2013), higher level of financial literacy boosts the impact of financial development and reduces economic inequality. The work of Grohmann *et al.* (2018) finds that while financial development can improve financial inclusion, higher degree of financial literacy strengthens its effect in terms of financial depth. It also suggests that financial infrastructure and financial literacy can substitute each other with respect to access to finance. In other words, people with higher level of financial literacy living in places with underdeveloped financial infrastructure have about the same level of access to finance, as someone with lower level of financial literacy living in a place with more advanced financial infrastructure. This indicates that both financial development and financial literacy are important, but lack of one does not necessarily handicap a person's access to finance. According to Lo Prete's (2013) findings, the existence of both can complement each other in terms of enhancing financial inclusion and reducing economic inequality. In fact, findings of the Russia Diagnostic Review point out that the on-going problems of financial pyramids undermine public confidence in financial markets. However, when Russian households with interest to obtain financial education were asked about what motivated them, majority answered that it was to protect their rights and to avoid involvement in financial pyramids (Rutledge, 2010).

When it comes to preventive measures against formation of Ponzi schemes, both depth of financial system and its development play important roles. According to Lewis (2015), even if the victims of Ponzi schemes are main parties to be blamed, the main reason for them falling victims to the schemes



is their attempt to make personal investment and retirement decisions without referring to financial consultants. He believes that financial regulations should be in place to ensure transparency of financial intermediaries. In the case of the CIS countries, people mainly invested in Ponzi schemes mainly due to lack of legitimate investment funds with transparent reporting of their activities. Development of financial infrastructure and accompanying regulations should thus assist in the prevention of Ponzi schemes. This requires regulators and government monitors to be trained better and to have adequate financial knowledge. General awareness trainings about such schemes and other possible financial frauds (Khan *et al.*, 2020), as well as improving financial literacy levels of government officials are crucial to identify such schemes in a timely manner to avert further harm to the society.

To date, there have been some legislative moves in some CIS countries to formally penalise and ban Ponzi type of financial pyramid schemes. For instance, in November 2013, the Verkhovna Rada (i.e. parliament) of Ukraine passed a law drafted on behalf of President Viktor Yanukovich to ban financial pyramids. According to this legislation, the organisers of either physical or virtual financial pyramids will be penalised with fines from 1.7 to 3.4 thousand hryvnias (\$200 to \$300) and can be imprisoned for a term of three to eight years. If there are several organisers or the harm to people was substantial, the punishment to the offenders could be more severe (Kozachenko *et al.*, 2017). Similarly, Federal Law No. 78-FZ dated 30 March 2016 “On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Code of Criminal Procedure of the Russian Federation” was signed by the President of the Russian Federation V.V. Putin. According to Article 172.2 of the Criminal Code, the organisation of pyramids is punishable with a fine of up to 1 million rubles or imprisonment up to five years. However, if the crime involved large amounts, the punishment extends to a fine of up to 1500 thousand rubles or imprisonment for up to six years (Anzhu & Pshenichnikov, 2017). Similar measures are also being taken in other CIS countries.

The danger of Ponzi schemes is in fact increasing with the emergence of financial technology (Fin-Tech) which is resulting in greater financial deregulation (DeFi) of online transactions. The emergence of crypto assets and currencies in particular, are leading to new forms of Ponzi schemes gaining momentum. In one of the cases in early 2010s, *SEC vs. Shavers*, a Ponzi scheme called Bitcoin Savings and Trust (BTCST) was formed by Trendon T. Shavers and advertised as a Bitcoin “investment opportunity”. The scheme promised investment returns as high as 7% per week while funds in Bitcoins were expected to be used for Bitcoin arbitrage opportunities. As in any Ponzi scheme, new cryptocurrency investments were used to pay promised returns to existing investors and the remaining would be spent to pay the organiser’s personal expenses (SEC, 2013b). In a more recent case, another Ponzi scheme was formed under the name BitClub Network which promised investors to profit from Bitcoin mining, where raised funds were supposed to be invested in the acquisition of necessary hardwares to solve complicated math algorithms in the mining process. Five scheme organisers who defrauded investors of \$722 million are facing trials in New Jersey for conspiring to sell unregistered securities to investors, as the sold investment certificates were not registered with the U.S. Securities Exchange Commission (SEC) (Levenson, 2019).

Such ‘Smart Ponzi Schemes’ using crypto assets and blockchain technology can be detected and prevented at an early stage. A research work by Chen *et al.* (2019) suggests a three steps approach to detect such Smart Ponzis. The first approach is to study the common features of such schemes for comparison and generalisation, and are used to analyse all open smart contracts to detect ones which match those features. The authors used the proposed approach and estimated that more than 500 smart Ponzi schemes are running on Ethereum. They recommend building a standardised platform to assess and scrutinise each smart contract as early warning signals of financial scams.

In summary, several policy recommendations can be offered in this chapter to prevent financial frauds. Firstly, it is important to improve financial education by instilling it into the education system as early as possible. Secondly, it is necessary to develop proper financial infrastructure that can increase the variety of investment alternatives. This includes enhancing financial regulation to consider new developments in the financial industry such as the introduction of crypto assets and cryptocurrencies. Given that Ponzi schemes using crypto assets is growing in popularity, the CIS governments can learn from the preventive measures taken by the SEC of United States to curb their formation. In the United States, irrespective of the currency used for investment (U.S. dollars, foreign or virtual currency), all investments in securities are subject to the SEC regulation. Any individual selling investment certificates also has to follow the licensing requirements either at federal or state level (SEC, 2013a). Similarly, Rutledge (2010) suggests that the securities supervisory agency should have broad powers to investigate any suspicious schemes to assist the criminal authorities in their prosecution. Solicitors of any public investment funds should also be required to obtain a license, thus the securities supervisors would be able to investigate any scheme that appears to be illegitimate.

Thirdly, it is crucial to train government authorities who are responsible to develop financial infrastructures and control the transparency as well as legitimacy of financial contracts. In particular, to increase the financial knowledge of legislators and staff of regulatory institutions. Without the skills and competencies to distinguish a genuine investment from a financial pyramid scheme, government officials may at times misguide the general public by approving such schemes either officially or unofficially. For instance, if there is official registration of the Ponzi scheme Sattylyk by the Justice Ministry in Kyrgyzstan, on the other hand, collaboration of the Chinaz district officials with Ahmadboi deems it as an unofficial legitimisation. Therefore, if officials become aware of the illegitimacy of such schemes, they would be more wary of associating themselves with such schemes and undertake greater scrutiny before approving their official registration. In the same vein, there is a need to form proper laws in all CIS countries which should stipulate legal penalties for financial frauds in both physical and virtual forms.

Finally, as Amoah (2018) recommends, financial market regulators should be more proactive by intensifying awareness on Ponzi schemes and collaborating with the Ministry of Education to provide it through financial literacy courses. They should also assist non-formal education centres such as adult and distance education providers to include financial literacy elements in their course syllabus, with Ponzi schemes being an integral part. Overall, active involvement of market and government participants such as financial planners, auditors, accountants, securities agencies and financial consultants is important to provide information about any Ponzi schemes or other similar suspicious activities to government agencies. Therefore, respective authorities should create greater awareness to the public on phone hotlines and websites that are available for them to report such activities, while ensuring the confidentiality of informants.

## **FUTURE RESEARCH DIRECTIONS**

This chapter tried to study reasons behind the formation of Ponzi schemes in the CIS countries and provided some general recommendation as solutions for the problem. Limited analysis of financial development and level of financial literacy indicate that each country in the CIS differ in both aspects. Additional research is required for each CIS member country to better understand the matter and to provide more specific recommendations. Given the possible cultural differences among the member countries, it can

be assumed that the underlying conditions may be different for the reasons behind the Ponzi scheme formation in each country. A separate study is required to analyse the relationship between Ponzi schemes and effects of national culture on financial decision making, which can provide some interesting results.

One limitation of this chapter relates to the qualitative nature of the research. Nevertheless, if quantitative methods can verify the analysis of the effect of financial literacy and financial development on Ponzi scheme formation, it could be supportive of this chapter's findings. It can also assist us to understand if there is a cause-effect relationship between those factors and Ponzi schemes in CIS countries. Latest literature in the field has also shed light on the behavioural finance aspect of Ponzi schemes. The scheme organisers are generally found to be skilled con artists who are able to manipulate investors' emotions, forcing them to make decisions which contradict logic or rationality. The economic behaviour of investors can thus be closely studied in the case of Ponzi schemes in the CIS. Such study would definitely complement the quantitative studies conducted in this chapter.

Some latest research use the greed-based economy theory as a new approach to the problem. For some reason, the greedy behaviour of both scheme masters and potential investors seem to complement each other in laying strong foundation for Ponzi schemes. If one further adds the corrupted behaviour of some government agents, it would make up a perfect recipe for systematic failure of the financial system. Despite the inclusion of some of these aspects in parts of the studied cases in this chapter, the author avoided focusing on them as they deviate from the chapter's scope. Therefore, the effect of economic and behavioural immorality on development of Ponzi schemes need to be further examined for CIS countries.

## **CONCLUSION**

This chapter discussed the impact of financial literacy and financial development on formation of Ponzi schemes, more specifically in the Commonwealth of Independent States (CIS) countries. The transition from planned to market economy in the initial years of independence was not an easy period for the majority of financially illiterate population of the CIS countries. The period was also characterised by low level of financial sector development and abundant Ponzi schemes in most CIS countries. Such schemes continued to appear in one form or another for many years later, which the author believes was mainly due to the underdeveloped finance industry and lack of financial literacy among the general public.

In studying several cases from the CIS countries, the findings of the chapter show that all of the hypotheses brought forward seem to hold. More specifically, most studied cases showed that lower level of financial literacy in the CIS countries motivated con artists to develop Ponzi schemes. Most schemes also continued to operate undetected for a long time due to the authorities' unfamiliarity with such schemes. Last but not least, underdeveloped financial sectors in most CIS member states led to the unavailability of viable investment alternatives, making Ponzi schemes an attractive option to ordinary citizens. These three factors play important roles in making the CIS countries a fertile ground for the formation and growth of Ponzi schemes.

Improving financial education and instilling it into the education system as early as possible is suggested as the first crucial step to ease the problem. This will to a certain degree address financial illiteracy among the population, thus reducing the frequency and extent of various financial frauds in the CIS countries. In developed countries, financial literacy plays an important role to help the society make correct investment decisions. Without proper financial education, people tend to make irrational decisions such as investing in Ponzi schemes, despite being suspicious of their fraud elements. A finan-

cially literate person is less likely to become a victim of financial frauds (Behrman *et al.*, 2012; Kefela, 2010; L. Mandell & Klein, 2009).

It is essential to note that development of financial infrastructure (especially financial markets and regulations) does not only serve to reduce financial crimes in the form of Ponzi schemes, but can also serve to enhance economic development. Nonetheless, most CIS countries generally maintained the main financial heritage of the Soviet Union in the form of pre-existing banking systems. In a study by Cojocaru *et al.* (2016) on post-Soviet countries (including CIS countries), they found that financial system efficiency and its competitiveness are more important for economic development of a country as compared to the amount of credit provided to the private sector. Their findings have shown that financial efficiency (measured as credit spread or bank overhead cost) is very important for the economy of the studied countries.

This chapter cannot be considered as a comprehensive study of the broad research field of Ponzi schemes since it is mainly limited to the CIS countries. However, the author believes it serves as a general preliminary study of the historical development of Ponzi schemes in these countries. There are many aspects of Ponzi schemes research which require detailed scrutiny, particularly in the present era of digital finance, crypto assets and cryptocurrencies that have expanded the playing field for con artists of Ponzi schemes. This should not discourage authorities neither in the CIS countries or other developing ones from fighting against such financial crimes and taking preventive measures, which include instilling financial education, market transparency and proper regulation. It is crucial for all legislators, regulators and prosecutors to have adequate financial knowledge to be able to distinguish genuine investment schemes from fake ones. The respective governments should therefore place greater emphasis in raising the level of financial literacy of individuals in the top ranks of the authority.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in his personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## REFERENCES

- Amoah, B. (2018). Mr Ponzi with Fraud Scheme Is Knocking: Investors Who May Open. *Global Business Review*, 19(5), 1115–1128. doi:10.1177/0972150918788625
- Andreff, W. (2019). The unintended emergence of a greed-led economic system. *Kybernetes*, 48(2), 238–252. doi:10.1108/K-01-2018-0018
- Anzhu, A. A., & Pshenichnikov, V. V. (2017). Phenomenon of financial pyramids: Nature and design. *Advances in Economics. Business and Management Research*, 38, 13–19. doi:10.2991/ttiess-17.2017.3
- Aris, B. (2011). *Russia: Where Ponzi schemes roam*. Financial Time. Retrieved from <https://www.ft.com/content/cd31ca25-cf99-3df7-bc0a-dcb73ea2bdb9>
- Arminfo. (2013). *Revived Russian Ponzi scheme, MMM, reaches Armenia*. <https://arminfo.info/index.cfm?objectid=34A68750-ED58-11E2-A1560EB7C0D21663>
- Azim, M., & Azam, M. (2016). Bernard Madoff's "Ponzi scheme": Fraudulent behaviour and the role of auditors. *Accountancy Business and the Public Interest*, 15, 122–137.
- Behrman, J. R., Mitchell, O. S., Soo, C. K., & Bravo, D. (2012). How financial literacy affects household wealth accumulation. *The American Economic Review*, 102(3), 300–304. doi:10.1257/aer.102.3.300 PMID:23355747
- Bhattacharya, U. (2003). The optimal design of Ponzi schemes in finite economies. *Journal of Financial Intermediation*, 12(1), 2–24. doi:10.1016/S1042-9573(02)00007-4
- Chen, W., Zheng, Z., Ngai, E. C. H., Zheng, P., & Zhou, Y. (2019). Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum. *IEEE Access: Practical Innovations, Open Solutions*, 7, 37575–37586. doi:10.1109/ACCESS.2019.2905769
- Cojocaru, L., Falaris, E. M., Hoffman, S. D., & Miller, J. B. (2016). Financial System Development and Economic Growth in Transition Economies: New Empirical Evidence from the CEE and CIS Countries. *Emerging Markets Finance & Trade*, 52(1), 223–236. doi:10.1080/1540496X.2015.1013828
- De Koker, L. (2012). *Pyramids and Ponzis: Financial Scams in Developing Countries*. CGAP. Retrieved from <https://www.cgap.org/blog/pyramids-and-ponzis-financial-scams-developing-countries>
- EurasiaNet. (2016a). *Uzbekistan: Officials Fired Over Pyramid Scheme*. EurasiaNet.Org. Retrieved from <https://eurasianet.org/uzbekistan-officials-fired-over-pyramid-scheme>
- EurasiaNet. (2016b). *Uzbekistan Arrests Its Own Bernie Madoff*. EurasiaNet.Org. Retrieved from <https://eurasianet.org/uzbekistan-arrests-its-own-bernie-madoff>
- EurasiaNet. (2018). *Kyrgyzstan: The Ponzi that Broke a Village* | Eurasianet. EurasiaNet.Org. Retrieved from <https://eurasianet.org/kyrgyzstan-the-ponzi-that-broke-a-village>
- Fei, L., Shi, H., Sun, X., Liu, J., Shi, H., & Zhu, Y. (2020). The Profile of Ponzi Scheme Victims in China and the Characteristics of Their Decision-making Process. *Deviant Behavior*, 00(00), 1–14. doi:10.1080/01639625.2020.1768639

Filippova, T. V., Kashapova, E. R., & Nikitina, S. S. (2016). Financial literacy as a key factor for an individual's social and economic well-being. *EDP Sciences*, 28, 5. Retrieved from <http://earchive.tpu.ru/handle/11683/33078>

Frankel, T. (2012). *The Ponzi scheme puzzle: a history and analysis of con artists and victims*. Oxford University Press. doi:10.1093/acprof:osobl/9780199926619.001.0001

Grohmann, A., Klühs, T., & Menkhoff, L. (2018). Does financial literacy improve financial inclusion? Cross country evidence. *World Development*, 111, 84–96. doi:10.1016/j.worlddev.2018.06.020

Hess, S., & Soltes, E. (2018). *MMM and bitcoin: Russian Ponzi mastermind Sergei Mavrodi is dead, but his legacy lives on in crypto* — Quartz. Quartz. Retrieved from <https://qz.com/1259524/mmm-and-bitcoin-russian-ponzi-mastermind-sergei-mavrodi-is-dead-but-his-legacy-lives-on-in-crypto/>

IMF. (2009). *IMF Survey: IMF Advice Helps Fight Financial Fraud as Schemes Multiply. Pyramid, ponzi schemes*. International Monetary Fund. Retrieved from <https://www.imf.org/en/News/Articles/2015/09/28/04/53/sopol021209a>

JMKR. (2020). *Электронная база данных юридических лиц, филиалов (представительств)*. Justice Ministry of Kyrgyz Republic. Retrieved from <https://register.minjust.gov.kg/register/Public.seam?publicId=445887>

Kefela, G. T. (2010). Promoting access to finance by empowering consumers-Financial literacy in developing countries. *Educational Research Review*, 5(5), 205–212. <http://www.academicjournals.org/ERR>

Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2

Kozachenko, I. Y., Gubareva, A., & Kovalenko, K. (2017). International popularization of financial pyramids: Theoretical and practical aspects. *Universidad y Sociedad*, 9(2), 261–264. <https://rus.ucf.edu.cu/index.php/rus>

Kruglikov, K., & Coalson, R. (2020). *Building A Fortune On Misfortune: Pyramid Schemes Still A Bane In Russian Hinterland*. RFE/RL's Russian Service. Retrieved from <https://www.rferl.org/a/russia-pyramid-schemes-veliky-ustyug-putin/30436190.html>

Levenson, M. (2019, December 11). 5 Charged in New Jersey in \$722 Million Cryptocurrency Ponzi Scheme. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/12/11/us/cryptocurrency-ponzi-scheme-nj.html>

Lewis, M. K. (2015). *Understanding Ponzi schemes: can better financial regulation prevent investors from being defrauded?* Edward Elgar Publishing Ltd., doi:10.4337/9781782549109

Lo Prete, A. (2013). Economic literacy, inequality, and financial development. *Economics Letters*, 118(1), 74–76. doi:10.1016/j.econlet.2012.09.029

Mandell, L. (2009). The Impact of Financial Education in High School and College On Financial Literacy and Subsequent Financial Decision Making. *The American Economic Association Meetings*, 1–38. Retrieved from <https://www.aeaweb.org/conference/2009/retrieve.php?pdfid=507>

- Mandell, L., & Klein, L. S. (2009). The impact of financial literacy education on subsequent financial behavior. - PsycNET. *Financial Counseling and Planning*, 20(1), 15–24. <https://psycnet.apa.org/record/2009-19876-001>
- Nikolova, M. (2017). *A new financial pyramid emerges in Russia every 48 hours*. FinanceFeeds. Retrieved from <https://financefeeds.com/new-financial-pyramid-emerges-russia-every-48-hours/>
- OECD. (2018). *Levels of Financial Literacy in Eurasia*. Organisation for Economic Co-operation and Development. Retrieved from <https://www.oecd.org/education/financial-education-cis.htm>
- Papava, V. (2013). Reforming of the Post-Soviet Georgia's Economy in 1991-2011. *SSRN Electronic Journal*, 1–152. doi:10.2139ssrn.2291142
- Patsuria, N. (2012, December 12). Center Point Group's Vast Ponzi Scheme. *Georgian Journal*. Retrieved from <https://www.georgianjournal.ge/business/21413-center-point-groups-vast-ponzi-scheme.html>
- Rafay, A. (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5
- RFE/RL's Uzbek Service. (2018). *Uzbek Financier Jailed For Pyramid Scheme*. Radio Free Europe / Radio Liberty' Uzbek Service. Retrieved from <https://www.rferl.org/a/uzbekistan-pyramid-schemer-jailed/29056501.html>
- Rutledge, S. L. (2010). *Consumer Protection and Financial Literacy: Lessons from Nine Country Studies* (No. 5326; Policy Research Working Paper, Issue June). <http://econ.worldbank.org>
- SEC. (2013a). Ponzi schemes using virtual currencies. In *Investor Alert: Vol. N.153-7/13*. U.S. Securities Exchange Commission. Retrieved from [https://www.sec.gov/files/ia\\_virtualcurrencies.pdf](https://www.sec.gov/files/ia_virtualcurrencies.pdf)
- SEC. (2013b). *SEC Charges Texas Man with Running Bitcoin-Denominated Ponzi Scheme*. U.S. Securities Exchange Commission. Retrieved from <https://www.sec.gov/news/press-release/2013-132#.Ue6yZODmp-I>
- Sloane, W. (1994). Firm Offers Public Huge Returns, But Government Calls it Illegal. *The Christian Science Monitor*. Retrieved from <https://www.csmonitor.com/1994/0728/28091.html>
- Tennant, D. (2011). Why do people risk exposure to Ponzi schemes? Econometric evidence from Jamaica. *Journal of International Financial Markets, Institutions and Money*, 21(3), 328–346. doi:10.1016/j.intfin.2010.11.003
- The World Bank. (2020). *World Development Indicators*. DataBank. Retrieved from <https://databank.worldbank.org/source/world-development-indicators#>
- TI. (2012). *Center Point Group – Georgia's Biggest Construction Scandal*. Transparency International.
- Tolstikova, N. (1999). *Mmm As a Phenomenon of the Russian Consumer Culture*. ACR European Advances, E-04. <https://www.acrwebsite.org/volumes/11384/volumes/e04/E-04/full>
- Trahan, A., Marquart, J. W., & Mullings, J. (2005). Fraud and the American dream: Toward an understanding of fraud victimization. *Deviant Behavior*, 26(6), 601–620. doi:10.1080/01639620500218294

UNECE. (2003). Progress in Systemic Reforms in the CIS. In *Economic Survey of Europe* (pp. 123–154). United Nations Economic Commission for Europe.

Witt, H. (1994). Russian investors entered stock scheme with eyes wide open. *Chicago Tribune*. Retrieved from <https://www.chicagotribune.com/news/ct-xpm-1994-07-31-9407310366-story.html>

Younas, K., & Rafay, A. (2021). (Forthcoming). Women entrepreneurship and financial literacy - Case of female borrowers in Pakistan. *Iranian Economic Review*.

## **ADDITIONAL READINGS**

Ferguson, S. (2019). *Five Charged in \$722 Million Cryptomining Ponzi Scheme*. Bank Info Security. <https://www.bankinfosecurity.com/five-charged-in-722-million-cryptomining-ponzi-scheme-a-13490>

Karnani, A. G. (2011). Mirage at the Bottom of the Pyramid. *SSRN Electronic Journal*. doi:10.2139ssrn.924616

Nesvetailova, A. (2007). Ponzi Capitalism Russian-style. In *Fragile Finance* (pp. 105–127). Palgrave Macmillan UK. doi:10.1057/9780230592308\_8

Radaev, V. (2000). Return of the Crowds and Rationality of Action: A history of Russian “financial bubbles” in the mid-1990s. *European Societies*, 2(3), 271–294. doi:10.1080/146166900750036286

Schiffauer, L. (2018a). Dangerous speculation: The appeal of pyramid schemes in rural Siberia. *Focaal: Tijdschrift voor Antropologie*, 2018(81), 58–71. doi:10.3167/fcl.2018.810105

Schiffauer, L. (2018b). Let’s get rich: Multilevel marketing and the moral economy in Siberia. *Critique of Anthropology*, 38(3), 285–302. doi:10.1177/0308275X18775207

Shelley, L. I. (1995). Privatization and Crime: The Post-Soviet Experience. *Journal of Contemporary Criminal Justice*, 11(4), 244–256. doi:10.1177/104398629501100405

Walsh, J. (1998). *You Can’t Cheat an Honest Man: How Ponzi Schemes and Pyramid Frauds Work... And Why They’re More Common Than Ever*. Silver Lake Publishing.

## **KEY TERMS AND DEFINITIONS**

**CIS Countries:** The member states of the Commonwealth of Independent States (CIS), a regional intergovernmental organisation which combined 12 member states which were once part of former USSR. Georgia withdrew from the organisation in 2008, leaving only 11 countries as members of the CIS.

**Crypto Currency:** A digital currency that uses cryptographic technology to hide the identity of the owner as well as transactions for which the currency is used.

**Financial Literacy:** The measure of an individual’s or society’s understanding of financial knowledge to make correct investment and financing decisions. It can also cover other measures such as components of financial behaviour or attitude.



**Financial Sector Development:** Development of financial institutions, instruments, markets and the legal and regulatory framework that permit cost efficient execution of transactions to assist investment and financing activities.

**Investment Decision:** A person's action with respect to making investment choices from the alternatives that are available for the individual.

**Market Economy:** An economic system where prices and distribution of resources are determined with respect to demand and supply of market participants. Individual property rights as well as freedom of economic choices are distinct aspects of a market economy.

**Planned (Command) Economy:** An economic system where decisions about pricing, consumption and distribution of economic resources are made by the central government. Factors such as public welfare and income equality, along with even distribution of resources take precedence over individual economic freedoms and property rights in a command economy.

**Ponzi Scheme/Financial Pyramid:** A financial scheme where contributions of the later investors are used to fund the dividends of the earlier ones, with the scheme organisers benefitting the most. The con artist in the scheme plans to expand the scheme as much as possible until new funds dry up, and the scheme collapses.

## ENDNOTE

- <sup>1</sup> Georgia is included in the analysis of this chapter even if it is no longer considered as a member of the CIS. Georgia withdrew from the commonwealth on 13 August 2008 as a result of the Russo-Georgian War. However, the author believes inclusion of Georgia in this study even though it is now not part of the CIS is justified since it was part of the union for most of its independence. Also, due to strong similarity of its economy with other member states of the CIS, and the fact that the studied case took place during its membership, most of the analysis derived are relevant to the objective of this study.

# Chapter 16

## Frauds in Unorganized Investment Schemes: The Case of India

**Narendra S. Bohra**

*Graphic Era University, India*

**Mahak Sethi**

*Graphic Era University, India*

### ABSTRACT

*Innumerable unorganized collective investment schemes' fraud cases have surfaced over time in India. However, there exists minimal descriptive literary text divulging these scams and frauds, which have drowned away the hard-earned money of millions of people. This chapter has been contributory in identifying the working models, administration, and organization of unorganized collective investment schemes (UCIS), where UCIS frauds remain the keystone of groundwork concerning the cases that have transpired over the last decade in India. The chapter aims to interpret the UCIS working models concerning UCIS fraud cases in India by exploring the various models of frauds adopted by UCIS organizers.*

### 1. INTRODUCTION

Network marketing or direct selling techniques have captured great attention, in less than two decades; it has provided huge self-employment opportunities and is now perceived to provide scope for creating self-dependencies especially for women (Bhattacharjee, 2016). Unorganized Collective Investment Scheme (UCIS) associations are similar to network marketing associations and “word of mouth” (WOM) is the biggest tool of success for such associations. Investor’s decisions are vigorously influenced by WOM since people undoubtedly trust their peers and relatives-the social network, in fact, these human tendencies are so strong that they are codified as a marketing strategy called “word-of-mouth” marketing (Trusov, Bucklin & Pauwels, 2009). WOM marketing strongly influences what people know, feel, and do and therefore, has a powerful effect on behavior (Buttle, 1998). WOM tends to be an efficient tool

DOI: 10.4018/978-1-7998-5567-5.ch016

for UCIS marketers in view of the fact that it produces low cost on their part and effective for the reason that it yields widespread payoffs. Significant media coverage on UCIS frauds in the last one decade in India led us to the selection of this problem for our study.

## **1.1 Objective of the Study**

The purpose of this study is to interpret *UCIS working modes* in relation to UCIS fraud cases in India by exploring the various models of frauds adopted by UCIS organizers. A critical examination of trapped UCIS investors' demographics is also proposed in this chapter.

## **2. BACKGROUND**

Innumerable dubious schemes have floated in India since decades proclaiming stellar returns. Many times, these entities get registered under companies act to gain investors' trust by depicting to be under the government's supervision. The Saradha Group financial scandal which had over 100 firms registered with the Registrar of companies made headlines in 2013 for duping 1.7 million investors with its multi-crore Ponzi scheme. Agents were hired to collect money from the investors & in turn, were promised commission ranging from 15-20 percent. Stellar returns such as a flat or a piece of land in return became key contributors that pulled investors to this fraud (Farooqui & Nisa, 2017). Abnormally high guaranteed returns become the key factor that attracts investment from the less aware public. However, when the occasion for fulfilling promises comes, these entities vanish into thin air. The conventional definition of a CIS is "an arrangement whereby a group of investors pools in a definite sum of money with a CIS manager, who in turn invests this corpus for the purpose of generating returns which are then distributed back to the investors in the proportion of their invested sum". The Securities and Exchange Board of India (SEBI) defines CIS as any scheme or arrangement, which satisfies the conditions of subsection (2) of section 11AA of the SEBI Act and covers any scheme or arrangement made or offered by any company under which the contributions, or payments made by the investors, are pooled and utilized with a view to receive profits, income, produce or property, and is managed on behalf of the investors. Investors do not have day-to-day control over the management and operation of such schemes or arrangements (Dhar, 2012). They are organized schemes which are managed by a collective investment management company which is incorporated under the provisions of the Companies Act, 1956 and registered with SEBI under the SEBI (Collective Investment Schemes) Regulations, 1999. As per SEBI act, 1992, section 11AA (3) CIS includes those schemes under which deposits are acknowledged under section 74 of the Companies Act, 2013. It is obligatory that every CIS must be registered as per CIS regulations. Only a Collective Investment Management company that has obtained a registration certificate under CIS regulations shall carry on, sponsor, or launch a CIS. CIS differs in terms of their legal form despite the fact that they are shared investment arrangements. Thompson & Choi, (2001) stated legal forms Collective Investment Schemes (CIS): First is the corporate form: The investors act as shareholders and the CIS association is deemed to be a separate corporate entity. Second is the trust form: as the name suggests, the CIS association is established as a trust and third is the contractual form: Under this, the functioning of CIS is similar to that of a contract where the funds of investors are managed by a CIS manager.

## **2.1 The Ecosystem and Legal Framework of UCIS**

In this chapter, we define UCIS as an umbrella term that includes all those financial schemes that collect deposits or invites subscriptions from the general public, without having authorization & consent from SEBI and one that does not satisfy the conditions of subsection (2) of section 11AA of the SEBI act. These schemes are neither regulated nor approved by any regulatory body. Absence of supervision and control on such associations contributes to a compounding number of frauds in all organization (Khan, Rafay & Shakeel, 2020). The same is true for the unorganized sector that enormously affects growing economies. Judiciary control by RBI, SEBI, or any other supreme body stands absent; therefore, these associations take advantage of the loopholes in the legal system. The regulatory authorities come into play only when the scam surfaces. West Bengal's Rose Valley scam of 2013 is one such financial scandal worth Rs 17000 crore. The operations of the Rose Valley group went unnoticed & were overlooked until The Saradha Group financial scandal of 2013 unveiled. It was only after this scam that the Supreme Court probed into the operations of The Rose Valley group. The legal authorities then became cognizant of the fact that the sister concerns of the group were illegally collecting deposits from small investors promising lofty returns. In India, UCIS takes up the form of Kitties, committees, and other similar unregulated bogus schemes. Kitty is the most famous form of UCIS. A Kitty is an amount of money that is made up of small amounts given by different people, used by them for an agreed purpose (Cambridge English Dictionary). To create a large pool of Kitty members, Kitty associations organize kitty parties in which an informal gathering, especially of middle-class women, are invited and unofficial savings schemes (neither regulated nor approved) are offered, where individual participants contribute a predetermined sum of money to form a huge corpus, known as kitty, which is then paid to a single participant on the basis of chit system by the kitty organizer, also known as the kitty host. Based on their form of organization as social gatherings they are referred to as 'Kitty Parties'. The proportion of women is high in such parties, who pool in a certain amount every month, which is auctioned or given in full through a draw of lots. It is an extravagant affair for women in India to socialize and it is popular amongst middle-income urban women (Sethi, Ardener & Burman, 1995). The new Indian middle class incorporates an educated and well-qualified group of people, aspiring to live a privileged life, owing to proliferation in status and reputation (Mathur, 2010). The basic rationale behind joining a kitty party is to fraternize with other members of similar age. For Homemakers, who literally have no time for themselves, UCIS such as Kitty parties are the only source of merriment. In addition to merriment, these schemes allow rotation of savings from one member to another that supports the homemakers to finance their needs of consumer durables. In view of the fact that Kitty associations are informal groups and offer an unofficial collective investment savings scheme, where the agreements passed between members are not governed by any statutory force, the members, thus, have no legal means of enforcing such agreements. The involvement of banks, issuing authority, government, or any other regulatory body stands absent, the terms and conditions of such associations, therefore, have no legal binding on the members.

Levi, M (2008) examined the backdrop of frauds in frame of reference to organized crimes. This study explicated the organization of frauds and securitizes the victim-centric typology of fraud. A threefold typology of frauds was elucidated in *The Phantom Capitalists* (Levi, 2008, originally 1981), where the following classification was put forward:

1. Pre-planned frauds, in which the business scheme is set up from the start as a way of defrauding victims (businesses, public sector, and/or individuals)

2. Intermediate frauds, in which people started out obeying the law but consciously turned to fraud later; and
3. Slippery-slope frauds, in which deceptions spiraled, often in the context of trying-however absurdly and over-optimistically-to rescue an insolvent business or set of businesses that in reality had no hope of repaying its debts in the future.

In context to Levi's work, UCIS frauds can be classified as pre-planned frauds or organized crime, where the organizer precontrives a strategy, that tempt people at large to put their hard-earned money in the irresistible schemes of the organizer. During the initial stages, a false image depicting a flourishing business is communicated to increase the member base. It is on the later stages when the fallacious image is unveiled, with delayed payments and intentional deception. Technology has also aided the UCIS organizers to fabricate their false identities to defraud the public at large.

## **2.2 Reasons Behind Successful Operations of UCIS**

Regulatory helplessness and inadequacy of the administration's supervision is one reason behind successful operations of UCIS associations. The absence of alert and diligent supervision lends a helping hand to such entities in exploiting the loopholes of the legal system.

Besides, the tactic of Multilevel Marketing (MLM) is illegitimately used with the help of Pyramid schemes (see figure 2) to build a gigantic member base that reckons continuity of operations. Exponential growth in the scheme is visible till the time new entrants are enrolled (Drew & Drew, 2010).

Lack of knowledge about safer and legal investment options, information insufficiency and awareness absenteeism make investors credulous and thereby promotes the progression of such schemes. The persistence of Financial illiteracy among a large number of investors opens the door for financial fraud because these investors are effortlessly influenced by too good to be true returns (Gui, Huang, & Zhao, 2020).

Under penetration of banking services in tier II & tier III towns in India is one factor that has added to the growth and uninterrupted flow of UCIS. These associations target those individuals who are outside the formal banking system and do not have access to banking and social welfare schemes. (Tiwari, Anjum, Chand, & Pathak, 2017; Rafay, Farid, Yasser & Safdar, 2020). False and fascinating claims attract uninformed investors towards such schemes.

## **3. METHODOLOGY**

A pragmatic approach has been adopted to rationalize how UCIS chains are configured & how the financially literate public is defrauded. To bolster our research scope, we constellated information of UCIS fraud cases that have come into sight in India post-2009. The chapter of the book presents 17 UCIS fraud cases (see Table 1) that have transpired in India post-2009. The primary data concerning the operational mechanism of UCIS have been obtained by interviewing the Victim Investors (VI), a total of 1000 VI were approached, out of which 400 individuals responded, a few were reluctant to share information about their investments.

## Frauds in Unorganized Investment Schemes

Table 1. UCIS Frauds in India

S.No	Name of UCIS Organizer	UCIS Type	Amount (Rs)
1.	Goodwin Jewelers, Maharashtra. (2019) <sup>1</sup>	Ponzi Scheme	25 Cr.
2.	Sudha & Ritu Agarwal, Uttarakhand (2019) <sup>2</sup>	Kitty	9 Lakhs
3.	JPV Capital, Gujarat (2019) <sup>3</sup>	Ponzi Scheme	3.5 Cr.
4.	Galaxy Enterprises, Uttar Pradesh (2019) <sup>4</sup>	Ponzi scheme	7.8 Cr.
5.	Gurukripa Kitty Dehradun, Uttarakhand (2019) <sup>5</sup>	Kitty	1.5 Cr.
6.	Triporf Trading Services Pvt. Ltd, Bengaluru (2018) <sup>6</sup>	Ponzi Scheme	77 Cr.
7.	Shivangi Tripathi, Uttarakhand (2018) <sup>7</sup>	Kitty	5 Cr.
8.	Shubh Shakti Cooperative Society Pune (2017) <sup>8</sup>	Ponzi Scheme	22 Cr.
9.	GIG Kitty Party, Uttarakhand (2017) <sup>9</sup>	Kitty	50 Cr.
10.	Thapar Case, Uttarakhand (2017) <sup>10</sup>	Kitty	4.5 Lakh
11.	Balwinder Kaur, Haryana (2017) <sup>11</sup>	Kitty	40.52 Lakh
12.	Datum Marketing Limited, Odisha (2016) <sup>12</sup>	Ponzi Scheme	60 Cr.
13.	Shri Balaji Traders Uttarakhand (2016) <sup>13</sup>	Kitty	12 Cr.
14.	Jindal & Chauhan Case, Punjab (2016) <sup>14</sup>	Gold & Diamond	1.47 Cr.
15.	Sadhna Sanjay Jain, Delhi (2015) <sup>15</sup>	Small Savings Scheme	3 Cr.
16.	Ashok Jadeja, Gujarat (2014) <sup>16</sup>	One-time Scheme	25 Cr.
17.	Annu Bajaj Case, Delhi (2011) <sup>17</sup>	Kitty	50 Cr.

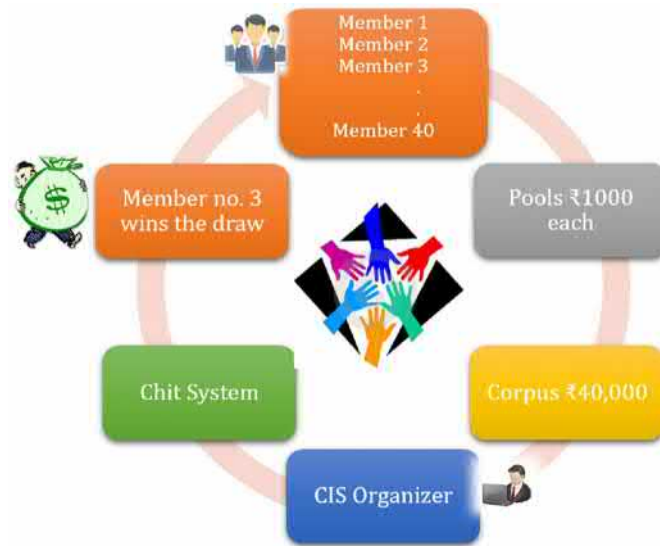
## 4. FUNCTIONING OF AN UNORGANIZED COLLECTIVE INVESTMENT SCHEME (UCIS)

Rotating Savings and Credit Associations (ROSCA) are among the oldest and most prevalent savings institutions found in the world and play an important role in savings mobilization in many developing economies. Each type of ROSCA allows individuals without access to credit markets to improve their welfare, but under a reasonable assumption on preferences, random allocation is preferred when individuals have identical tastes (Besley, Coate, & Loury, 1993). Economic theories suggest that individuals join ROSCA to finance the purchase of lumpy durable goods, as a response to intra-household conflict over preferences, or to provide insurance (Gugerty, 2007). A ROSCA is a voluntary grouping of individuals who agree to contribute financially at each of a set of uniformly spaced dates towards the creation of a fund, which will then be allotted in accordance with some prearranged principle to each member of the group in turn. The allotment is either through lottery random ROSCAs or auction bidding ROSCAs (Calomiris & Rajaraman, 1998). In an indistinguishable way, the operational mechanism of UCIS is identical to ROSCAs, where the basic UCIS model functions to eliminate the financial crunch of its present members. All the members pool in the predetermined sum of money to support the member in need of funds (Sethi, Ardener & Burman (1995). In this study, all models of UCIS has been derived on the basis of data pertaining to UCIS fraud cases of India.

#### **4.1 UCIS Model 1: Kitty**

In a span of 20 months, 40 investors, pool in Rs 1000 each, through which a corpus of Rs 40,000 is generated. The UCIS organizer collects the corpus and draws a chit, where names of each and every member are mentioned on chits of identical shape, size & color. A chit is then drawn at random, and the member whose name appears on the chit receives the full corpus of Rs 40,000, which in our example (see figure 1) is won by member number three. The cycle continues for the next 19 nineteen months, and the member whose name appears in the draw would not participate in the following chit draws but would continue to pay Rs 1000 (Reference: UCIS S. No. 13 in Table: 1). Since times immemorial, UCIS which takes up the form of social gathering such as Kitty parties has been a fount of rejuvenation for people in their late 40's where participation is fostered by the need for socialization. Social interactions develop a social relationship that facilitates trust-building, and it is this trust that fraudsters use to exploit innocent investors. (Manning, 2018). Over time, this rationale has changed with the increase in desire for more money, due to which people fall prey to such Ponzi Schemes (Investment fraud that involves the payment of purported returns to existing investors from funds contributed by new investors – US Securities and Exchange Commission). Organizing UCIS has become a business, though unregistered and unregulated, that yields high amounts of unlawful profits for the UCIS organizers. The basic concept of a regulated CIS has been diluted by high yielding bogus schemes, which we aim to explain in this chapter, with UCIS fraud cases that have transpired in India after 2009.

*Figure 1. Kitty Model of UCIS*



#### **4.2 UCIS Model 2: Pyramid Model**

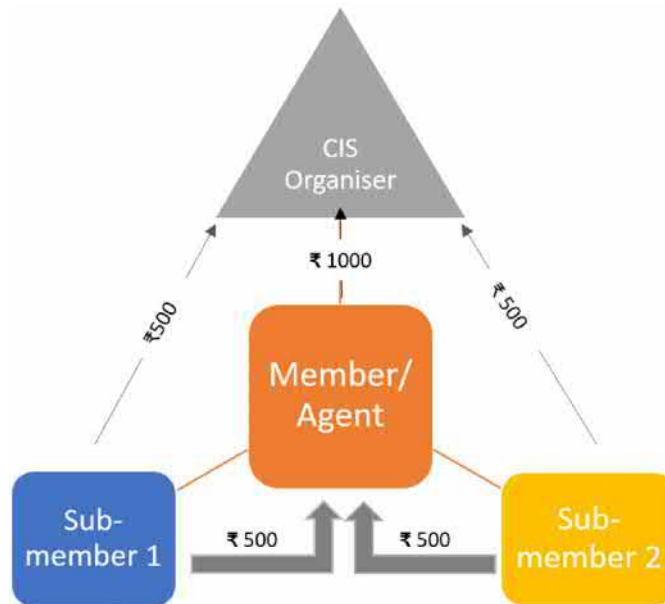
The pyramid model creates hierarchy with people joining under others who have joined the scheme previously, and in which those who join make payments to those upstream in the hierarchy, with the

## ***Frauds in Unorganized Investment Schemes***

expectation of being able to collect payments from those downstream (Takim, Ismail, Nawawi, & Jaafar, 2009). The major implications of pyramid schemes are that majority of participants have less than 10 percent chance of recouping their initial investment when a small profit is achieved as soon as they recruit three people and that, on an average, half of the participants will recruit no one else and lose all their money (Gastwirth, 1977).

Thus, this chapter asserts, that a pyramid scheme is a vertical business strategy, which helps the central operator of the scheme to increase its user base with minimal marketing costs. The central operator chains a member, who simultaneously acts as an agent of the operator and assists the operator in chaining more members to the scheme. The agent, in turn, receives certain benefits (monetary, non-monetary, or both) for every member chained. The members chained by the primary agent, may also act as agents of the operator and shall further chain more members to the scheme, which makes them entitled to similar benefits. These schemes are now frequently set within the context of Multi-level marketing (MLM) business opportunity, which siphons money from later entrants to compensate earlier entrants, delivering easily foreseen losses to the majority of participants (Bosley, & Knorr, 2018). A typical case of MLM is The Bernie Madoff Ponzi scheme, 2008. An American financier who was responsible for one of the massive financial frauds in the history of financial crimes. The fraud was structured in a manner that required Madoff to continuously receive new investments from others so that the money can be redistributed to previous investors as returns. (Quisenberry, 2017).

*Figure 2. Pyramid Model of UCIS*



Fundamentally, the key difference between Pyramid schemes and Ponzi schemes is in the destination of new investors' money. Investors in a Ponzi scheme typically send their money to either a central investment house or a person which is supposed to send the promised returns back to investors. However, new pyramid investors give their money directly to the people above them (Falk, & Blaylock, 2012).



UCIS functions on a similar pyramid scheme model (see figure 2). The central operator/ UCIS organizer appoints a member for a scheme of Rs 1000/month for 16 months. The member/agent who chains further members to the scheme is entitled to 50% commission (Rs 500) of the introductory amount (Rs 1000). Hence, as per the case, from the introductory amount of Rs 1000, Rs 500 gets deposited with the organizer and the remaining Rs 500 brims pockets of the agents.

This well-planned strategy, thus, turns almost every member into an agent of the scheme. The tactic not only helps UCIS organizers to build a wide network but also helps them in hiding their identities, as most of the members get connected through agents and submit their amounts through agents only.

### 4.3 UCIS Model 3: CIS Model

Conventionally, most of the UCIS especially kitties and committees, runs on a monthly basis (see figure 1). UCIS entities twist the basic monthly scheme model in order to provide intensely towering returns. To understand the monthly scheme model in detail, we list down the scheme of Shri *Balaji* Traders Fraud case of Uttarakhand. At a single point in time, numerous groups functioned, labeled from A to Z, where each group consisted of either 300 or 350 members. Every member who joined a particular scheme received a scheme card, where each card carried a label, representing the group he's a part of. The time duration of the monthly scheme was 15 months. As per the scheme, each member was obliged to deposit Rs 1000 on the First Thursday of every month, with the UCIS organizer, which generated a corpus of Rs 3,00,000 during the first month. The benefits of the schemes were rewarded by 'Draws' which took place through the chit system. The chief benefit of the scheme was the Bumper price, worth Rs 20,000 every month to one member only. The member, who won the draw, was entitled to receive the Bumper prize and further, did not pay any monthly amount. His/her card was discarded then and there. Thus, the first-month bumper draw resulted in a whopping profit of Rs 19000. Similarly, the second-month bumper draw, resulted in a profit of Rs 18000, followed by the third month with a profit of Rs 17000 and so on till the 15<sup>th</sup> month with a profit of Rs 5000. Thus, if we calculate the estimated amount of return for the member who wins the first bumper prize i.e., Rs 20000 on payment of Rs 1000 only, the figure comes out to be 1900 percent (profit of Rs 19000 on payment of Rs 1000 only), which is imaginary in reality but, at the same time, was payable by Shri *Balaji* Traders. Another reason that lured the public towards this UCIS, were the other benefits of the scheme. Apart from the bumper draw, they also conducted 42 other draws every month that served various benefits (see figure 3).

*Figure 3. CIS Model*



## ***Frauds in Unorganized Investment Schemes***

Apart from stellar returns, the UCIS organizers of the concerned case also guaranteed a profit of Rs 1000 to every member, at the termination of the scheme, if the member in question does not win the bumper prize. Consequently, every member was assured to receive positive returns on their amount deposited. However, the duration, amount, terms, and conditions, and benefits vary from scheme to scheme and case to case.

### **4.4 UCIS Model 4: Festival Bonanza Model**

To sustain their illegal business and surge the demand for their schemes during the festivals, UCIS organizers magnetize people through New Year and Diwali bonanza schemes. One-time payment in such schemes furnishes prodigious benefits such as motor vehicles (cars and two-wheelers), gold and diamond jewelry, and other consumer durables.

*Figure 4. Festival Bonanza Model*

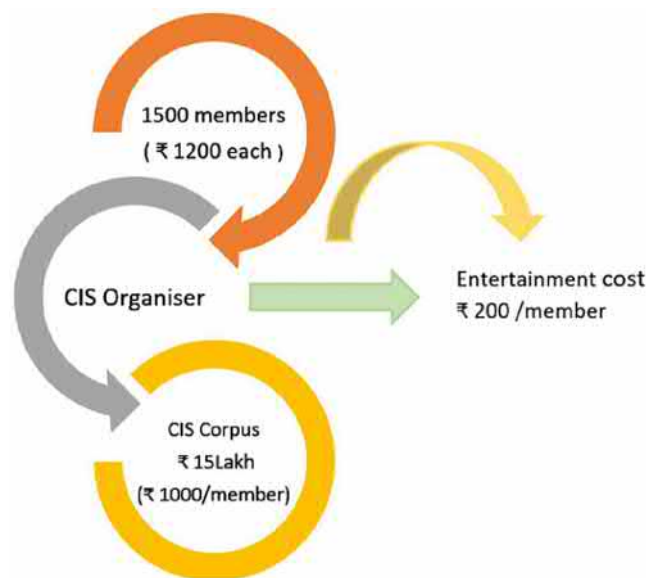


Figure 4 symbolizes the New Year bonanza scheme model adopted by various UCIS entities. This scheme comprises of 1500 members, where each member is obliged to deposit Rs 1200 each with the UCIS Organizer. Out of the contribution made by each member, Rs 200 is added to the entertainment cost which includes the cost of food, party games, and other entertainment activities, and Rs 1000 is added to the UCIS corpus. Thus, the contribution results in a humongous corpus of Rs 15 lakh. The benefits of this scheme are also delivered by way of draws through the chit system, out of the generated corpus of Rs 15 Lakh. The scheme serves exceptional benefits to the subscribed members, which included Maruti Suzuki Alto Car to three members and Honda two-wheeler (Bike or Activa) to two members. Thus, five members who win the draw were entitled to receive these exceptional benefits. The remaining members have the option to take away any available consumer durable goods (Pure its RO, Suitcase, Blender, or a Dinner set) against their contribution of Rs 1200.

## **5. ANALYSIS OF INVESTORS (VICTIM INVESTORS) DEMOGRAPHICS**

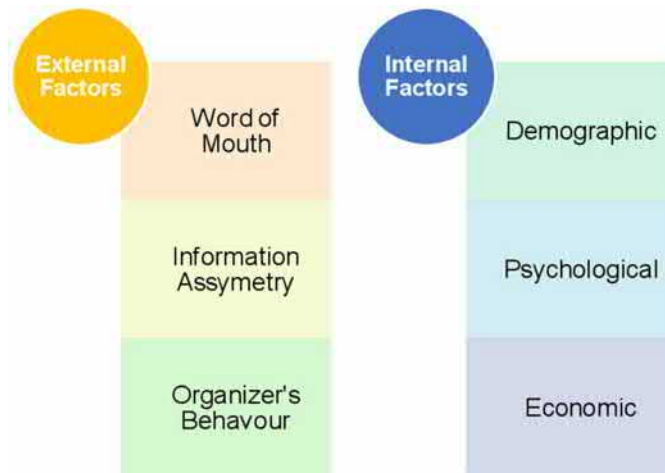
The foundational purpose for constellating data was to understand the operational mechanism of Unorganized Collective Investment Schemes (UCIS) and to analyze the rationale of people who participated in the same. To fortify our purpose, the fundamental categories for which data was collected included the personal information of the victims (Gender, Age, Qualification, Occupation, and Income) and data concerning the rationalized perception of the victims, who've fallen prey to tactics of these Ponzi schemes. The outcome of analysis has been consistent with the findings of Hasler & Lusardi (2017) which pinpoints "Financial illiteracy is widespread, but it is particularly pronounced among women". It is found that the major chunk that has fallen prey to phony schemes of UCIS associations constitute females. Due to low levels of financial literacy compared to their male counterparts females often get trapped in such facade. One probable reason which accounts for the avoidance of safer financial instruments by women is the manifestation of lesser financial knowledge amongst them. Therefore, an uneven gender gap in the data collected was noticeable, due to the inclination of women towards unofficial and unregulated savings schemes, where the division accounted for 90 percent female and 10 percent male respondents. The predominance of respondents belonging to the age category of "above 35 years" was detectable to be 50 percent. A striking result that manifested in the case, gave a macroscopic view of the Qualification of the victims of Unorganized CIS, which pointed out that only 10 percent of the answers were uneducated. The majority (90 percent) possessed some degree of qualification, which further pointed that 40 percent of the respondents were graduated, 25 percent had completed high school, 15 percent possessed post-graduation degrees, and the remaining 10 percent belonged to others category. The majority of the victims were literate as they possessed some degree of qualification, despite that they stand in need of awareness. Increasing rapacity of literates, to make easy money confined them to be duped by *Balaji Traders*, *Gurukripa*, *Renu Sethi*, *Datum Marketing Ltd*, and many others. Money making is the new grail, which has twisted the rationale of CIS participants, as the results of inquiry substantiate that, people no more join CIS schemes such as Kitties and committees, for social engagement and enjoyment. The occupation was measured belonging to one of the three categories, ranging from Housewife, Self-employed, and Service sector, where an inescapable result revealed that 45 percent of the respondents were Housewives, 35 percent worked in the Service sector and 20 percent were self-employed. Income was measured along one of the seven brackets ranging from less than Rs 1 lakh to above Rs 25 Lakhs where conspicuously 60 percent of the respondents had an annual income of less than Rs 1 lakh. While investigating the perception of the victims, It was notified 15 percent of the respondents would still believe their CIS organizer and join his/her scheme, if the subject under question offered them higher returns than banks and government securities, whereas 10 percent responded with the statement "That's high, I don't believe you!" and the major chunk (75percent) would ask for more information. High returns, past performance, and relationship with the organizer (60, 65, and 60 percent respectively) were the main attraction of investors for joining the UCIS. A noteworthy fact of analysis delineated that 80 percent of the respondents rated "Word of mouth" as a highly important factor that persuaded them to join these schemes. At the same time, 65percent of the respondents also considered "Irresistible schemes" as a key factor of motivation. A surprising yet, dull-witted outcome of the study, uncovered that 100 percent of the respondents contributed to the scheme based on "Friend's or Family's recommendations." Only 15 percent of the respondents had joined these schemes for enjoyment and engagement. The examination also reflected that 35 percent of the answers tend to ignore the negative comments about their CIS organizer and 70 percent of them have never verified their organizer's profile

from a regulatory authority. A tongue-tied aftermath proclaimed that even after suffering unexplained delays in payments, 55 percent of the respondents continued to contribute to the scheme because of faith in the organizer. Yet, 15 percent stop further contributing, 20 percent of them stop making further contributions but have hopes to recoup their Invested amount and only 10 percent of them tend to register a complaint against the organizer because of lack of trust on him.

### **5.1 Taxonomy of Factors Influencing Investment Decision Making in UCIS**

In relation to the evidence from existing literary text, the present chapter of the book is identifying that investment decision making in regulated markets such as stock market tend to be one of the most explored issues where buying and selling of stocks are not just bounded by rationality, but by psychological, social and economic factors. Guided by the generalizations drawn for the stock market by researchers in the past, this section of the chapter seeks to explore why people invest in such schemes i.e., the behavior of Kitty Investors and the indispensable factors that influence investment decision making in Kitties. The taxonomy of these determinants is grouped into two broad categories viz. External factors and Internal Factors.

*Figure 5. Taxonomy of Factors Influencing Investment Decision Making in UCIS*

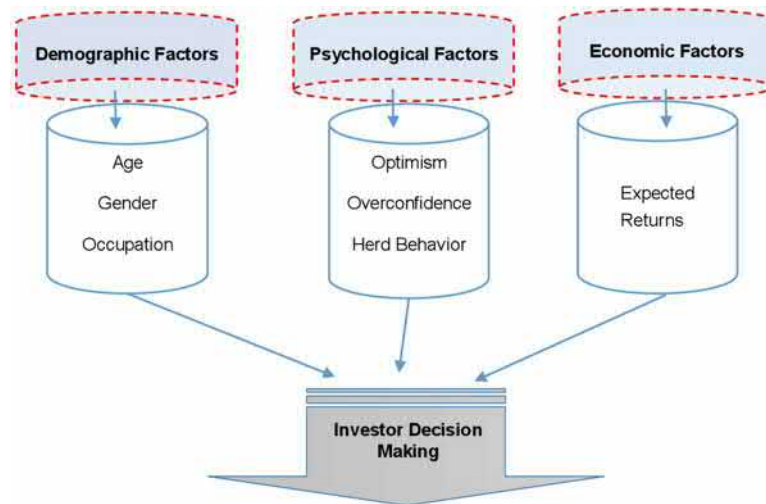


1. **External Factors:** As the name suggests, these factors include the forces that exist in the surroundings of an individual and influence his decision-making ability. They are the indirect variables that strongly influence one's decision making and intensely exert influence on his/her investment choices. Word of Mouth, Information asymmetry, and organizers' behavior fall in the purview of external factors.
  - a. **Word of Mouth:** Word of mouth generally abbreviated as WOM is an oral communication tool that has helped marketers overtime to target customers by magnifying their products/ services familiarity amongst the prospects. It is considered to be an efficient tool in view of the fact that it produces low cost on part of the marketer and effective for the reason that it

has widespread payoffs. WOM can be simply defined as the passing of information, facts, statements, or beliefs whether true, deceptive, misleading, or imaginary, produced intentionally or unintentionally about a product, service, or an event from one individual to another. Thus, WOM can have an impact that can be both positive & negative. Investor's decisions are vigorously influenced by WOM since people undoubtedly trust their peers and relatives. Such as in the case of *Balaji* Trader Kitty Fraud-BTKF (Reference: UCIS S. No. 13 in Table 1) we identified that the majority of Kitty investors were chained to the scheme on the basis of their friend's and family's recommendations. During the initial years, *Balaji* Trades was consistent in rendering the promised benefits that helped them to gain the trust of their early members. Contented and assured with the returns the early members engaged in WOM with their friends and family, the chain continued for a few years till the time when the Jains unveiled their hidden agenda.

- b. **Information Asymmetry:** A transaction is said to occur when there exit two parties engaged in a certain deal. However, when either of the party has greater access to material information about the transaction in process or its consequence thereafter, under those circumstances, information asymmetry prevails. Under unregulated schemes, the operator of the scheme is at an information advantage because the ultimate mission of the scheme is known to the operator only. The operators filter the information and supply only that part of the information which allures the investors towards his deceptive schemes. Therefore, the investors stand at the information disadvantage point on the continuum. Information asymmetry thus exerts a strong influence on investment decision making in kitties because the literal purpose is unknown to the investors and their decisions are based on only the misleading information floated by the fraudsters.
- c. **Organizers' Behaviour:** Unregulated schemes are likely to be successful in defrauding people only when the operators are able to build and sustain investors' faith. The operator formulates a master plan whereby he presents his unconventional idea through a business model that easily lures the investors. Payment of sky-high returns and absolute benefits in the early stages is one of the strategies of a fraudster's master plan for gaining trust. Therefore, no operator betrays its members during the initial years. Once a substantial amount of trust is built, the operator at this stage supports his master plan to sustain this trust by boasting his lush and pretentious lifestyle. This behavior is evident from the *Gurukripa* fraud case (Reference: UCIS S. No. 5 in Table 1) where the Sehgal's kept their social media handles updated with pictures of their Travel diaries of India and abroad. The cost of supporting these phony signals is extremely high, for instance, elegant facade, luxury lifestyle, bounteous employee welfare, advertising, marketing activities, celebrity advocacy, etc. (Ji, 2019)
2. **Internal Factors:** These include the factors that are directly associated with the decision-maker and as a result have utmost weightage in the ultimate decision. They are further dissected into three sets viz. Demographic factors, Psychological Factors & Economic Factors.
3. **Demographic Factors:** These include the socio-economic variables that indicate the general characteristics of the population under consideration. The influence of demographic variables such as age, gender, and occupation are discussed in the analysis section of this chapter (see analysis of Victim Investors demographics).

*Figure 6. Internal Factors Influencing Investment Decision Making in UCIS*



4. **Psychological Factors:** Aspects affiliated to an individual's mind, emotions or psyche falls in the category of Psychological Factors. They can range from one's emotions to his beliefs that tend to make an impact on the decision-making process. Cognitive attributes such as thoughts & feelings tend to direct an individual's behavior. These factors in the first place exert influence on the thinking of an individual thereby influencing his decision-making. (Sarwar & Afaf, 2016) The psychological factors that guide investment in kitties are as follows-
  - a. **Optimism:** The circumstances where an individual has a positive view about a transaction, event, or phenomenon and is of a strong opinion that he/she is less likely to face the negative consequences. An optimistic investor will always have trust in the firm, even when the market is flooded with negative information (Baker, & Nofsinger, 2002). It is closely related to overconfidence, when an investor has trust in his organizer & is overconfident about his beliefs, he remains optimistic about his investment and returns.
  - b. **Overconfidence:** The state of overconfidence prevails in an investor when he has the utmost belief in his abilities and misjudges the same to be superior to others in the market. Even in the stock market, the vulnerability of investors towards overconfidence is high as they are of the opinion that their judgments are more accurate compared to others (Chen, Kim, Nofsinger, & Rui, 2007) While investing in kitties, despite their unregulated nature people have utmost faith in their ability of judging the organizer/operator. The operator gains the trust of its members in a way that members on their part base their investment decision
  - c. **Herd Behavior:** When individuals direct their decisions on the basis of decisions taken by others, even when their own information suggests taking a distinctive action, then they are said to exhibit Herd Behaviour (Banerjee, 1992). Society follows those who have information/ knowledge useful for making a decision. The fraudster/leader supplies influential information that with the help of herd behavior forms an information cascade (Ji, 2019). In kitties or other unregulated schemes, this cascade effect is a consequence of the Word of Mouth. Investors follow their peers & relatives and thus make uninformed decisions, guided by the information possessed by others and hence, ignore self-possessed information.

- d. **Economic Factors:** The variables which are concerned with profitability and returns are placed under the economic category.
- e. **Expected Returns:** It is one of the principal factors determining investment behavior since all investments are made for the purpose of generating returns. The Fraudster draws a fascinating picture of the scheme in front of his prospects which eventually shoots up the investor's conjecture regarding the returns thereby, influencing him to invest in the scheme in dreams of high returns.

## 6. CONCLUSION

Endogenizing financial knowledge has important implications for welfare, as well as policies intended to enhance levels of financial knowledge in the larger population. (Lusardi & Mitchell, 2010). Due to low level of financial literacy, individuals are misguided by the bluffed schemes of fraudsters, who tend to exhibit moneyed ventures that are nothing more than a charade. On analyzing the existing work, it has been found that the operational mechanism of UCIS is similar to that of ROSCAs, where members contribute a pre-determined amount into a collective 'pot' which is then given to a single member, this member is then excluded from receiving the pot in future meetings, while still be obliged to contribute to the pot. Our basic model of UCIS is in tune with the functioning of ROSCAs as explained by Anderson, Baland & Meone (2003).

A further analysis unveiled that UCIS such as Kitties & Committees typically run on a monthly basis, in the form of a monthly scheme model. In order to pump up the scheme corpus during special occasions, these entities rely on occasional marketing models such as the New Year Bonanza scheme and Diwali Bonanza scheme that served exceptional benefits to magnetize people. It is found that the marketing model of UCIS is undifferentiated from Ponzi schemes, where techniques like multi-level marketing are used in the name of Pyramid scheme to increase the member base. A plausible story travels by way of word of mouth among people who know each other well, this leads to investment in Ponzi scheme (Wilkins, Acuff, & Hermanson, 2012). In line with this, it is found that "Word of Mouth" from relatives and friends turned out to be one of the significant factors that influenced the investment behavior of the victim investors. At the same time, friend's and family's recommendations were the most influential factor for participation in UCIS schemes. The results have also been consistent with the findings of Hasler & Lusardi (2017) which pinpoints "Financial illiteracy is widespread, but it is particularly pronounced among women". It is found that the major chunk that has fallen prey to phony schemes of UCIS associations constitute females. Due to low levels of financial literacy compared to their male counterparts females often get trapped in such a façade. It is traumatizing that the majority of the victims were literate as they possessed some degree of qualification, despite that they stand in need of awareness. The investigation also uncovers the increasing rapacity of literates, to have more money, which confined them to be duped by *Balaji Traders*, *Gurukripa*, Renu Sethi, Datum Marketing Ltd, and many others. Money making is the new grail, which has twisted the rationale of UCIS participants, as the results of inquiry substantiate that, people no more join CIS schemes such as Kitties and committees, for social engagement and enjoyment. Unexpectedly, after being cheated 15 percent would still invest in a CIS scheme that would offer them higher returns than Banks and government securities. The avarice is such that, few would still invest in dreams of getting rich quickly. In hopes of earning quick money investors many times end up losing their life savings in financial scandals. Such scandals can have a

## ***Frauds in Unorganized Investment Schemes***

catastrophic effect on an individual's physical and mental health. The aftermath of any such crime is disastrous, which has on many occasions even led to the loss of lives. An increase in suicide rates of the victim investors of Saradha scam 2013 is one such instance. A 35-year-old victim investor who had invested around Rs 4 Lakh in Saradha Group's scheme hung himself after being bankrupt. On another occasion, a 50-year-old victim investor set herself on fire (Reported NDTV, 2013). India has been a victim of these Unorganized CIS frauds for many decades. Several such schemes have been busted since then, despite that, many of these unregulated schemes are still operational in anticipation of deceiving innocent investors. With this work, this chapter scope for further research in the field of Unorganized Collective Investment schemes, UCIS frauds, and the Steps taken by the ministry to terminate such frauds, so that the public at large can be rescued and safeguarded.

## **7. RECOMMENDATIONS**

The outreach of UCIS in India is massive; still, the legal framework of such association appears to be blur. Therefore, it becomes quintessential to have precise and intelligible provisions governing the same. A proactive supreme body is the need of the hour that can become cognizant of such events prior to their occurrence. State governments should exercise active supervision and control on small entities so that such practices are not overlooked. Extension of formal banking services in tier II and tier III cities should be given utmost priority as these scams smoothly flourish at places lacking these services. Investors on their part should make informed decisions and park their savings in recognized investment avenues instead of falling prey to easy money bogus schemes.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.



## REFERENCES

- Anderson, S., Baland, J. M., & Moene, K. O. (2003). *Sustainability and organizational design in informal groups with some evidence from Kenyan Roscasm* (Working paper No. 2003, 17). Oslo: University of Oslo. Retrieved from <http://hdl.handle.net/10419/63174>
- Baker, H. K., Nofsinger, J. R., & Weaver, D. G. (2002). International cross-listing and visibility. *Journal of Financial and Quantitative Analysis*, 37(3), 495–521. doi:10.2307/3594990
- Banerjee, A. V. (1992). A simple model of herd behavior. *The Quarterly Journal of Economics*, 107(3), 797–817. doi:10.2307/2118364
- Besley, T., Coate, S., & Loury, G. (1993). The Economics of Rotating Savings and Credit Associations. *The American Economic Review*, 83(4), 792–810.
- Bhattacharjee, D. (2016). Problems and Prospects of Network Marketing in Assam (India). *International Journal of Business and Management Studies*, 5(2), 167–182.
- Bosley, S., & Knorr, M. (2018). Pyramids, Ponzis and fraud prevention: Lessons from a case study. *Journal of Financial Crime*, 25(1), 81–94. doi:10.1108/JFC-10-2016-0062
- Buttle, F. A. (1998). Word of mouth: Understanding and managing referral marketing. *Journal of Strategic Marketing*, 6(3), 241–254. doi:10.1080/096525498346658
- Calomiris, C. W., & Rajaraman, I. (1998). The role of ROSCAs: Lumpy durables or event insurance? *Journal of Development Economics*, 56(1), 207–216. doi:10.1016/S0304-3878(98)00059-5
- Chen, G., Kim, K. A., Nofsinger, J. R., & Rui, O. M. (2007). Trading performance, disposition effect, overconfidence, representativeness bias, and experience of emerging market investors. *Journal of Behavioral Decision Making*, 20(4), 425–451. doi:10.1002/bdm.561
- DharK. (2012). SEBI and Collective Investment Schemes. *National Academy of Legal Studies and Research (NALSAR) University*. Available at SSRN 2014416. Retrieved from: doi:10.2139ssrn.2014416
- Drew, J. M., & Drew, M. E. (2010). *Ponzimonium: Madoff and the red flags of fraud* (Working Paper No. 2010, 07). Griffith Business School, University of Griffith Australia. Retrieved from <http://hdl.handle.net/10072/390466>
- Falk, C. F., & Blaylock, B. K. (2012). The H Factor: A Behavioral Explanation of Leadership Failures in the 2007-2009 Financial System Meltdown. *Journal of Leadership, Accountability and Ethics*, 9(2), 68–82.
- Farooqui, A., & Nisa, S. (2017). Corporate Frauds and Its Impact: An Analysis of Select Cases. *Asian Journal of Management Applications and Research*, 8(1), 82–95.
- Gastwirth, J. L. (1977). A probability model of a pyramid scheme. *The American Statistician*, 31(2), 79–82.
- Gugerty, M. K. (2007). You can't save alone: Commitment in rotating savings and credit associations in Kenya. *Economic Development and Cultural Change*, 55(2), 251–282. doi:10.1086/508716

- Gui, Z., Huang, Y., & Zhao, X. (2020). *Financial Fraud and Investor Awareness* (Working Paper). doi:10.2139/ssrn.3025400
- Hasler, A., & Lusardi, A. (2017). The gender gap in financial literacy: A global perspective. Global Financial Literacy Excellence Center, The George Washington University School of Business.
- Ji, Z. (2019). The Role of Information: Analysis of organizers' and Investors' Behavior in Ponzi scheme. *9th International Conference on Education and Social Science (ICESS 2019)*. 10.25236/icess.2019.141
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology & Criminal Justice*, 8(4), 389–419. doi:10.1177/1748895808096470
- Lusardi, A., Mitchell, O. S., & Curto, V. (2010). Financial literacy among the young. *The Journal of Consumer Affairs*, 44(2), 358–380. doi:10.1111/j.1745-6606.2010.01173.x
- Manning, P. (2018). Madoff's Ponzi investment fraud: A social capital analysis. *Journal of Financial Crime*, 25(2), 320–336. doi:10.1108/JFC-06-2017-0057
- Mathur, N. (2010). Shopping malls, credit cards and global brands: Consumer culture and lifestyle of India's new middle class. *South Asia Research*, 30(3), 211–231. doi:10.1177/026272801003000301
- Quisenberry, W. L. (2017). Ponzi of all Ponzis: Critical analysis of the Bernie Madoff scheme. *International Journal of Econometrics and Financial Management*, 5(1), 1–6.
- Rafay, A., Farid, S., Yasser, F., & Safdar, S. (2020). Social Collateral and Repayment Performance: Evidence from Islamic Micro Finance. *Iranian Economic Review*, 24(1), 41–74.
- Sarwar, A., & Afaf, G. (2016). A comparison between psychological and economic factors affecting individual investor's decision-making behavior. *Cogent Business & Management*, 3(1), 1–18. doi:10.1080/23311975.2016.1232907
- Sethi, R. M., Ardener, S., & Burman, S. (1995). *Women's ROSCAs in contemporary Indian society*. In *Money-Go-Rounds: The Importance of Rotating Savings and Credit Associations for Women*. Berg.
- Takim, R., Ismail, K., Nawawi, A. H., & Jaafar, A. (2009). The Malaysian private finance initiative and value for money. *Asian Social Science*, 5(3), 103–111. doi:10.5539/ass.v5n3p103
- Thompson, J. K., & Choi, S. M. (2001). *Governance systems for collective investment schemes in OECD countries* (Occasional paper No. 1). OECD. Retrieved from [http://www.energytoolbox.org/library/infra2007/references/environmental\\_issues+compliance/Governance\\_Systems\\_for\\_Collective\\_Investment\\_Schemes.pdf](http://www.energytoolbox.org/library/infra2007/references/environmental_issues+compliance/Governance_Systems_for_Collective_Investment_Schemes.pdf)
- Tiwari, R., Anjum, B., Chand, K., & Pathak, R. (2017). An exploratory study of unethical practices in financial services in India. *International Research Journal of Management and Commerce*, 4(7), 219–228.
- Trusov, M., Bucklin, R. E., & Pauwels, K. (2009). Effects of word-of-mouth versus traditional marketing: Findings from an internet social networking site. *Journal of Marketing*, 73(5), 90–102. doi:10.1509/jmkg.73.5.90

Wilkins, A. M., Acuff, W. W., & Hermanson, D. R. (2012). Understanding a Ponzi scheme: Victims' perspectives. *Journal of Forensic and Investigative Accounting*, 4(1), 1–19.

## KEY TERMS AND DEFINITIONS

**Collective Investment Scheme:** A Collective investment scheme is any scheme or arrangement, which satisfies the conditions, referred to in sub-section (2) of section 11AA of the SEBI Act. Any scheme or arrangement made or offered by any company under which the contributions, or payments made by the investors, are pooled and utilized with a view to receive profits, income, produce, or property, and is managed on behalf of the investors is a CIS. Investors do not have day-to-day control over the management and operation of such schemes or arrangements (SEBI).

**Committees:** An unorganized association wherein investors pool in a predefined sum of money on a monthly basis that is auctioned at the end and given to the member who makes the lowest bid for the accumulated corpus.

**Information Cascade:** A phenomenon that leads to a series of same decisions, wherein individuals guide their decisions based on the actions/decisions of others simultaneously neglecting their personal knowledge/information.

**Kitties:** A fund of money for communal use, made up of contributions from a group of people.

**Multi-Level Marketing (MLM):** Multilevel marketing (MLM) is a strategy some direct sales companies use to encourage existing distributors to recruit new distributors who are paid a percentage of their recruits' sales. The recruits are the distributor's "downline." Distributors also make money through direct sales of products to customers. Amway, which sells health, beauty, and home care products, is an example of a well-known direct sales company that uses multilevel marketing (Investopedia).

**Network Marketing:** A business model that aggressively sells a product, service, or idea through an independent representative (agent) hired on a commission basis.

**Rotating Savings and Credit Association (ROSCA):** A rotating savings and credit association (ROSCA) is a group of individuals who agree to meet for a defined period in order to save and borrow together, a form of combined peer-to-peer banking and peer-to-peer lending.

**UCIS Associations:** An illegal entity set up by an individual or a group of people organized for a joint purpose. Kitty associations and committees are the most common form of UCIS associations in India.

**UCIS Chains:** Chain of investors fabricated with the help of Network Marketing, Word of Mouth Marketing, and Pyramid schemes. These tactics when executed through agents leads to the widening of the UCIS investor base.

**Unorganized Collective Investment Scheme (UCIS):** Similar to the Collective Investments Schemes (CIS) but not comes under SEBI preview and offered by associations which may or may not be registered.

**Victim Investors:** The investors who have invested in a scheme of UCIS association and have later been duped by organizers of such schemes.

**Word of Mouth:** WOM can be simply defined as the passing of information, facts, statements or beliefs whether true, deceptive, misleading, or imaginary, produced intentionally or unintentionally about a product, service, or event from one individual to another.

## **ENDNOTES**

- <sup>1</sup> Gold and jewelry schemes were floated by the jeweler, the scheme allowed investors to deposit a fixed amount every month for predetermined tenure. As per the terms of the scheme, in the end, investors would receive gold at a value equal to the total money deposited with a bonus or discount depending on the gold price at which the transaction takes place that is the one prevailing on maturity. (Times of India, Dec 24, 2019).
- <sup>2</sup> Mrs. Sudha Agarwal and her daughter Ms. Ritu Aggarwal resident of Dehradun (Uttarakhand) committed a UCIS fraud of approximately Nine Lakh rupees. A Kitty amount card issued and signed by the organizer was the unique feature of this UCIS. (Amar Ujala, Nov 22, 2019).
- <sup>3</sup> JPV Capital attracted the investors by offering lucrative returns. The firm assured monthly returns if the investment was retained for 13 months. It offered investors 5% monthly returns on investments above Rs 3 lakh and 4% on investment above Rs 5 lakh. (Hindustan Times, April 04, 2019).
- <sup>4</sup> Galaxy Enterprises, A Kanpur based firm opened its 100 branches across the country. In 1999, it offered a lucrative savings scheme to people by promising good returns on their investments. The company generated Rs 7.8 crore through its Ponzi business. The Uniqueness of this Ponzi Model was that the company was registered in UP (India) but most of the Victim investors were out of its registered state. (Business Standard, June 22, 2019).
- <sup>5</sup> Mr. Deepak Sehgal and his wife Mrs. Simran Sehgal resident of Dehradun (Uttarakhand) cheated investors through a Kitty Association. This UCIS had two unique facets one was the deluxe life of the Sehgal couple and the other is a religious name (*Gurukripa*) of their Kitty Association. (Dainik Jagran, April 22, 2019)
- <sup>6</sup> High returns were the key feature of Triporf Trading Services Pvt. Ltd UCIS. This company promised investors to pay a monthly return of 10% on their investments. They conducted events around *Jayanagar* (Bengaluru) and promoted their schemes on Facebook and other social media platforms. (Times of India, Jan 25, 2019)
- <sup>7</sup> Shivangi Tripathi a women resident of Haridwar (Uttarakhand) committed a Kitty Fraud of Rs Five Cr. An old and strong connection with a reputed political party was the key to success for this UCIS. (Times of India, May 14, 2019)
- <sup>8</sup> *Shakti* Multipurpose Cooperative Society Limited, Pune, a cooperative society that started 42 investment schemes similar to the collective investment schemes (CIS). In one of the schemes, they asked people to invest Rs One lakh each and assured that they would get a commission for the next 17 investors who would invest on their reference. The society had claimed to have investments in media, real estate, and diagnostic centers. Till January 2018, the investors had received their share of commission and after that, the commission money was stopped.
- <sup>9</sup> GIG Kitty Group hired agents who lured investors, especially women. Doubling the money was the main theme of this kitty fraud. GIG kitty deposited the money of people for 11 months and assured the returns of 12 months. The first case of kitty fraud worth Rs 50 crore surfaced in 2017 when the GIG Kitty owner Mr. Gurpreet Kaur refused to repay the money of members. (Times of India, Sep 4, 2019)
- <sup>10</sup> Mr. Tushar Thapar and his wife Mrs. Preeti Thapar resident of Dehradun (Uttarakhand) has been organizing Kitties since 2017. One of the victim Investors from Mussoorie professed that the couple delivered the promised benefits for a year but started making delays in 2018. As reported by Hindi

Dainik Amar Ujala, the couple went missing after January 14<sup>th</sup>, 2020, and disabled all routes of contacting them.

- <sup>11</sup> A lady police officer of Panchkula (Haryana) cheated corpus worth Rs 48.52 lakh through a Kitty fraud. The unique model of this UCIS was, it was being operated by a police officer which maximized investors' network as trust-building was made easy. (The Tribune, June 4, 2019)
- <sup>12</sup> UCIS model of Datum Marketing Limited was the mix of multilevel marketing (MLM) and collective investment scheme (CIS). This UCIS lured people to invest by promising them to multiply their money in a short span of time. When the company did not pay the depositors even after the maturity of their investments, several of them had demonstrated in front of the company's office demanding a refund of their invested corpus. (source: NDTV Nov 06, 2018)
- <sup>13</sup> *Shri Balaji* Traders in Uttarakhand has created Rs 12 Cr corpus through a Kitty model of UCIS, this model had different variants under Kitty. The Kitty organizer used the chit system to deliver promised benefits, where names of each and every member were mentioned on chits of identical shape, size & color.
- <sup>14</sup> Shilpy Jindal and Raj Rishi Chauhan the organizer of kitty has followed some similar modus operandi: inviting people to invest in kitties, giving them prizes for a couple of months, a sudden drying up of these 'prizes' and then disappearing after shutting shop. (The Indian Express, Sep 7, 2017)
- <sup>15</sup> Ms. Sadhna Jain resident of Delhi conducted a series of 'kitty parties' and floated small investment schemes. A victim investor invested in two schemes of Ms. Jain one was the 16 months' scheme and the other was the 20 months' scheme. In the first scheme, he invested Rs 25000 per month and in another scheme, he invested Rs 10,000 per month.
- <sup>16</sup> Ashok Jadeja, who was earlier arrested by the Gujarat Police for cheating several people. He duped over 2,800 people to the tune of Rs 25 crore by promising them to triple their investment through divine intervention. Jadeja, along with three associates, was arrested by the Gujarat Police for duping over two lakh people across the country of around Rs 562 crore. They promised the victims that they would double or even triple the amount invested by them. They had duped over 2,800 people to the tune of over Rs 25 crore in Delhi and investigators in the capital are looking for Jadeja's other associates, who are still at large. (The Indian Express, Dec 18, 2013)
- <sup>17</sup> Annu Bajaj, her husband Shankar Bajaj, and their daughter Neha organized a series of Kitty, each kitty used to consist of around 200 members. Annu would charge about Rs 1000 from each person. She would hand over a cheque to the lucky draw winner that would later bounce. (NDTV, Sep 26, 2011)

# Chapter 17

## Approaches to Detect Securities Fraud in Capital Markets

**M. Fevzi Esen**

 <https://orcid.org/0000-0001-7823-0883>

*University of Health Sciences, Turkey*

**Tutku Tuncali Yaman**

 <https://orcid.org/0000-0001-8742-2625>

*Beykent University, Turkey*

### ABSTRACT

*Financial markets are vibrant and fragile in terms of structure and mechanism and more prone to risks, failures, and exploitations than the other markets. This motivated the researchers to discuss and analyse the backstage of fraudulent activities in the capital markets. This chapter explains the main characteristics of securities markets and certain types of securities fraud which encompass a wide range of deceptive practices in capital markets. Traditional and modern approaches are reviewed which are used to detect and prevent fraudulent activities using qualitative and data-driven techniques. It is concluded that investors, market professionals, and regulators seek autonomous data mining techniques to combat securities fraud, especially stock market manipulation.*

### INTRODUCTION

The current market prices play a crucial role in explaining price fluctuations, market anomalies and market performance. In an efficient market, it is expected that the prices reflect all available public and private information about the asset. In the 1970s, it was widely concluded that financial markets are remarkably efficient and capable of reflecting all relevant information into the current prices; therefore no one can accurately predict future prices or inconsistent changes in market activities. However, there are risks and misconducts that are based on various reasons such as judicial, managerial, cultural, behavioral and psychological.

DOI: 10.4018/978-1-7998-5567-5.ch017

It is widely acknowledged that financial frauds have received the attention of accounting and finance literature (Reurink, 2018). As a part of the financial markets, securities market offers more profits than other markets, and it leads investors to deposit their savings on financial instruments (e.g. stocks, bonds, options, swaps) and to supply them as funds. For every financial instrument, there is a minimum of single agreement between at least two parties (issuer and investor); therefore, this reveals the necessity of a regulated trading environment where market participants can exchange financial instruments for future economic benefits under the rules with transparency and confidence. In a regulated market, efficient price discovery liquidity maintenance that motivate an investor to modify or trade his instrument, reduced transaction costs and investor protection can improve the efficiency of resource allocation, increase returns from investments, thereby boost economic growth.

Global economic cost of fraud is estimated to reach around \$5.12 trillion in 2019 and the losses owing to economic crimes have risen by almost 60% since 2009 (Gee & Button, 2019). According to Association of Certified Fraud Examiners (ACFE) report of 2020, 21% of fraud cases cause losses over \$1 million and companies lose 5% of their revenues to fraud each year (ACFE, 2020a). Roughly half of reported cases that experienced a fraud resulting in losses more than \$50 million are committed in financial markets and nearly 35% of those are deceptive practices, which encompass a wide range of illegal acts in stock or commodities markets (PwC, 2020). In addition to the direct economic losses that arise naturally from the breach of securities laws, indirect costs such as loss of productivity and profits, brand damage, employee and stock market demotivation, breach of fiduciary duty can lead to volatile stock prices; therefore, resulting an increase in economic losses.

The term fraud refers to a broad terminology that involves illegitimate or unlawful actions characterized by act of deceit. While the definitions of fraud vary among jurisdictions and seems problematic, the legal concept of the definition is shaped by guile and deception (Kapardis, 2016). It denotes the entire spectrum of illegal conducts in the financial markets by individuals from inside or outside, for the benefit of the organization or personal gain. The concept of fraud is not limited to a single activity or statutory offence in the law and practice. For example, in UK, Serious Fraud Office (SFO) provides the definition of fraud as “gaining dishonest advantage, which is often financial, over another person by misuse of position with material falsehoods” (Palmer, 2017). According to the ACFE, intentional or deliberate acts perpetrated by individuals or a group of persons that relate to the deprivation of property, money, service or other legal rights constitute fraud (ACFE, 2020b). As a civil wrong, fraud has been identified as a tort, which resulting in someone’s suffer or loss and it can include injuries, emotional distress, privacy breaches and so on. In common law, fraud is a criminal offence and a fraudulent act must meet the following requisites: (1) false statement or nondisclosure, (2) violation of trust or intent to deceive, (3) material, factual fact that makes a reasonable change in investment decisions, (4) being in a state of justifiable reliance in which a plaintiff must rely to his/her detriment, (5) the deception must result in loss of one party (Krauss, 2019). Section 1001-1040 of Title 18 of the U.S.C. states that the definition of fraud can include falsifying, concealing or covering up the material fact by any device or schema and it is not only a false statement statute but also failure to disclose of material information, knowingly and willfully (18 U.S.C. § 1001).

The definition of fraud involves much more than economic bubbles, credit card and financial statements frauds, theft and scams. Fraud has an elusive concept in finance and accounting literature, and it is generally attributed to white-collar crime that refers to false representation or suppression of a material fact with a purposeful intent to deceive and induce another. Tax evasion, embezzlement, illegal insider trading, cybercrime, Ponzi schemes, money laundering, bribing, forgery, and stock market manipulation

are the examples of white-collar crimes (Rafay, 2021). Although a precise classification of white-collar crime is difficult within the context of financial market activities, type of offense (e.g. cash, inventory, other assets, financial statement) and class (e.g. management, employee or nonemployee) or socioeconomic status and occupation of the perpetrator determine the contextualization of overall framework (Croall, 2010). For example ACFE (2020a) developed a taxonomy from the reported cases that relates to occupation and provided a classification system and schema to explore the mechanisms of fraud. This classification system includes three primary categories of offences such as corruption, asset misappropriation and financial statement fraud. According to the Statement of Auditing Standards issued by the American Institute of Certified Public Accountants (AICPA), a common understanding and detailed comparison of fraud have been proposed. To help auditors, managers and employees prevent or detect fraud, a collection of required procedures are also discussed in detail. Although these standards incorporate some recommendations about misstatements arising from the reports of financial transactions or misappropriation of financial assets, it describes the risk factors and auditing practices that deter and detect fraud (AICPA, 2019; Ramzan *et al.* 2020).

Despite the recent developments in regulatory activities and data analytics, there are uncertainty and variability in detecting and preventing financial fraud (Khan *et al.*, 2020). While regulatory agencies combine technology with anti-fraud strategies and standards to combat fraud, they are perhaps incompetent to develop strategies for different individuals and organizations (Tang & Karim, 2018). Moreover, fraud detection requires both technology and talent. Fraud investigators may not obtain sufficient evidential matter during the examination and they may experience subjectivity when reporting fraud. They may be incapable of dealing with complexity of the fraud or adapting analytical procedures and data mining technologies (Gray & Debreceeny, 2014).

This chapter focuses on types of securities fraud and its detection by traditional and modern approaches. In this chapter, we describe the main characteristics of securities market with its instruments and participants, and we give the definition of securities fraud and focuses on the types of fraudulent acts on the market. The approaches for the detection of securities fraud are also discussed. Finally, we summarize major conclusions and provide perspectives for future works.

## **THE MAIN CHARACTERISTICS OF SECURITIES MARKET**

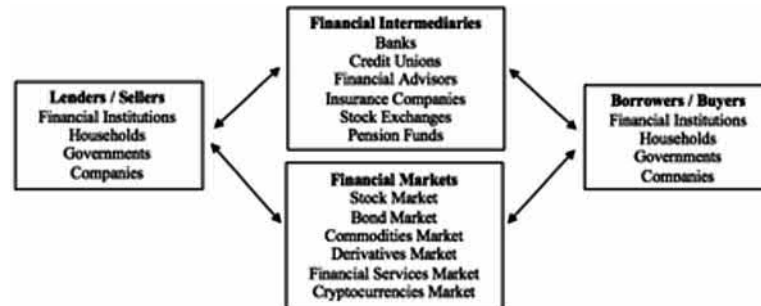
Financial markets are located in the global financial system. As shown in Figure 1, these markets are the mediators of financial system in which the financial instruments (e.g. stocks, bonds, derivatives and other securities) can be traded between market participants (e.g. lenders and borrowers or sellers and buyers) by setting reciprocity relations. This mechanism also creates opportunities for financial investments and supports businesses, which need funds for their project expansions and business spending. Investors, savers, securities dealers, and speculators trade financial securities of the companies to earn interest, dividend or stock appreciation (Rose & Marquis, 2006).

Financial markets are classified according to various characteristics such as type of securities, unit price, market level and competition degree. But traditionally, there are two subsets of financial markets as capital markets, for long-term investments, and money markets for short-term investments. Capital market has a broader meaning that implies a component of financial market in which the securities are more diverse and riskier than the other markets. It is basically the marketplace where a broad spectrum of securities including long-term borrowing instruments, derivatives, equities and commodities are bought



*Figure 1. Global Financial Ecosystem*

*Source: Authors' own work*



and sold. On the other hand, short-term securities such as certificate of deposit, commercial papers, and treasury bills can be traded in money markets. Due to smaller maturity periods, these securities are usually reviewed as low-risk and secure investments (Strumeyer & Swammy, 2017). Although there are aforementioned differences between the two markets, it is not possible to distinguish them with bold lines.

The concept of a security, which constitutes the term securities market, is defined as a tradeable financial asset that refers to a manifestation of promise by an issuer to pay interest and return capital, or share ownership of a company (Arnett, 2011). Securities are issued to trigger flow of funds by attracting new capital on the markets and provide earnings stream both to individuals and the economy. In many cases, its legal definition depends on either the contracts between the parties or jurisdictions. Exchange Act of 1934 sets a broader definition for securities based on debt, equity and derivatives by excluding interest rate swaps and credit default swaps (15 U.S.C. § 2B). Ownership rights, term to maturity, industrial sector, country or region of the principal market in which the securities exchanged, currency of denomination, credit score and liquidity ratio of the issuer are the main factors for the categorisation of the securities. Typically, securities include shares, sovereign bonds, deposits, mutual funds, options, warrants, debentures, notes, mortgage obligations, and other financial instruments that are negotiable.

Securities markets consist of many participants, including, but not limited to, investors, issuers, broker-dealers, clearing agencies, electronic communications networks (ECNs), securities exchanges, transfer agencies and regulatory organizations. These participants may be legal persons, corporations or governments. Issuers are the entities that are legally responsible for producing, registering and distributing a security. Investors are the registered users who buy or sell securities through broker-dealers in stock, bond or derivatives markets in which the regulators can monitor market activities. Institutional investors accumulate the funds of investors and trade blocks of securities in large quantities on behalf of its shareholders. Banks, mutual funds, credit unions, venture capital funds, pensions, insurance companies, real estate investment trusts and investment advisors are typical institutional investors that can manage the funds of their clients by creating a positive effect on the price dynamics. As another participant of the markets, brokers are the registered professionals or companies that engage in securities trading for their customers' accounts. However, dealers trade securities through the brokers for their own accounts (SEC, 2020). Broker-dealers can trade both on their own behalf and on behalf of their customers. Besides, they fulfill vital roles in securities markets such as financial consulting, market making, source of investment research and easing information flow on the markets. Moreover, clearing agencies are registered persons or companies that provide a counterparty function in clearing and settlement of the

## ***Approaches to Detect Securities Fraud in Capital Markets***

trades while transfer agencies keep the records of securities ownerships and handle investor's problems including issuing or canceling the certificates.

Securities market encompasses equity, debt, and derivatives markets. It induces capital formation by collection, mobilization and the use of savings within supply-demand framework and subject to separate regulatory regime from other markets. For the protection of market efficiency and safeguarding securities and funds, regulations impose special requirements on transactions and practices of issuers, inside and outside investors, intermediaries, and operators involved in securities market.

### **Types of Securities Fraud**

The participants of securities market can involve in intentional irregularities that presumably include fraudulent transactions and practices (e.g. intentional misrepresentation of information relation to the transactions and events, manipulation or falsification of records and documents, willfully violation of securities laws) as well as unintentional practices (e.g. incorrect interpretation of facts, mistakes in deriving data from securities and errors in accounting principles, and disclosure failures of the securities). In general, securities fraud is defined as the intentional use of the securities through misrepresentations or other deceptive practices for the purpose of manipulating someone to trade in a fashion that is not good for their own (Straney, 2011). In accounting and finance literature, economists and criminologists distinguish the definitions of financial fraud and error. Researchers focus on the term of intentional act that aims to deceive shareholders or related parties to gain improper advantage, usually through the use of preferential information. Almost all the definitions of fraud rely on the breaches of the trust and confidence by violating securities law and regulations (Jones, 2012).

Securities fraud encompasses a broad category of specialized areas and various forms. Even if it causes massive monetary damages, some practices cannot be described as fraud. Securities law and regulations play a vital role in determining the definition of fraud. Due to this reason, there is a lack of unified theory that explains victims and winners, defendants and litigants, gains and losses in securities market. In this chapter, we only focus on most costliest securities frauds, insider trading and market manipulation.

### **Insider Trading**

In securities market, fraudulent practices mostly relate to asymmetric information and to externalities that are not directly involved in transactions. These practices are generally orchestrated by management or the people who have a positional power or preferential access to private information. McGeever (2017) provides a list of recent scandals and prosecutions on insider trading and market manipulation. It shows that the total amount of fines paid by recent perpetrators reaches more than \$10 billion and dozen of traders are prosecuted for fraud at U.S. courts. PwC (2020) states that 43% of fraudulent practices caused by corporate managers and those are potentially far more damaging than externalities.

Insider trading is the most important fraud that reduces information transparency and violates investors' confidence in the securities market. It refers to the illegal trades of corporate insiders based on material non-public information. Many studies prefer to explain insider trading in a broad sense by including anyone (inside or outside) who uses undisclosed information to gain transactional advantage or to damage anyone resulting a loss (Wang & Steinberg, 2010). Insiders are the employees, managers or controlling shareholders of a company who have knowledge of or access to material non-public information. Insiders are legally obliged to disclose their trades by virtue of relationship of trust with shareholders. Many

*Table 1. Potential scenarios for illegal insider trading*

Scenario	Activity	Definition
1	A company begins a new drug in the laboratory and completes preclinical and clinical research. In the meantime, it announces detailed information about drug development process to the public. Its stocks starts to rise and reaches an all-time high. Then, the company submits an application to market the drug. After FDA's review, the drug is found as ineffective and unsafe; therefore, FDA rejects the drug and notifies the company about the rejection. After receiving the notification, CEO sells his holdings in the company's stock at a higher price. Following the disclosure of the notification, share price falls 70% by panic, resulting in a significant loss of investors.	<ul style="list-style-type: none"> <li>-CEO gains an unfair advantage in selling his shares at a higher price by taking inside information that is not available to investors. He violates fiduciary duty rule and damages investor confidence.</li> <li>-The company may announce the information of rejection to the public within the legal notification period, but CEO may trade on inside information before its disclosure by concealing the truth.</li> <li>- CEO may disclose the inside information to someone else (e.g. friend, relative, competitors, beneficial owners) who trade on it.</li> </ul>
2	A web designer becomes aware of advantageous information from a financial services company, which she serves. She purchases the stocks of the company at lower prices. After stock reflects the information, she reverses the transaction for the profit.	-Although she owes no legal fiduciary relationship with the company, she misappropriates confidential or valuable inside information of a company by theft. Consequently, she violates securities market law as an corporate outsider.
3	A broker-dealer receives the information of an impending takeover. He executes purchase order for his own account and (or) executes sell order on behalf of his customers.	-A broker-dealer is responsible to deal fairly with his clients. He has a confidence and trust relationship with the clients as well as an obligation to disclose the material information.
4	Treasury committee work on a national financial policy to avoid market abuse. The policy limits some transactions and reinforces specific companies to trade by increasing daily trading limits. Some members of the committee act upon the information of the new policy and purchase specified companies' shares before the policy is put into practice. Stock prices of these companies doubled in a short time following the enactment of the policy.	In most countries, members, officers, or employees of congress, house of representatives, securities and exchange commissions, board of governors and related committees, civilian employees of executive offices of government departments and agencies and legislative branch are prohibited from using nonpublic information for their benefits, and for someone's purposes. These people are required to report their financial transactions within a specified time period.

courts have broadened the scope of insiders under fiduciary duty rule and specified various classes of people including investment advisors, corporate partners, trustees, tippees-tippers, attorneys, contractors and brokers who have a beneficiary interest or relationship with companies.

Materiality of the information states a condition that a reasonable investor would significantly change his investment decisions when the information becomes available to him. In other words, the information must have an effect on security prices when it is disclosed to the public. Some scenarios are given in Table 1. Under the misappropriation doctrine, there is no distinction between inside information originating from the company and market information (Humke, 1997). However, there is still an ongoing discussion about the determination of materiality of information in the literature.

Insider trading is the most problematic topic that has been debated through a wide literature. While some studies emphasize the necessity of deregulation of insider trading for enhancing the efficiency of stock markets and compensating corporate entrepreneurs for innovations, some studies support the argument that insider trading harms public's confidence to issuer of securities and the market. It also delays the transmission of information, resulting decrease in accuracy of prices in securities market (Bainbridge, 2001).

## **Market Manipulation**

Chartered Financial Analyst (CFA) institute's global market survey shows that financial market manipulation is one of the most important market abuse that affects listed companies each year (CFA, 2014). The estimates report that nearly 14% of US companies have faced the negative consequences of market manipulation and 93% of managers in these companies lose their jobs (Alexander and Cumming, 2020). According to Wheatley Report on the London Interbank Offered Rate (LIBOR), the manipulation of securities prices and interest rates affected in excess of \$300 trillion worth of financial contracts (Crown, 2012).

Manipulation in securities markets refers to the deliberate interference in the prices by artificially altering supply and demand function of the market. Securities prices do not reflect market conditions and this leads to price fluctuations resulting volatile stocks. Manipulation is conducted by manipulators attempting to create artificial, false or misleading prices and it has a negative impact on financial market efficiency, transparency, public trust and economic growth (Fischel & Ross, 1991). It leads to an increase in the weighted average cost of the capital of business entities and sharp decrease in the stock prices of listed companies. For this reason, manipulation is strictly forbidden in most countries.

Market manipulation takes many forms depending either the type and number of participants, volume of transactions or the type of financial assets. The basic idea behind the manipulation is effecting securities prices to gain unfair profits to the detriment of other investors. In most cases, expectations, predictions or behaviors of investors are steered through distorting (e.g. inflating or deflating) fair prices of the securities. For example, Boesky who is an arbitrager in Wall Street, accumulated 3.4 million shares of Gulf & Western Industries through his companies at the suggestion of a partner. Based on a speculation, the expectation was that the stock was undervalued and would go up in the short run. Then, Boesky got in contact with the management of G&W and asked to sell the shares back to the company at \$45. He stated that he had 4.9% of the company's shares and he would try a leveraged buyout if they refuse the offer. The company refused to buy the shares back at \$45 and they offered to buy with the latest price at the time of last sale. After this, Boesky contacted with a registered broker before 11 a.m. on October 17, 1985 and told him to not pay more than \$45 for G&W stocks. Before this call, G&W stocks were traded at \$44.75. The broker's company bought 75,000 shares between 11.04 and 11.10 a.m. and the stock price was \$45 at 11.10 a.m. Immediately afterwards, at 11.17 a.m., Boesky and his partner sold 6,715,700 shares back to G&W at \$45. At the same day, G&W stock was closed at \$43.63, resulting an unfair profit of more than \$1.5 million for Boesky and his partner (Markham, 2014). Enron, Citibank, WorldCom, Tyco International and Bernard Madoff cases are well known frauds that are convicted of financial market manipulation.

Securities markets can be manipulated by information, trade or action. Some forms of manipulation are based on placing orders and some other forms aim to perform deceptive actions. But generally, it is divided into three groups of actions: (1) Information based manipulation refers to the spread of false or misleading financial information about the securities. To change security prices to rise, fall or remain stable, manipulators spread rumors through various channels such as reports, e-mails, social media or newspapers. In a sense, this can be carried out by complex reporting practices such as fictitious revenues, anonymous news or reports and creating timing differences. (2) In trade based manipulation, one or more traders fill large volume of purchase or sell orders to mislead investors without releasing false information and they can make abnormal profits by mimicking informed traders in a short time. (3) In action based manipulation, the perceived value of a financial asset is changed. For example, a manipulator purchases

a company's stock and then announces unserious takeover bid. Stock price increases and he sells the stocks at an elevated price level. Corporate insiders are generally addressed to action-based manipulation.

Manipulators can use a single market or multiple markets to execute their trades. They may be profiting in one market, while losing in another. For this reason, manipulative schemes continuously evolve over time and manipulators employ special methods to avoid getting caught. The Committee of European Securities Regulators (CESR) defined a wide range of techniques in market abuse directive, which are commonly used by manipulators. It should be noted that some practices may involve overlap or cover the trades of different parties; therefore, a precise definition may not be possible (CESR, 2020). Some types of securities market manipulation are given in Table 2.

In financial markets, information technologies have overwhelming benefits on a wide range of fields including trading platforms, investment decisions, market communication, asset management and its related risks, but it is not completely able to eliminate securities fraud. Manipulators have immense ability in managing thousands of accounts simultaneously and place several types of orders from various markets by using high-speed order systems. Therefore, detection and surveillance of market manipulation become difficult for supervisors, regulators and decision makers.

Due to the complexity of total losses and effects on organizations and financial markets, recognition and detection of securities fraud require an interdisciplinary perspective of finance, accounting, auditing, business management and statistics.

*Table 2. Market manipulation methods*

Method	Description
Wash sales	Manipulators intend to artificially increase volume of a stock or give passive selling orders to mislead investors. This does not cause changes in the ownership of a security.
Pumping and dumping	It is a type of economic bubble. Manipulators insistently purchase a stock at increasingly higher prices. This creates a price momentum. Once manipulators sell their overvalued stocks, the prices plummet. Pumping and dumping generally takes place through social media, spam and cold calls.
Cornering	In cornering market, manipulators control a large portion of the targeted security or securities. They force the prices up and down.
Painting the tape	This is defined as the series of transactions that aim to give false impression about the price of a security to the public (IOSCO, 2000).
Marking the open/ marking the close	Those refer to the high opening/closing prices in securities market. Manipulators buy or sell securities at the beginning/end of the trading session to distort prices. For marking the close, many stock exchanges implemented some mechanisms that collect orders of traders at the closing auction and execute the trades at one price.
Improper matched orders	This practice involves different or similar types of orders that are executed at the same time with similar quantity and price by different but colluding parties. The distinction between wash trades and improper matched orders is the change in beneficial ownership.
Advancing the bids	This is a false signal (offer) about security price for investor to sell or buy his securities by prevailing best quotes. For example, a manipulator enters orders to sell his securities. Prices fall over time and orders narrow the spread. Manipulator cancels the best sell order. After a while, the manipulator enters considerable buy order that executes against remaining best sell order.
Spoofing	Spoofing is illegal biddings or offerings that intend to create artificial imbalance in the orders. This activity attracts investors to induce a market reaction. It is generally employed by high frequency trading.
Pooling	In pooling, two or more manipulators decide to trade together by following the leading manipulator towards his/her directions. Pooling manipulators may be working in different companies and they may employ both cornering and wash sales to keep the securities prices at a desired level.

## **DETECTION OF SECURITIES FRAUD**

The prevention and detection approaches for securities fraud have been diversified and evolved from qualitative-based to data-driven techniques. Qualitative-based techniques include manual inspection that focuses on initial assessment of the corporate information received such as false entries, falsification of asset values, violations or misrepresentation of financial conditions. In general, literature analysis and formal questionnaires are performed to inspect fraud within qualitative-based techniques. On the other hand, data-driven techniques are the integral part of automated systems that help to detect abnormal cases or fraudulent transactions by systematical analyses. These offer a wide range of applications (e.g. dashboards, metrics, charts) both for routine and real-time operations by using a variety of statistical techniques. This section starts with an informative part related to traditional techniques in fraudulent acts and continues with modern approaches that focused on data analytics.

### **Traditional Approaches**

Since the securities fraud is an area of interest in criminal justice, many regulatory practices applied as preventive actions. One of the well-known establishment is U.S. Securities and Exchange Commission's (SEC) investigation guideline. The investigations are dependent on various factors and conducted through inquiries, interviewing witnesses, documents, media reports, securities market data and other relevant documents (SEC, 2020).

Many countries have regulatory institutions that focus on manual investigation mechanism. In addition to that, public or private fraud investigators can pursue inspection whose reports include assessable empirical evidence. As a leading provider of financial crime detection, The Association of Certified Financial Crime Specialists (ACFCS) has an internationally valid certification process for candidates for the Certified Financial Crime Specialist (CFCS). In addition to ACFCS, The Association of Certified Fraud Examiners (ACFE) offers a certificate for applicants with documented academic and professional qualifications. Certified prosecutors, private investigators (Gilsinan *et al.*, 2008) or police enforcement (Levi, 2009; Diih, 2005) can follow the investigation process. Either way, the main goal of the investigation may be the discovery of unseen facts of the case. The investigation phase starts with defining solvability factors, obtaining documentary evidences, and interviewing with related people. Essential tools that will be useful in analyzing phase are presented in Silverstone *et al.* (2004). Finally, the fraud investigation reports regarding the case are evaluated by the client. The important criteria in the evaluation process is dealing with certain empirical evidence for forensic analysis. Another crucial point is the constitution of an effective organization which involves in investigation process minutely. This organization will also be responsible of accurate documentation, data analysis, proofing and conclusion (Gottschalk, 2018). For further detail, Benson & Simpson (2014) provides a comprehensive list of electronic sources regarding fraudulent actions in finance.

After a principal entry with traditional approaches on securities fraud detection, in the next section, more sophisticated methods are discussed in detail.

### **Modern Approaches**

With the start of the 21st century, data-driven approaches started to play a more essential and dominant role in our understanding of human interactions to a wider extent. Fraud detection approaches have also

taken its share from the applications of analytical techniques. Most of the well-known statistical analysis tools adapted to various fields in the use of information creation.

The rise of data-driven analytics started with the 1<sup>st</sup> International Conference on Knowledge Discovery and Data Mining in 1995. At the same period, the first data-mining companies and commercial/non-commercial software programs were launched. Leading applications in financial fraud detection with data-mining approaches was on credit-card-fraud detection (Curley, 2011). Most of the initial studies led by computer scientists and applications made by limited datasets (Lee & Stolfo, 1998). An early work on discovering patterns of insider trading in the stock market with data-mining tools offered by Westphal and Blaxton (1998). In the early 2000s, Kou *et al.* (2004) presented a review of fraud detection techniques. Ferdousi and Maeda (2006), in their paper called “Unsupervised Fraud Detection in Time Series Data”, performed Peer Group Analysis (PGA) in time series financial data with the aim of finding outliers. Westphal (2008) states that all of these advances will be predominantly depend on involving a better understanding of data in terms of accessibility, interpretation, analyzing, and reporting.

In 2009, two separate emerging market applications were published by Ögüt *et al.* (2009) and Mongkolnavin and Tirapat (2009). The first study was conducted with the use of Artificial Neural Networks (ANN) and Support Vector Machines (SVMs) and the second study was a practice of association rules to detect market manipulations. Ngai *et al.* (2011) provided a stunning paper with a discussion on data-mining techniques for fraud detection. Their work was followed by West and Bhattacharya (2016). Diaz *et al.* (2011) presented a set of decision rules. These are gathered from the concept of Decision Trees (DT) that can be simply understood by a financial expert. Although Ngai *et al.* (2011) stated that there is a lack of research on securities fraud, Golmohammadi and Zaiane (2012) published their research that includes an all-inclusive methodical literature review for the detection of market manipulation. Inspected papers in their research cover 38 articles that address fraud detection on securities market and the proposal of the authors was the use of various applicable data-mining techniques to identify manipulations in the same area. Even though literature about data-driven approaches in the detection of financial fraud covers many advanced analytical techniques, pattern recognition, outlier detection, rule induction, social network analysis and, data visualization are most widely used techniques. Song *et al.* (2012) suggested Coupled Behaviors Analysis (CBA) scheme in the identification of group-based market manipulation. Both domain and data-driven approaches were performed in the acquisition of more comprehensive couplings in the Asian Stock Market. Results of their proposed approach with proper domain knowledge among stocks functioned better than the antecedent benchmark Coupled Hidden Markov Model (CHMM). Holton (2009) combined text mining and Bayesian belief networks in order to detect so-called annoyed employees anticipated to commit financial fraud. Another example of a text mining application performed by Zaki and Theodoulidis (2014). They proposed an approach for extracting valuable information from SEC’s litigation releases (SEC, 2019).

In the last decade, the implementation of cutting-edge techniques such as supervised, semi-supervised, and unsupervised learning algorithms are revealed (Beg *et al.*, 2019; Sekmen & Hatipoglu, 2019). Dhanalakshmi and Subramanian (2014) widened the point of view by adding heuristic algorithms with various classification and clustering approaches without indicating each of them as certain solutions to the detection of certain fraudulent activities in the securities market. Under the light of the knowledge that actual fraud detection approaches depend on a set of rules, Golmohammadi *et al.* (2014) proposed the use of supervised learning algorithms such as Classification and Regression Trees (CART), Conditional Inference Trees (CIT), C5.0, Random Forest (RF), Neural Networks (NN), SVMs, Naïve Bayes (NB), and k-Nearest Neighbour (k-NN) algorithm in order to identify questionable or probable manipulative

activities in the stock market. As stated by authors, these techniques are better fit into the uncertain and dynamic nature of the fraudulent activity. Conforming to their results, Naïve Bayes performed well. In another study, Golmohammadi and Zaiane (2015) encompassed contextual outlier detection for time series fraud detection with a prediction-based Contextual Anomaly Detection (CAD) method. In this paper, window-based, proximity-based, prediction-based, Hidden Markov Model (HMM)-based, and segmentation based methods are performed. Therefore, any of them was found as a superior because of pros-and-cons, authors proposed their CAD method which exceeded better results than k-NN and Random Walk. Islam (2018), implemented a comparison of the results of both pattern recognition and anomaly detection techniques, with the use of Normalized Cross-Correlation (NCC). A recent work of Rukmi *et al.* (2019) presented an application of Density-Based Spatial Clustering of Application with Noise (DBSCAN) which performed well in time-series with noise in the Indonesian stock market. Castro and Teodoro (2019) aimed to model possible anomalies (e.g. insider trading) by using different techniques. Probabilistic approaches that cover C4.5 and Bayesian Networks (BN) performed better compared to NN. Esen *et al.* (2019) proposed a two-step clustering-based outlier detection approach for the detection of suspicious insider transactions in the stock markets. In addition, graph-based detection approaches for the detection of securities fraud were implied by Tamersoy *et al.* (2013), Tamersoy (2016), and Rayes and Mani (2019). After a short review of selected papers from the literature, the main data-mining techniques associated with well-known goals in securities fraud detection are discussed in the following section.

### **Statistical Approaches**

In the era of big data, most of the informative sources in the field of financial fraud do not significantly involve one of the most challenging task: processing massive amounts of data. Prior to performing advanced methodologies (e.g. unsupervised machine learning) that require sophisticated hardware technology, for discovery purposes, both descriptive and inferential methods of statistics can be used in forming a general framework of the attempted case. Exploratory bivariate techniques such as examining the distribution of variables, graphs, and frequency tables can offer ideas for large samples. A basic visualization could open a path for experts in the identification of suspicious activities, alias anomalies in securities, and traders transactions (Golmohammadi & Zaiane, 2012). Likewise, multivariate analysis techniques such as cluster, factor and discriminant analysis, multidimensional scaling, canonical correlation, stepwise linear regression, and CART can be useful in identifying main patterns of multivariate data sets. Especially, principal component (PCA) analysis and regression based approaches are largely used to determine both influential variables and relationships between various variables in different financial markets (Zhang & Zhou, 2004). In the interest of prediction, as well as basic linear and non-linear regression models, Auto-Regressive Conditional Heteroskedasticity (ARCH) models which postulates volatility of financial indicators are widely used to measure unexplained effects by time series models. Generalized Auto-Regressive Conditional Heteroskedasticity (GARCH) models, Autoregressive Integrated Moving Average (ARIMA)-based models have been also used in financial data sets to estimate the volatility of returns for stocks, bonds, and market indices (Ye, 2017; Yan & Yan, 2019). By analyzing historical data, one may forecast the current data in order to identify the difference between the predicted and actual data. Significant differences can be a good sign of fraudulent activity.



## Pattern Recognition

Patterns are any mix of inputs that involve a valid composition within the investigated context. Clusters, trends, sequences, or relationships are in the context of the pattern definition. For example, trend discovery in a time series data enables us to understand “normal” and “anomaly” Within the fraud detection context, unexpected or unusual patterns show fraudulent activities.

In pursuance of identifying unexpected patterns that represent fraudulent activities, clustering methods are usually preferred. Clustering methods are also known as unsupervised machine learning techniques because of the information about clusters that intended to find is not present initially. After constituted clusters are analyzed and defined, hereby unexpected patterns can be unveiled. One can call these approaches as a form of learning by observation. Most frequently used clustering techniques are k-means and k-medoids. Those are based on the distances between investigated objects and they are frequently used in image pattern recognition, artificial intelligence-based applications and web searches (Han *et al.*, 2012). Only a few examples are seen in financial fraud detection. Mainly, supervised machine learning techniques like SVMs, NB, BN, discriminant analysis, NN, Evolutionary algorithms (EA), k-NN, Fuzzy Classifiers, and DT, as classification methods are engaged in pattern recognition in financial fraud cases. In the classification perspective, one has prior information about the definition of fraudulent patterns. In some cases, these patterns (classes) can be defined as rule sets or relational models. According to the nature of the problem, the equivalent technique can be applied. DT, NB, NN, EA, probabilistic methods such as HMM, and k-NN algorithms are some of the common classification techniques in financial fraud detection along with logistic regression. Normally, logistic regression is counted as one of the approaches in generalized linear models in which the dependent variables can be either numerical or categorical, is usually utilized with classification purposes in practice.

Mining frequent patterns contribute to the identification of uncovering associations and correlations within the data. Since Association analysis is a leading technique in rule induction, it is also useful for searching for relationships between variables and sequential patterns. Even though the use of association analysis is relatively common in marketing as market basket analysis, applications in financial fraud detection are noted as link analysis for detecting non obvious relationships and associations (Westphal, 2008). As far as the association rules or sequences of items derived, they start to play an important role in a transaction database. For example, with the help of referred rules, the patterns or structure of some covered network of investors can be revealed (Nisbet *et al.*, 2018).

## Outlier Detection

Apart from aforementioned approaches, outlier detection is used to find unexpected and unusual patterns within a data set. In financial fraud detection, revealing “outliers” is applicable to differentiate fraudulent subjects or cases from authentic data. Visualization techniques are also practical tools for identifying data anomalies, which may show potentially fraudulent transactions or trading schemes. In addition to visualization, regression analysis is useful to detect “normal” or “expected” observations before investigating the outliers.

Since clustering methods are mostly based on measuring distances from defined clusters, they can be used for outlier detection. In this perspective, defined outliers mean different than common cases. Examples of outlier detection cover credit card fraud detection and investigation of criminal activities in electronic commerce (Han *et al.*, 2012). According to Aggarwal and Yu (2005) many outlier detection

algorithms are either distance-based or density-based. Considering the financial data that has a high dimensional nature, Ngai *et al.* (2011) stated that there is a research gap in the applications of outlier detection techniques for financial fraud detection.

### **Text-Mining**

Text mining can be classified as an interdisciplinary field that covers essentially the similar approaches of data mining to the compilation of textual data in a deliberate structure. Since previous surveys on text mining have an attempt to handle financial statements fraud, contemporary text analysis applications are interested in group dynamics such as social network analysis. One of the examples with predictive purposes belongs to Vu *et al.* (2012). They generated a detection model of stock price movements of based on messages in Twitter with the help of Sentiment Analysis. Bollen *et al.* (2011) derived feedbacks from Twitter messages about the Dow Jones Industrial Average and their results showed that the Dow Jones predictions were increased by the involvement of different mood dimensions. Although this approach is highly useful for fraud types with large amounts of textual data, there are only a few practices noted in securities fraud detection (Kumar & Ravi, 2016). Zaki *et al.* (2011) demonstrated a fraud ontology by processing all document types related to securities transactions on the markets. In addition, Teoh *et al.* (2019) proposed text analytics to discover abnormal stock movements by using deep learning algorithms.

## **CONCLUSION AND FUTURE RESEARCH DIRECTIONS**

Investors, market professionals and regulators are involved in seeking alternative data mining techniques to detect fraudulent transactions and stock market manipulations. These techniques can handle large volumes and varieties of financial data to detect fraudulent activities. However, data mining involved autonomous intelligence application in securities fraud detection is a challenging attempt in practice. Considering a financial data set involving such transactions, the data becomes massive and multidimensional nature in spatio-temporal domain. It is also a common challenge that data labeling is very rare in fraud detection. Data preprocessing in labeling is time consuming and requires expert investigation.

As far as we know, pattern recognition in large datasets involves some special methods that are eligible to use within the database systems. In order to achieve fraud detection, there is a need for transformation of data into a proper structure. Data preprocessing, which involves database management, modeling, and inference, is an important function to manage data. Contemporary approaches implied dynamic (real-time) analyses with such combinations of different machine learning algorithms called as hybrid techniques. For example, both Saldanha and Omar (2019), Castro and Teodoro (2019) proposed to use machine learning approaches to create a learning database in order to detect patterns with the help of predefined rule sets.

Nowadays, computer processors and data storage alternatives are getting widely available with low-cost and information technologies that are rising their capabilities in integrating big data. However obtaining data quality remains its vital importance. Hence the quality of data plays a crucial role in the accuracy and reliability of securities markets monitoring systems. In the finance industry, simple errors directly affect the quality of analysis. Therefore, practitioners should evaluate the data before investigation process and minimize errors or inconsistencies by facilitating data analytics.

## DISCLAIMER

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

- ACFE. (2020a). *Global study on occupational fraud and abuse*. ACFE Publication.
- ACFE. (2020b). *Fraud examiners manual*. ACFE Publication.
- Aggarwal, C. C., & Yu, P. S. (2005). An effective and efficient algorithm for high-dimensional outlier detection. *The VLDB Journal*, 14(2), 211–221. doi:10.1007/00778-004-0125-5
- AICPA. (2019). *AICPA professional standards*. Wiley.
- Alexander, C., & Cumming, D. (2020). *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation*. Wiley.
- (2011). An Intrusive World. In Curley, R. (Ed.), *Issues in Cyberspace: From Privacy to Piracy* (pp. 45–60). Britannica Educational Publishing.
- Arnett, G. W. (2011). *Global Securities Markets*. Wiley. doi:10.1002/9781118258385
- Bainbridge, S. M. (2001). *The Law and Economics of Insider Trading: A Comprehensive Primer*. SSRN Electronic Journal. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=261277](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=261277) doi:10.2139/ssrn.261277
- Beg, M. O., Awan, M. N., & Ali, S. S. (2019). Algorithmic Machine Learning for Prediction of Stock Prices. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 142–169). IGI Global. doi:10.4018/978-1-5225-7805-5.ch007

- Benson, M. L., & Simpson, S. S. (2014). *Understanding white-collar crime: An opportunity perspective*. Routledge. doi:10.4324/9780203762363
- Bollen, J., Mao, H., & Zeng, X. (2011). Twitter mood predicts the stock market. *Journal of Computational Science*, 2(1), 1–8. doi:10.1016/j.jocs.2010.12.007
- Castro, P. A. L., & Teodoro, A. R. (2019). A Method to identify anomalies in stock market trading based on Probabilistic Machine Learning. *Journal of Autonomous Intelligence*, 2(2), 42–52. doi:10.32629/jai.v2i2.44
- CESR. (2020). *Market abuse*. European Securities and Markets Authority. Retrieved from <https://www.esma.europa.eu/sections/market-abuse>
- CFA. (2014). Retrieved from <https://www.cfainstitute.org>
- Croall, H. (2010). Middle-Range Business Crime: Rogue and Respectable Businesses, Family Forms and Entrepreneurs. In F. Brookman, M. Maguire, H. Pierpoint, & T. Bennett (Eds.), *Handbook on crime*. Willan Publishing.
- Crown. (2012). *The Wheatley Review of LIBOR*. UK Treasury Publications. Retrieved from <https://assets.publishing.service.gov.uk/>
- Dhanalakshmi, S., & Subramanian, C. (2014). An analysis of data mining applications for fraud detection in securities market. *International Journal of Data Mining Techniques and Applications*, 3(1), 9–1. doi:10.20894/IJDMTA.102.003.001.003
- Diaz, D., Theodoulidis, B., & Sampaio, P. (2011). Analysis of stock market manipulations using knowledge discovery techniques applied to intraday trade prices. *Expert Systems with Applications*, 38(10), 12757–12771. doi:10.1016/j.eswa.2011.04.066
- Diih, S. S. (2005). *The infiltration of the New York's financial market by organised crime: pressures and control* [Unpublished Ph.D. Dissertation]. Cardiff University.
- Esen, M. F., Bilgic, E., & Basdas, U. (2019). How to detect illegal corporate insider trading? A data mining approach for detecting suspicious insider transactions. *Intelligent Systems in Accounting, Finance & Management*, 26(2), 60–70. doi:10.1002/isaf.1446
- Ferdousi, Z., & Maeda, A. (2006). Unsupervised outlier detection in time series data. In *22nd International Conference on Data Engineering Workshops (ICDEW'06)* (pp. 51–56). IEEE. 10.1109/ICDEW.2006.157
- Fischel, D. R., & Ross, D. J. (1991). Should the Law Prohibit 'Manipulation' in Financial Markets? *Harvard Law Review*, 105(2), 503–553. doi:10.2307/1341697
- Gee, J., & Button, M. (2019). *The financial cost of fraud*. Retrieved from <http://www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf>
- Gilsinan, J. F., Millar, J., Seitz, N., Fisher, J., Harshman, E., Islam, M., & Yeager, F. (2008). The role of private sector organizations in the control and policing of serious financial crime and abuse. *Journal of Financial Crime*, 15(2), 111–123. doi:10.1108/13590790810866854

- Golmohammadi, K., & Zaiane, O. R. (2012). Data mining applications for fraud detection in securities market. *2012 European Intelligence and Security Informatics Conference*, 107-114. 10.1109/EISIC.2012.51
- Golmohammadi, K., & Zaiane, O. R. (2015). Time series contextual anomaly detection for detecting market manipulation in stock market. *IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 1-10. 10.1109/DSAA.2015.7344856
- Golmohammadi, K., Zaiane, O. R., & Díaz, D. (2014). Detecting stock market manipulation using supervised learning algorithms. *International Conference on Data Science and Advanced Analytics (DSAA)*, 435-441. 10.1109/DSAA.2014.7058109
- Gottschalk, P. (2018). Fraud Examiners in Private Investigations of White-Collar Crime. In *Fraud and Corruption* (pp. 213–235). Springer. doi:10.1007/978-3-319-92333-8\_11
- Gray, G. L., & Debreceeny, R. S. (2014). A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. *International Journal of Accounting Information Systems*, 15(4), 357–380. doi:10.1016/j.accinf.2014.05.006
- Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques*. Morgan Kaufmann Publishers.
- Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Support Systems*, 46(4), 853–864. doi:10.1016/j.dss.2008.11.013
- Humke, J. (1997). Comment, The Misappropriation Theory of Insider Trading: Outside the Lines of Section 10(b). *Marquette Law Review*, 80(3), 819–852.
- IOSCO. (2000). *Investigating and prosecuting market manipulation*. International Organization of Securities Commissions Report. Retrieved from <https://www.iosco.org/>
- Islam, S. R. (2018). *A Deep Learning Based Illegal Insider-Trading Detection and Prediction Technique in Stock Market*. Retrieved from <https://www.semanticscholar.org/paper/A-Deep-Learning-Based-Illegal-Insider-Trading-and-Islam/ffb4bf38805fdf58bcd3aba7829b379996f24059>
- Jones, M. J. (2012). *Creative Accounting, Fraud and International Accounting Scandals*. Wiley. doi:10.1002/9781119208907
- Kapardis, M. K. (2016). *Corporate Fraud and Corruption*. Palgrave MacMillan. doi:10.1057/9781137406439
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Kou, Y., Lu, C., Sirwongwattana, S., & Huang, Y. (2004). Survey of fraud detection techniques. *IEEE International Conference on Networking, Sensing & Control*, 749–754.
- Kumar, B. S., & Ravi, V. (2016). A survey of the applications of text mining in financial domain. *Knowledge-Based Systems*, 114, 128–147. doi:10.1016/j.knosys.2016.10.003

## ***Approaches to Detect Securities Fraud in Capital Markets***

- Lee, W., & Stolfo, S. (1998). Data mining approaches for intrusion detection. *Proceedings of the 7th USENIX Security Symposium*. Retrieved from [https://www.usenix.org/legacy/publications/library/proceedings/sec98/full\\_papers/lee/lee.pdf](https://www.usenix.org/legacy/publications/library/proceedings/sec98/full_papers/lee/lee.pdf)
- Levi, M. (2009). White-Collar Crimes and the Fear of Crime: A Review. In S. S. Simpson & D. Weisburd (Eds.), *The criminology of white-collar crime* (pp. 79–109). Springer. doi:10.1007/978-0-387-09502-8\_5
- Markham, J. (2014). *Law Enforcement and the History of Financial Market Manipulation*. Routledge.
- McGeever, J. (2017). *Timeline - The global FX rigging scandal*. Retrieved from <https://www.reuters.com/article/global-currencies-scandal/timeline-the-global-fx-rigging-scandal-idUSL5N1F14VV>
- Mongkolnavin, J., & Tirapat, S. (2009). Marking the close analysis in the Thai bond market surveillance using association rules. *Expert Systems with Applications*, 36(4), 8523–8527. doi:10.1016/j.eswa.2008.10.073
- Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569. doi:10.1016/j.dss.2010.08.006
- Nisbet, R., Miner, G., & Yale, K. (2018). Advanced Algorithms for Data Mining. *Handbook of Statistical Analysis and Data Mining Applications*, 149–167. doi:10.1016/B978-0-12-416632-5.00008-6
- Öğüt, H., Doganay, M., & Aktas, R. (2009). Detecting stock-price manipulation in an emerging market: The case of Turkey. *Expert Systems with Applications*, 36(9), 11944–11949. doi:10.1016/j.eswa.2009.03.065
- Palmer, A. (2017). *Countering economic crime: a comparative analysis*. Routledge. doi:10.4324/9781315227122
- PwC. (2020). *Global economic and fraud survey of 2020*. Retrieved from <https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf>
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.
- Rayes, J., & Mani, P. (2019). Exploring Insider Trading Within Hypernetworks. In P. Haber, T. Lampoltshammer, & M. Mayr (Eds.), *Data Science – Analytics and Applications*. Springer. doi:10.1007/978-3-658-27495-5\_1
- Reurink, A. (2018). *Financial Fraud: A Literature Review*. Max Planck Institute for the Study of Societies.
- Rose, P. S., & Marquis, M. H. (2006). *Money and Capital Markets: Financial Institutions and Instruments in a Global Marketplace*. McGraw-Hill.
- Rukmi, A. M., & Soetrisno, W. A. (2019). Role of clustering based on density to detect patterns of stock trading deviation. *Journal of Physics: Conference Series*, 1218(1).

- Sekmen, T., & Hatipoglu, M. (2019). FinTech and Stock Market Behaviors: The Case of Borsa Istanbul. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 170–205). IGI Global. doi:10.4018/978-1-5225-7805-5.ch008
- Silverstone, H., Sheetz, M., Pedneault, S., & Rudewicz, F. (2004). *Forensic Accounting and Fraud Investigation for Non-experts*. Wiley.
- Song, Y., Cao, L., Wu, X., Wei, G., Ye, W., & Ding, W. (2012). Coupled behavior analysis for capturing coupling relationships in group-based market manipulations. *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, 976-984. 10.1145/2339530.2339683
- Straney, L. L. (2011). *Securities Fraud: Detection, Prevention, and Control*. Wiley.
- Strumeyer, G., & Swammy, S. (2017). *The Capital Markets: Evolution of the Financial Ecosystem*. Wiley. doi:10.1002/9781119220589
- Tamersoy, A. (2016). *Graph-based algorithms and models for security, healthcare, and finance* [Unpublished Doctoral dissertation]. Georgia Institute of Technology.
- Tamersoy, A., Xie, B., Lenkey, S. L., Routledge, B. R., Chau, D. H., & Navathe, S. B. (2013). Inside insider trading: Patterns & discoveries from a large scale exploratory analysis. In *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (pp. 797-804). Retrieved from <https://ieeexplore.ieee.org/document/6785794>
- Tang, J., & Karim, K. E. (2018). Financial fraud detection and big data analytics – implications on auditors' use of fraud brainstorming session. *Managerial Auditing Journal*, 34(3), 324–337. doi:10.1108/MAJ-01-2018-1767
- Teoh, T., Lim, W. T., & Nguwi, Y. Y. (2019). From Technical Analysis to Text Analytics: Stock and Index Prediction with GRU. In *IEEE International Conference on Cybernetics and Intelligent Systems and IEEE Conference on Robotics, Automation and Mechatronics*, (pp. 496-500). Bangkok: IEEE.
- Vu, T. T., Chang, S., Ha, Q. T., & Collier, N. (2012). An experiment in integrating sentiment features for tech stock prediction in twitter. *Workshop on Information extraction and entity analytics on social media data*, 23–38.
- Wang, W., & Steinberg, M. (2010). *Insider Trading*. Oxford University Press.
- West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47–66. doi:10.1016/j.cose.2015.09.005
- Westphal, C. (2008). *Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies*. CRC Press. doi:10.1201/9781420067248
- Westphal, C., & Blaxton, T. (1998). *Data mining solutions: Methods and tools for solving real-world problems*. John Wiley & Sons, Inc.
- Yan, S., & Yan, D. (2019). Volatility Estimation in the Era of High-Frequency Finance. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 99–141). IGI Global. doi:10.4018/978-1-5225-7805-5.ch006

## ***Approaches to Detect Securities Fraud in Capital Markets***

Ye, T. (2017). Stock forecasting method based on wavelet analysis and ARIMA-SVR model. *3rd International Conference on Information Management*, 102-106. 10.1109/INFOMAN.2017.7950355

Zaki, M., Theodoulidis, B., & Solís, D. D. (2011). “Stock-touting” through spam e-mails: A data mining case study. *Journal of Manufacturing Technology Management*, 22(6), 770–787. doi:10.1108/17410381111149639

Zhang, D., & Zhou, L. (2004). Discovering golden nuggets: Data mining in financial application. *IEEE Transactions on Systems, Man, and Cybernetics. Part C*, 34(4), 513–522.

## **ADDITIONAL READING**

Commerce and Trade Act, 15 U.S.C. 2B (2006).

Crimes and Criminal Procedure Act, 18 U.S.C. 1001 (2011).

SEC. (2019). *Litigation releases*. Retrieved from <https://www.sec.gov/litigation/litreleases.shtml>

SEC. (2020). *Broker-Dealers*. Retrieved from <https://www.sec.gov/>

## **KEY TERMS AND DEFINITIONS**

**Association of Certified Financial Crime Specialists (ACFCS):** An international organization that offers certificate for applicants with documented academic and professional qualifications on financial crime detection.

**Financial Fraud:** Fraud has an elusive concept in finance and accounting literature, and it is generally attributed to white-collar crime that refers to false representation or suppression of a material fact with a purposeful intent to deceive and induce another.

**Insider Trading:** Illegal practices that are generally orchestrated by management or the people who have a positional power or preferential access to private information.

**Market Manipulation:** Manipulation in securities markets refers to the deliberate interference in the prices by artificially altering supply and demand function of the market.

**Pattern Recognition:** Analytical approaches that detect trends, sequences, or relationships within a dataset.

**Securities Market:** securities market is defined as a tradeable financial asset that refers to a manifestation of promise by an issuer to pay interest and return capital, or share ownership of a company. It encompasses equity, debt, and derivatives markets.

**Text Mining:** This term covers essentially the similar approaches of data mining to the compilation of textual data in a deliberate structure.



# Chapter 18

## Capital Market Frauds: Concepts and Cases

**Shailendra Singh**

*Capital Market Consultants, India*

### ABSTRACT

*In recent times there has been a significant development in financial markets that include global integration, internet-based trading, and financial innovation to name a few. Now financial markets are more sophisticated, diversified, and internationalized than ever. During the last decade, as a result of the Enron and WorldCom scandals, numerous legislations, amendments, and restructuring policies are introduced across the world. This chapter mainly covers various aspects of capital market frauds, manipulation practices, and country case studies from global financial markets. The chapter also highlights international regulatory frameworks, guidelines, and challenges being faced by the regulatory authorities. Fraud detection mechanisms and opportunities for the future are also discussed.*

### INTRODUCTION AND BACKGROUND

Scandals like Enron and WorldCom had a massive effect on the world economic system. As a result of this economic turmoil, numerous legislations, amendments, and restructuring policies are introduced across the world. Market abuse made headlines during the last few decades. Besides a primary reason of the massive scandals, market abuse is also a major cause for capital market manipulations (Dohadwala, 2019). It is natural that investors are concerned about the quality, transparency and integrity so designing of proper legislation is significant in order to ensure that the market for financial services exhibits all these traits. However, there has been a debate about how to define and measure market manipulation scope of its prohibition. All market players always look for flexible rules, loose government controls and least interference economic particularly for dealing rules.

Financial markets have a vital role in our economic system and is a marketplace for sale and purchase of financial securities, commodities, and other comparable items of value. The financial market is a concept consisting of different markets depending on the categorization used, such as capital markets, which in turn consist of securities market. In recent times there has been a significant development in

DOI: 10.4018/978-1-7998-5567-5.ch018

## **Capital Market Frauds**

financial markets that include global integration, internet-based trading, and financial innovation to name a few. Now financial markets are more sophisticated, diversified and internationalized than ever.

## **REGULATIONS<sup>1</sup>**

### **Purpose of Regulations**

Regulator to act in response to the perceived need for rules. Regulation is required when market solutions are inadequate for a variety of reasons. Understanding the purpose of these regulation makes it easier for the industry participants to anticipate and meet regulatory needs.

The broad objectives of regulation include the following:

### **Safeguarding the Customers**

In financial services industry, there are different types of consumers and the regulations are required to safeguard all Investors, depositors and borrowers etc. from any abusive practices including capital market frauds - in the financial markets. Regulators normally prevent investment firms from the sale of the complex or high-risk investment to individuals. Regulations also require the investment managers to provide the caution notice to investor such as “Investment is subject to market risk”.

### **Economic Growth and Stability**

Economic growth and stability are dependent on productive uses of capital. The financial markets bridge the gap between suppliers of capital and users of Capital (companies and governments). Regulator seeks to ensure a healthy financial market in order to stimulate economic development. The regulator is also trying to reduce risk in the financial markets. Due to excessive use of debt in the financial markets, there is always a risk of system failure that may derail the economy. As a result, credit facility may be suspended or substantially reduced due to collapse of financial markets. So, regulations are required to ensure to prevent financial system failure that may lead to economic disability.

### **Fairness**

All the market participants do not have the same set of information. Financial product seller may choose not to convey adverse information about financial instruments such as risk factor of the products they sell. Insiders who know more than the rest of the market might trade based on their insider information. This information irregularity may discourage investors from investments which eventually detriment the economic growth. Regulations are required to deal with this unpublished price sensitive information by demanding the fair and full disclosure of relevant information in a timely manner. So strict action against the insider trading is also expected. Regulators should maintain a “fair and orderly” market to minimize an unfair advantage for any market participant.

## Social Up-Lifting

Governments can use regulation to achieve social goals. These objectives could include increasing the provision of credit financing to certain needy groups, encourage home ownership through various government schemes, or increasing the interest rate on saving instruments such as national savings rate. Other social purpose is to prevent criminals from using the company in the financial services industry for the transfer of money from illegal operations to, other legal activities - a process known as money laundering (Saeed, Mubarik & Zulfiqar, 2021). As a consequence of the transfer, the money to be “clean”. Regulations helps to prevent money laundering, detecting criminal activity and prosecute individuals involved in illegal activities (Amjad, Arshed & Anwar, 2021).

## REGULATORY PROCESS

The process was developed where the rules vary from jurisdiction to jurisdiction and even within jurisdictions. This section describes the steps involved in a typical regulatory process and comparing different types of regulatory regime.

Figure 1 depicts the steps in a typical regulatory process, from the need for regulation to its implementation and enforcement.

*Figure 1. Regulatory Process*

*Source: CFA Institute Investment Foundation*



## NEED IDENTIFICATION

Regulations develop in response to the perceived needs. Perception will come from numerous sources. Perhaps, for instance, be political pressure on the govt. to react the perceived defect within the financial markets, such as consumer protection is inadequate. Market veterans of capital market industry may try to influence regulatory bodies to recommend rules advantageous to the interests of their clients. Rules can be developed proactively in anticipation of future needs; or regulations will be developed reactive in response to a scandal or other problems.

## **IDENTIFICATION OF LEGAL AUTHORITY**

During this step, the regulatory body/bodies is/are identified which is/are responsible for implementation of regulations.

## **NEED ANALYSIS**

Once the needs are identified, regulators do careful analysis. Regulators consider various regulatory approaches that can be used to achieve the desired results. Possible approaches include a mandate and / or restrict certain behaviors, defining the rights and responsibilities of certain parties, and impose taxes and subsidies to influence behavior. The analysis carefully weighs the costs and benefits of the proposed regulation, although the advantage is often difficult to quantify. Regulations impose costs, including direct costs incurred to hire people and construction systems to attain compliance, monitor compliance, and enforce regulations. This fee increases the price of ongoing operations of regulators and companies, among others. A regulation could also be effective in resulting the required behaviors but it is not very efficient considering the price associated with it.

## **PUBLIC OPINION**

Relevant Regulators ask for public opinion about proposed regulations. This public consultation offers the chance to collect a suggestions and comments about the problem. This step is a valid method to enhance the standard and applicability of the regulations. A regulation might bear multiple rounds of proposal, consultation and amendments before it is adopted for implementation.

## **ADOPTION**

After accommodating all proposals and suggestions, the regulation is formally adopted by the regulator. Supporting guidelines for successful adoption are also issued by the regulatory authority. Companies or individuals who do not comply with the regulations are at a risk of violation (Sinha, 2021).

## **IMPLEMENTATION**

Some rules apply immediately and some are phased in over time. Because the company has an obligation to comply with the new regulations that are relevant, they need to monitor information from regulators and act on change. Sometimes regulators contact the company directly about the new rules, but not always.

## **MONITORING AND ENFORCEMENT**

Regulators monitor firms and entity to assess the compliance of regulations and possibility of any prohibited activities (Rafay, 2021). It also includes routine examinations of companies, investigation of complaints, and special monitoring of specific activities. For example, regulators may routinely investigate all stock purchases just before a takeover announcement to identify any insider trading (Garfinkel & Nimalendran, 2003). There are systems in place for receiving and investigating complaints about violations. Regarding enforcement, it is also in place in all regulatory regimes in order to identify and punish lawbreakers. Examples are heavy penalties, license suspension and imprisonment in some cases.

## **DISPUTE RESOLUTION**

Arbitration process is useful to sort out disputes. An effective dispute resolution system is managed by the regulator to improve the market reputation and to promote the economic efficiency. Alternative dispute resolutions prove very useful to resolving disputes fastly and economically by avoiding court cases.

## **PERPETUAL REVIEW AND UPDATING**

Regulations needs to amend or modified to match the pace in the investment industry. For this purpose, an effective regulatory system must have its review procedures in place to determine the effectiveness and identify the proposed amendments.

## **REGULATORY REGIME CLASSIFICATION**

There are certain types of regulatory regimes which are classified on the basis of different geographies. These are important to understand for an individual or particularly for a company who operates at a global level. Regulatory regimes are often described as:

### **PRINCIPLES-BASED**

Principles-based regulation doesn't specify a methodology or any procedure that an entity must follow instead these are defined as the guiding principles that must adhere by the investment industry and it is expected from them to operate within that arena.

### **RULES-BASED**

Regulations that apply systematically to all financial establishments. Rules around client engagements are usually applicable in this manner, ensuring an identical treatment of customers regardless the size of the firm providing those service.

## **MERIT-BASED**

Sometimes, regulators attempt to ensure investor protection and market integrity by limiting the products sold to clients. For example, a regulator may decide that a firm should sell its hedge fund product based on investor risk profile because it is highly risky (Jayasekara, 2021). Hedge funds investment should always be restricted to investors that have a certain level of risk appetite and investment expertise.

## **DISCLOSURE-BASED**

In this regulator seeks to ensure whether the investment is appropriate for investors, but only when all material information is disclosed to investors. The philosophy behind disclosure-based regulations is that properly informed investors can make their own determinations regarding whether the potential return of an investment is worth the risk.

## **REGULATORY FRAMEWORK**

Across the globe several financial institutions have been adhering to many market regulations (Shah, 2021). Since 2008 sub-prime crises, there has been increase in this number. It is mandatory for all global investment banks to implement these new regulations effectively. Within defined deadline firms need to sufficiently analyze and harmonize multiple compliance initiatives. These regulatory frameworks are required for investment firms operating across the globe and are aimed at achieving more transparency and greater protection for investors.

## **MARKETS IN FINANCIAL INSTRUMENTS DIRECTIVE (MIFiD/MiFID II)**

### **Scope of MIFiD/MiFID II**

Markets in Financial Instruments Directive II (MiFID II) regulate financial markets in the EU bloc and improve protections for investors. Its aim is to standardize practices across the EU and restore confidence in the industry, especially after the 2008 financial crisis. MiFID II came into force on January 3, 2018, representing one of the biggest changes in regulatory oversight of financial markets for a decade. The regulation extended the responsibility and scope of its predecessor, the original MiFID that was introduced in 2007 and its aim was to improve the competitiveness in European markets by creating a single transparent market for investment services and activities, and ensuring harmonized investor protection across Europe (ESMA, 2020). Technically, MiFID II applies to the legislative framework, and the rules it outlines are actually the Markets in Financial Instruments Regulation (MiFIR); but colloquially, the term MiFID is used to mean both (Stafford, 2017).

The MiFID II regulation amends many previous provisions covering the conduct of business and organizational requirements for providers of investment services and specifies requirements and organizational rules that must be applied to different types of trading venues. (Thomson Reuters, 2020). MiFID rules that were limited to equities trading on regulated platforms are extended to equity like and

non-equity instruments traded on any trading platform, including multilateral trading facilities (MTFs) and organized trading facilities (OTFs), with a view to ensuring that all trading takes place on regulated platforms. Systematic internalizers that trade Over the Counter (OTC) derivatives are subject to expanded transparency obligations. Table 1 highlights the significant milestones of MiFID II.

*Table 1. Significant Milestones*

October 26, 2012	European Parliament approves MiFID II
May 13, 2014	EU Council adopts Level 1 text
July 2, 2014	MiFID II enters into force
September 28, 2015	ESMA publishes final report on Regulatory Technical and Implementing Standards
February 10, 2016	European Commission proposes one-year delay
June 7, 2016	European Parliament confirms delay
November 10, 2016	ESMA issues draft Regulatory Technical Standards for package orders
July 3, 2017	Transposed into national law for Members State
January 3, 2018	MiFID II apply within Members State

Source: <https://www.thomsonreuters.com/en.html>

## Challenges for MIFiD/MiFID II

Following are some of the important challenges which are being faced by MiFID II

- Manage high complexity of affected functions, regions, legal entities and clients
- Increase standardization grade of a diverse systems landscape to enable integration
- Collect data for various functions and stakeholders for reporting
- Adjustment of the IT-infrastructure to report additional securities' data
- Increase level of data granularity and quality to comply with regulatory requirements
- Re-design organization and processes to enable implementation
- Increased “cost to serve” through expenditures necessary to comply with new directive

## THE EUROPEAN MARKETS INFRASTRUCTURE REGULATION (EMIR)

### Scope of EMIR

The European Markets Infrastructure Regulation (EMIR) regulates the European derivative markets, central counterparties (CCPs) and trade repositories (TRs). It sets requirements for the authorization, registration, organization and supervision of European TRs. EMIR Legislation was implemented in 2014 (DTCC, 2020). EMIR is the European Union's response to the G20 Pittsburgh agreement of 2009 to clear and report all over-the-counter (OTC) derivative contracts by end of 2012. It entered into force on 16 August 2012 (EC, 2020). The basic purpose of this directive is to improve the transparency of OTC

## Capital Market Frauds

derivatives markets and reducing the risks associated with those markets. There are certain regulations in this regard. Table no. 2 highlights the significant milestones of EMIR (Europex, 2020a).

- OTC derivatives which meet certain requirements are subject to a clearing obligation;
- Risk mitigation techniques must be applied in respect of all OTC derivatives that are not centrally-cleared; and
- All derivatives transactions must be reported to TRs.

*Table 2. Significant Milestones (EMIR)*

August 16, 2012	Effective date
February 12, 2014	First reporting deadline
May, 2015	European Commission launches review of legislation
June 21, 2016	First clearing deadline
September 1, 2016	First margin requirements deadline
January, 2017	EMIR 1.5 is adopted
November, 2017	Compliance with EMIR 1.5
June 12, 2018	European Parliament votes to make changes to EMIR that are likely to result in EMIRII
Sept 26, 2018	ESMA issues updated Q&A regarding EMIR implementation
May 28, 2019	ESMA issues updated Q&A regarding the EMIR Refit
June 17, 2019	EMIR Refit enters into force

Source: <https://ec.europa.eu>

## Challenges for EMIR

Following are some of the important challenges which are being faced by EMIRII

- Increase level of data granularity and quality to meet regulatory requirements
- Cope with increased data volumes resulting from additional archiving and reporting regulations
- Adjust the IT-infrastructure to report additional data on securities
- Contractual review of existing agreements with clearing brokers, collateral managers, and custodian banks
- Higher complexity of attributes as a result of more granular and sensitive data
- Profound implications of regulation for front offices and core systems
- Time constraints regarding information on OTC derivatives trades



## MARKET ABUSE REGULATION (MAR)

### Scope of MAR

Market Abuse Regulation (MAR) strengthens EU rules on market integrity and investor protection that were first adopted in the 2003 as Market Abuse Directive (MAD). The regulation aims to challenge insider dealing and market manipulation in Europe's financial markets and is part of an updated EU rulebook that also includes the Directive on Criminal Sanctions for Market Abuse (also known as Market Abuse Directive, or MAD). MAR has been applicable since July 3, 2016 (Europex, 2020b).

MAD II requires member states to provide harmonized criminal offenses of insider dealing and market manipulation and to impose the maximum criminal penalties of not less than 2 to 4 years in prison for the most serious violations of market abuse. MAR extends the market abuse regime to commodity derivative market and the manipulation of benchmarks which may also contain provision of High-Frequency Trading (HFT). Regulators will be garnished with greater investigative powers (EC, 2020b)

Table 3 highlights the significant milestones of EMIR.

*Table 3. Significant Milestones*

July 1, 2005	MAD implemented
December 12, 2012	MAR text approved by European Council
Sept 10, 2013	MAR endorsed by European Parliament
July 2, 2014	Effective date
November 11, 2014	ESMA issued two consultation paper concerning MAR i.e., 1) Draft technical advice on possible delegated acts, 2) Draft technical standards.
March 2, 2015	ESMA to provide technical advice to the commission on implementing acts concerning procedures for reporting infringements to competent authorities.
July 2, 2015	Deadline for ESMA to submit final draft RTS and implementing technical standard to the commission.
June 2, 2016	Publication in impending acts concerning procedures for reporting infringements to competent authorities.
July 3, 2016	MAR and implementing acts will apply; deadline for transposition of MADII into national law.
January 3, 2017	Compliance deadline

## TYPES OF FINANCIAL MARKET REGULATION

Regulation of financial institutions focus on the stability of the financial system, fair competition, consumer protection, and the prevention and reduction of financial crime. Each set of rules focuses on the type of investment industry activity. Following are some of the principles explained by the CFA Institute:

- Scrutiny and screening the investment professional are required to maintain the standards of integrity and competence. For this purpose, passing of certain licensing exam are required in many financial markets. This is directly linked with quality of professional advice provided by the investment managers to the potential investors.

## **Capital Market Frauds**

- Certain regulations are required to follow in order to operate in financial services industry. It may include, maintaining a certain level of net capital to ensure enough resources to honor obligations when required. High levered companies pose a high risk for all relevant stakeholders due to high chances of bankruptcy.
- Segregation of customer assets from the assets of investment manager is important to avoid any misuse of customers' valuable assets.
- All relevant information about company, risk, financial instruments should be disclosed. Rules define what information is mandatory to disclose. Specially, corporate issuers are required to disclose detailed information to potential buyers before the offering of securities. Some information regarding the justification of price of a security that is being offered, should be disclosed. In this regard, stock exchanges, on which the securities are being listed, may ask for some additional information. Any information disclosed or advertised should not be misleading.
- Conflict of interest may emerge in case of dual role of investment firms as these may be engaged in investment consultancy and investment research at the same time.
- Know your customer strategy or due diligence of customer is significant before starting any engagement with customer
- Regulators frame certain regulations in order to avoid abusive trade practices, e.g., insider trading, wash sales, pump and dump, front running, self-trading, soft money arrangements, money laundering etc.

## **MARKET MANIPULATION**

Market manipulation exists when someone artificially affects the supply or demand for security (for example, causing stock prices to rise or to fall dramatically). Market manipulation may involve techniques including Spreading false or misleading information about a company, engaging in a series of transactions to make security appear more actively traded; and rigging quotes, prices etc. (US-SEC, 2020a).

The issue of market manipulation exists in most of the global market and in almost all the asset class. There is a wide variety of manipulative strategies. The magnitude of these manipulative strategies can be multifold and it can severely hamper the investor confidence and the overall goodwill of the market. Some of the most recent example manipulative example which impacted the global market badly are LIBOR manipulation which come into the category of benchmark manipulation. These benchmarks underpin the pricing of hundreds of trillions of dollars worth of financial contracts and securities such as floating rate loans/bonds, swaps, forward rate agreements, futures, and options (Duffie and Stein, 2015). This manipulation exceeded the total market capitalization of all companies listed in US stock market. The outcome of such investigation could lead to billion-dollar fines including imprisonment. Such manipulation could be the tipping point for new legislative reforms and benchmark setting mechanism.

To overcome with market manipulation regulators enforcing the need of effective market surveillance systems. Markets surveillance is not a new requirement for financial institutions but it is becoming more complex by the day. All regulations including MAR and MiFID II dictate that firms must have comprehensive surveillance programs to detect and prevent market manipulation. MAR also raised the regulatory bar by broadening the definition of regulated asset classes requiring firms to monitor for cross-product and cross-market manipulation, as well as intent. Additionally, it's no longer sufficient just to have a market surveillance program in place. Some regulations also mandate that regulatory risk

management controls and supervisory procedures must be reasonably designed – which makes one-size-fits all approaches to market surveillance less viable. Compromising on markets surveillance comes at a high cost. As well as being fined and sanctioned for engaging in market manipulation, firms can also be penalized for not implementing reasonable measures to detect it in the first place. In today's increasingly regulated environment, there's no room for compromise.

## **TYPES OF MANIPULATION STRATEGIES**

The term “market manipulation” encompasses a wide variety of different strategies. To map out the relations between the various forms of market manipulation, Figure 2 provides the most common type of market manipulation.

At the broadest level, market manipulation can be divided into six categories: trade-based, information-based, order-based, behavior-based, submission-based, and auction-based. These categories and mechanisms are not mutually exclusive and there are also hybrid manipulation strategies that combine several of the individual techniques or elements of the techniques.

In the first category of market manipulation, Trade-based market manipulation involves instances where a member or candidate knew or should have known that his or her actions could affect the pricing of security. This type of manipulation includes transactions that artificially affect prices or volume to give the impression of activity or price movement in a financial instrument, which represent a diversion from the expectations of a fair and efficient market. Securing a controlling, dominant position in a financial instrument to exploit and manipulate the price of a related derivative and/or the underlying asset (US-SEC, 2020a). Information-based market manipulation includes spreading false rumors to induce trading by others e.g., pump and dump policy.

## **MANIPULATIVE AND FRAUDULENT PRACTICES**

### **Concept**

Manipulation is a kind of fraud where all the elements and ingredients of fraud apply to manipulative conduct. Investor's trust is eroded and economic growth is affected due to market manipulation. In the words of Supreme Court of India:

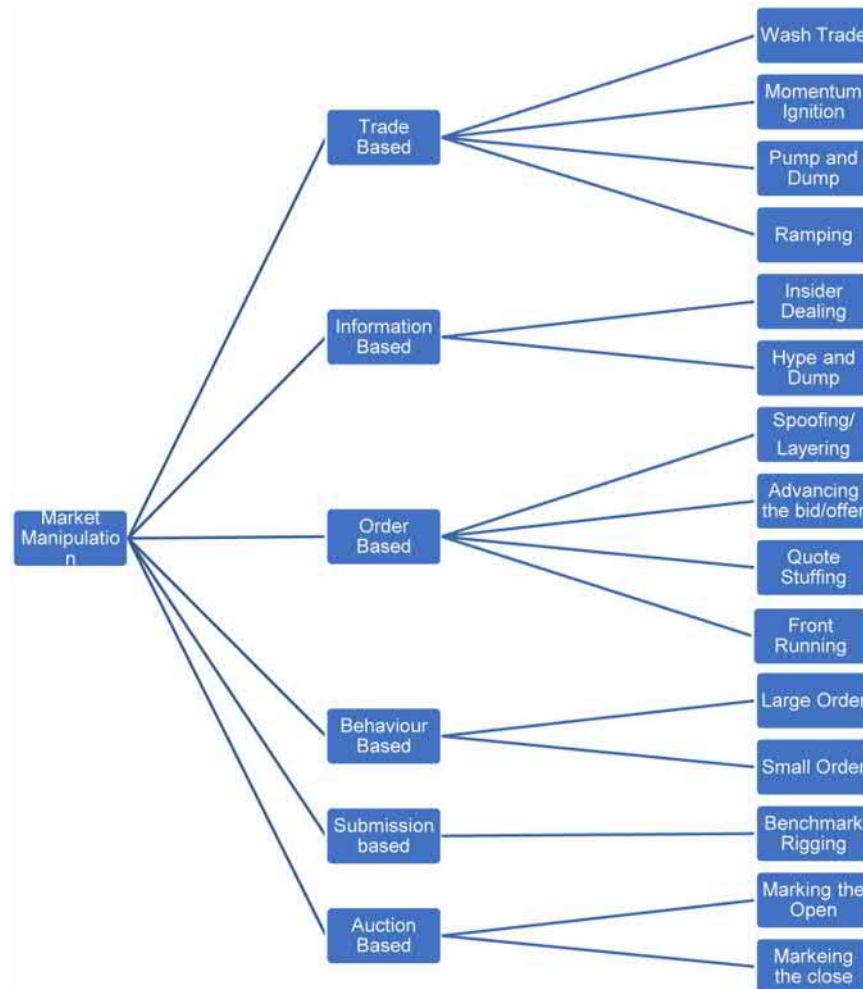
*Market abuse refers to the use of manipulative and deceptive methods, giving out incorrect or misleading information, so as to encourage investors to jump into conclusion, on wrong premises. The same can be achieved by inflating the company's revenue, profit, security deposits and receivables, resulting in price rise of scrip. Investors are then lured to make their investment decisions on those manipulated results. (Supreme Court of India, 2013).*

## **TYPES OF FRAUDULENT TRADING PRACTICES**

Some of the prominent fraudulent trading practices are listed below:

Figure 2. Types of Market Manipulation<sup>ii</sup>

Source: Author



### Wash Trading: Concept

Monetary Authority of Singapore defines Wash Sales as follows:

*Wash trades occur when there is a simultaneous purchase and sale of the same security where there is neither a change in the beneficial ownership nor a transfer of risk. Such trades artificially increase trading volumes or maintain prices, which may constitute false trading. (MAS, 2020)*

Wash trades disrupt the marketplace as a result of the over-inflated perception of trade volume. Organizations that leverage the illegal practice ultimately discredit their industry and destabilize the market. The above definition can be break down in two different sections:

- Due to wash sales, there are artificially inflated volumes that create a misleading impression of excessive liquidity to allure investors. In the words of US Securities and Exchange Commission:

*“Many investors may value this increase in the liquidity as a positive indicator for the relevant stock. In another set up, a manipulator initially gives a number of passive selling orders for the stock and then matches her own orders by giving binding buy orders. Thereby, manipulator can increase the price of the stock successively whereas there is no genuine change in the ownership of the shares. But in most of the cases, the other investors can not recognize this fact and perceive this movement as a regular rise in the stock price”*

- Due to wash sales, there are artificially inflated prices by using the nominee accounts by manipulators. They trade among accounts owned, essentially, by the same individual or group.

## Wash Trading: Case Study

See Box 1.

## Pump and Dump: Concept

“Pump and dump” manipulation Strategy is a two-step process. In the first, promoters try to boost the price of a stock with false or misleading statements about the company. Once the stock price has been pumped up, fraudsters move on to the second part, where they seek to profit by selling their own holdings of the stock, dumping shares into the market. Now a days, major source of this manipulation is internet by urging readers to buy a stock quickly. The message sender claims to have “inside” information about a development that will be positive for the stock. After these fraudsters dump their shares and stop hyping the stock, the price typically falls, and investors lose their money (US-SEC, 2020c).

Figure 3. Pump and Dump Process

Source: StockCharts



## Capital Market Frauds

### Box 1.

<b>Case Detail:</b> ADMINISTRATIVE PROCEEDING File No. 3-16316
<b>Respondents:</b> PAUL J. POLLACK AND MONTGOMERY STREET RESEARCH, LLC,
<p><b>Case Summary</b></p> <p>The SEC has charged Paul Pollack and his firm Montgomery Street Research LLC for engaging in wash trading to manipulate the stock price of a company and with acting as brokers for the company without the required SEC registration. Pollack and Montgomery Street Research were retained in two private placement offerings to raise capital for a company and to generate interest among investors in the stock. Trading in the company's shares was sparse. To drum up business, Pollack and Montgomery Research allegedly engaged in 100 wash trades of the company's stock over a one-year period. The misleading trading activity made it appear to investors that there was more trading activity in the shares than actually existed.</p>
<p><b>Case Detail</b></p> <p>Pollack had exclusive trading authority over at least ten online brokerage accounts at five broker-dealers. Seven of these accounts were in the name of three entities that Pollack solely-owned and controlled, including three accounts in the name of Montgomery Street; three accounts in the name of Toro Holdings; and one account in the name of Bhog Partners.</p> <p><u>Account Activity</u></p> <p>From December 31, 2010 through October 8, 2012, in open market transactions, the ten Pollack-controlled accounts had a following transactions in Arete Industries Inc.:</p> <p>Buy – 5,347,557 shares  Sell – 5,661,051 shares  Total 4,341 transactions were conducted on 300 trading days,  On 140 of the 300 trading days, the Pollack controlled accounts were responsible for over 50% of the trading volume in Arete Industries total trading volume.  On 19 of the 300 trading days, the Pollack controlled accounts were responsible for over 90% of the trading volume in Arete Industries total trading volume.  Some of the Pollack wash trades in Arete Industries on 15<sup>th</sup> August 2011, Pollack conducted eight wash trade in three separate accounts he controlled, and Pollack trading was responsible for about 99% of Arete Industries total reported volume. As per data, seven out of his eight wash trades were separated by 30 seconds or less.</p> <p><b>ACCOUNT TICKER ORDER DATE ORDER TIME TRADE TIME SELL/BUY PRICE QUANTITY</b></p> <p>Toro Holdings Account 1 ARET 08/15/2011 10:22:38 10:25:02 Buy \$3.25 200  Toro Holdings Account 1 ARET 08/15/2011 10:24:06 10:25:02 Buy \$3.25 1000  Montgomery St Account 1 ARET 08/15/2011 10:24:49 10:25:02 Sell \$3.25 1200</p> <p>Toro Holdings Account 1 ARET 08/15/2011 10:28:05 10:28:15 Buy \$3.30 500  Montgomery St Account 1 ARET 08/15/2011 10:28:11 10:28:15 Sell \$3.30 500</p> <p>Toro Holdings Account 1 ARET 08/15/2011 13:45:30 13:46:04 Buy \$3.20 1999  Montgomery St Account 1 ARET 08/15/2011 13:45:52 13:46:04 Sell \$3.20 2000</p> <p>Montgomery St Account 2 ARET 08/15/2011 13:50:12 13:50:55 Buy \$3.25 1500  Montgomery St Account 1 ARET 08/15/2011 13:50:27 13:50:55 Sell \$3.25 1500</p> <p>Montgomery St Account 1 ARET 08/15/2011 13:52:35 13:52:57 Buy \$3.30 500  Montgomery St Account 1 ARET 08/15/2011 13:52:45 13:52:57 Sell \$3.30 500</p> <p>Toro Holdings Account 1 ARET 08/15/2011 14:44:27 14:44:38 Buy \$3.49 501  Montgomery St Account 1 ARET 08/15/2011 14:44:34 14:44:38 Sell \$3.49 501</p> <p>Montgomery St Account 1 ARET 08/15/2011 14:44:34 14:45:50 Sell \$3.49 499  Toro Holdings Account 1 ARET 08/15/2011 14:45:28 14:45:50 Buy \$3.49 500</p> <p>Montgomery St Account 2 ARET 08/15/2011 15:10:17 15:11:05 Buy \$3.25 2000  Montgomery St Account 1 ARET 08/15/2011 15:10:47 15:11:05 Sell \$3.25 2000</p> <p>Pollack engaged in this manipulative strategy repeatedly. From approximately July 2011 through June 2012, Pollack conducted approximately 100 wash trades in "ARETE" stock where the buy/sell orders came within 90 seconds of one another, and where the price and quantity were identical or virtually identical. In 85 of those instances, the buy/sell orders came within 60 seconds of one another. In many cases, Pollack wash trade orders were placed only seconds apart.</p>

Source: US-SEC (2020b)

## Pump and Dump: Case Study

See Box 2.

Box 2.

<b>Case Detail:</b> Jason C. Nielsen (Release No. LR-24832 on Jun. 10, 2020)
<b>Respondents:</b> Jason C. Nielsen
<p><b>Case Summary</b></p> <p>During the COVID-19 pandemic, Defendant Jason C. Nielsen defrauded other investors for his personal profit. Specifically, from March 2, 2020 to April 13, 2020, Nielsen engaged in a “pump and dump” scheme involving the stock of Arrayit Corporation, a biotechnology company.</p> <p>Jason C. Nielsen owned approximately 10% in Arrayit Corp and defendant started posting numerous false and misleading statements on an internet forum that were designed to encourage other investors to buy Arrayit stock and, thereby, drive up the price of the stock. Nielsen then sold his shares of Arrayit stock at the artificially-inflated price and reaped the profit.</p>
<p><b>Case Detail</b></p> <p>In March and April 2020, the news cycle in America was saturated with reports and commentary on the severity of the COVID-19 virus, the need for accurate and rapid COVID-19 tests was severe, and there was a significant downturn in the stock market and global economy due to the COVID-19 pandemic.</p> <p>During this time, Jason C. Nielsen used an anonymous username, “PennyStock Alert,” to post messages on the internet forum, “Investors Hub” and promoting “Arrayit” stock claiming that they had a rapid COVID-19 test which was approved from the FDA.</p> <p><u>Account Activity</u></p> <p>On 2<sup>nd</sup> March 2020, Jason C. Nielsen held 114,803,532 shares of Arrayit stocks which represents 10.19% of total outstanding shares. Total market value of Nielson holdings was \$1,998,051.26.</p> <p>Actually, Jason C. Nielsen trading records reveal that he was dumping his shares close in time to when he was posting messages touting Arrayit’s stock.</p> <p><u>Fact</u></p> <p>Arrayit did not apply for Emergency Use Authorization to the FDA until on or about April 13, 2020. As per Nielsen’s statements, Arrayit’s pending application were false at the time they were made (before on or about April 13, 2020).</p> <p>With respect to his statements about Arrayit having an “approved” COVID-19 test, Nielsen either knew, or was reckless in not knowing, that these statements were false and misleading.</p>

Source: US-SEC (2020d)

## Insider Trading Manipulation: Concept

Insider trading is defined as the illegal buying and selling of investments, including stock, based on information that has not yet made public. Insider trading does happen as a direct result of access to privileged information, particularly in financial institutions and companies intimately involved in research and development, as well as the banking industry in general (Rafay *et al.*, 2016). By strict legal definition, insider trading is defined by United States Securities and Exchange Commission as under:

*“Illegal insider trading generally occurs when a security is bought or sold in breach of a fiduciary duty or other relationship of trust and confidence while in possession of material, nonpublic information.”*  
(US-SEC, 2020e)

## Insider Trading Manipulation: Case Study

See Box 3.

## Capital Market Frauds

### Box 3.

<b>Case Detail:</b> Financial Service Authority, London Vs Mr. David Massey, (Dated: 21 <sup>st</sup> Feb 2011)
<b>Respondents:</b> Mr. David Massey
<b>Case Summary</b> Massey was a corporate advisor to Eicom plc. He was aware that Eicom were to undertake an equity placing at a significant discount to the current market price. Massey shorted the stock ahead of that new issue and subsequently covered the position with new issue stock the lower price.
<b>Case Detail</b> On 1 November 2007, Mr. Massey possessed an insider information concerning Eicom plc (a company listed on the Alternative Investment Market of the London Stock Exchange). Eicom had expressed his willingness, short of a legally binding commitment, to issue up to 3 million shares (which is more than 9% of Eicom's existing issued share capital) at 3.5p per share (around a 59% discount to the market price) to Mr. Massey. Mr. Massey knew that it was very likely that Eicom would proceed to issue if he requested them to do so. By a series of emails, Mr. Massey agreed with Eicom that it would hold the offer to issue the shares open until 2 November 2007. On the morning of 1 November 2007, Mr. Massey sold 2.5 million Eicom shares to the third party for 8p per share. Almost immediately afterwards, Mr. Massey contacted Eicom stating that he would like to purchase 2.6 million Eicom shares at a price of 3.5p per share, as had previously been discussed. Eicom did issue the 2.6 million shares to Massey thereby enabling him to cover his short position on the 2.5 million shares he had sold earlier at 8p per share. This transaction resulted in Massey making a personal profit of £111,474.

Source: FSA (2009)

## Front Running Manipulation: Concept

Front-running is an unethical and illegal trading practice in which a broker with advance knowledge of a specific market order in a currency or other financial security for a client earns a profit by placing an order for their own account in advance of the client's larger order. Using this private information, a front runner places an order in advance of another client for personal unwarranted profit (CFI, 2020)

## Front Running Manipulation: Case Study

See Box 4.

## Marking the Close: Concept

Marking the close is a form of market manipulation involving the purchase or sale of an instrument near or at market close with the objective of artificially fixing the closing price. It gives the impression that the instrument is of a higher or lower value than what it actually is and is not a genuine reflection of market forces. As closing prices are regularly quoted as a measure of an instrument's price performance, a trader wishing to support or depress its price may attempt to enter orders and execute trades towards the end of the trading session and avoid trading in the other parts of the day where better prices may be available (Kyle & Viswanathan, 2008). This is a tactics by a trader to establish closing prices of an illiquid or thinly traded instrument. Trades executed outside of the closing routine may also set the closing price, in the absence of subsequent transactions. A trader that frequently trades close to or at the intraday high/low price for an instrument should warrant member's attention. The trading malpractices of marking the close can emerge as the execution of a series of trades over a period of time, depending on the traders' objective (Comerton-Forde & Putniņš, 2011).



## Box 4.

<b>Case Detail:</b> ITG Inc. and AlterNet Securities Vs Securities Exchange Commission
<b>Respondents:</b> ITG Inc. and AlterNet Securities
<p><b>Case Summary</b></p> <p>The SEC alleged that ITG Inc. operated an alternative trading system, commonly referred to as a dark pool, known as POSIT. AlterNet, an affiliate of ITG, provided trading algorithms and smart order routers that sent orders to various market centers including POSIT. According to the SEC, between April and July 2011, ITG operated a proprietary trading desk known as “Project Omega.” Project Omega accessed live feeds of ITG customer and POSIT subscriber order and execution information and traded algorithmically based on that confidential information in both POSIT and other market centers. The SEC claimed that as part of one of its trading strategies, Project Omega identified and traded with sell-side POSIT subscribers and ensured that those subscribers’ orders were configured in POSIT to trade “aggressively” so as to benefit Project Omega.</p>
<p><b>Case Detail</b></p> <p>This matter involves violations of the federal securities laws by ITG in the operation of its dark pool and its misuse of customer information between April 2010 and July 2011.</p> <p>ITG Inc. is the owner and operator of POSIT, an alternative trading system (“ATS”) commonly referred to as a “dark pool.” POSIT is not a registered national securities exchange, but is a private execution venue that accepts, matches, and executes orders to buy and sell equity securities that it receives from ITG customers and POSIT subscribers. As of March 31, 2015, POSIT was the ninth largest ATS as measured by dollar volume of executions with over \$109 billion in executions during the first quarter of 2015. During that same quarter, ITG executed trades for over 5.6 billion shares in POSIT.</p> <p>Between approximately April 2010 and July 2011, ITG violated the federal securities laws and regulations in multiple ways as a result of its operation of an undisclosed proprietary trading desk known within ITG as “Project Omega” (“Project Omega” or “Omega”). During the period of April to December 2010, Project Omega accessed live feeds of ITG customer and POSIT subscriber order and execution information and traded algorithmically based on that information in POSIT and in other market centers. In connection with one of its trading strategies, Project Omega identified and traded with sell-side subscribers in POSIT and ensured that those subscribers’ orders were configured in POSIT to trade “aggressively,” or in a manner that benefitted Omega by enabling it to earn the full “bid-ask spread” when taking the other side of their orders.</p> <p><u><i>Project Omega’s Revenues and Total Shares Traded</i></u></p> <ul style="list-style-type: none"> <li>• During the time period that Project Omega was in operation, from approximately April 2010 to July 2011, Project Omega traded a total of approximately 1.3 billion shares, including approximately 262 million shares traded with unsuspecting subscribers in POSIT in connection with the Facilitation Strategy.</li> <li>• ITG’s gross revenues from Project Omega’s trading activities totaled approximately \$2,081,304.</li> </ul> <p><u><i>Violations</i></u></p> <ul style="list-style-type: none"> <li>• ITG failed to make any disclosure regarding Project Omega or its proprietary trading activities either publicly or to any of its customers or prospective customers.</li> <li>• During the time period when Project Omega was in operation, ITG continued to market and promote itself publicly, as well as to customers and prospective customers, as an “agency-only” broker that did not engage in proprietary trading. ITG also promoted its products and services as “reducing market impact” and protecting against “information leakage” and “gaming” of customer orders.</li> <li>• ITG Failed to Restrict Access to POSIT Subscriber Information.</li> </ul>

Source: US-SEC (2018)

The following example illustrates, how marking the close may be carried out. In this example, the trader bids up the price of the security and attempts to maintain the closing price above \$11 over a 4-day period. The chronology of traded security over 4 trading days is set out in Box 5.

With reference to the above illustration, the erratic trader entered to buy the security during the closing routines. As a result of his trade executions, the security closed at \$11.00 or higher on each of the mentioned trade days.

The figure 4 shows the impact of the erratic trader’s marking the close activities on the closing price of the security over a period of 15 days. It compares the closing price set by the trader with what they would have been without him marking the close. The prices were maintained or supported at \$11.00 or higher as a result of the trader moving prices upward. It is apparent that the security would have closed at prices significantly lower if not for his marking the close.

## Capital Market Frauds

Box 5.

Client	Side	Timestamp	Last Price	Trade Price	Bid Change	Volume
Day 1						
Other Trader	Sell	15:40	\$11.00	\$10.88	(12)	5000
Other Trader	Sell	15:59	\$10.88	\$10.87	(1)	3400
Rogue Trader	Buy	17:04	\$10.87	\$11	13	100
Day 2						
Other Trader	Sell	11:04	\$11.00	\$10.92	(8)	5500
Other Trader	Buy	14:15	\$10.92	\$10.90	(2)	6500
Other Trader	Sell	15:35	\$10.90	\$10.88	(2)	10000
Rogue Trader	Buy	17:04	\$10.88	\$11		100
Day 3						
Other Trader	Buy	10:10	\$10.96	\$10.95	1	1000
Other Trader	Sell	11:40	\$11.02	\$10.98	(4)	15000
Other Trader	Buy	13:40	\$10.98	\$10.92	(6)	1000
Rogue Trader	Buy	17:04	\$10.92	\$11.03	11	100
Day 4						
Other Trader	Sell	12:10	\$11.03	\$10.96	(7)	8900
Other Trader	Sell	14:25	\$10.96	\$10.87	(9)	5000
Rogue Trader	Buy	17:04	\$10.87	\$11.10	23	100

Source: Singapore Exchange (SGX)

Figure 4.

Source: Singapore Exchange (SGX)



## Marking the Close: Case Study

See Box 6.

Box 6.

<b>Case Detail:</b> ATHENA CAPITAL RESEARCH, LLC Vs Securities Exchange Commission
<b>Respondents:</b> ATHENA CAPITAL RESEARCH, LLC
<p><b>Case Summary</b></p> <p>Athena, an algorithmic, high-frequency trading firm based in New York City, used complex computer programs to carry out a familiar, manipulative scheme: marking the closing price of publicly-traded securities. Through a sophisticated algorithm, Athena manipulated the closing prices of thousands of NASDAQ-listed stocks over a six-month period.</p>
<p><b>Case Detail</b></p> <p>Athena, an algorithmic, high-frequency trading firm based in New York City, used complex computer programs to carry out a familiar, manipulative scheme: marking the closing price of publicly-traded securities. Through a sophisticated algorithm, Athena manipulated the closing prices of thousands of NASDAQ-listed stocks over a six-month period.</p> <p>In the period between June to December 2009, Athena made a large purchases or sale of the stocks in the last two seconds before NASDAQ's 4:00 p.m. close in order to drive the stocks' closing prices slightly higher or lower. The manipulated closing prices allowed Athena to reap more reliable profits from its otherwise risky strategies. Internally, Athena called the algorithms that traded in the last few seconds "Gravy."</p> <p>By using high-powered computers, complex algorithms, and rapid-fire trades, Athena manipulated the closing prices of tens of thousands of stocks during the final seconds of almost every trading day during the Relevant Period.</p> <p>Although Athena was a relatively small firm, it dominated the market for these stocks in the last few seconds. Its trades made up over 70% of the total NASDAQ trading volume of the affected stocks in the seconds before the close of almost every trading day.</p> <p>Athena's manipulative trading focused on trading in order imbalances in securities at the close of the trading day. Imbalances for the close of trading occur when there are insufficient on-close orders to match buy and sell orders, i.e., when there are more on-close orders to buy shares than to sell shares (or vice versa), for any given stock.</p> <p>Every day at the close of trading, NASDAQ runs a closing auction to fill all on close orders at the best price, one that is not too distant from the price of the stock in the continuous book. Leading up to the close, NASDAQ begins releasing information, called Net Order Imbalance Indicator ("Imbalance Message"), concerning the closing auction to help facilitate filling all on-close orders at the best price. At 3:50:00 p.m., NASDAQ issues its first Imbalance Message.</p> <p>Athena's general strategy for trading based on Imbalance Messages worked as follows: Immediately after the first Imbalance Message, Athena would issue an Imbalance Only on Close order to fill the imbalance. These orders are only filled if there is an imbalance in a security at the close. Athena would then purchase or sell securities on the continuous book on the opposite side of its on-close order, until 3:59:59.99, with the goal of holding no positions (being "flat") by the close. It called this process "accumulation," and the algorithms that accumulated these positions were called "accumulators."</p> <p>Athena was acutely aware of the price impact of some its strategies, particularly its last second trading Gravy strategies. Athena used these strategies and its configurations to give its accumulation an extra push, to help generate profits.</p> <p>Example, in April 2009, an Athena manager ("Manager 1"), after analyzing trading in which Gravy accumulated only approximately 25% of its accumulation, and, thus, had no price impact on the stock, emailed another Athena manager ("Manager 2") and Athena's Chief Technology Officer ("CTO") suggesting that they: "make sure we always do our gravy with enough size." (Emphasis added). In fact, Athena traded nearly 60% of its accumulation in the final 2 seconds of the trading day.</p> <p>With the helping hand of its Gravy strategy, Athena refined a method to manipulate the daily process, known as the "Closing Cross," that NASDAQ uses to set the closing price of stocks listed on the exchange. Manipulating the closing process can increase market volatility (thereby frustrating the very purpose of the closing auction) and throw off critical metrics linked to the closing price of stocks. A stock's closing price is the data point most closely scrutinized by investors, securities analysts, and the financial media, and is used to value, and assess management fees on mutual funds, hedge funds, and individual investor portfolios.</p> <p>Athena, however, did not want to push the price of the stocks it traded too much because it created certain trading risks, but also because Athena was concerned about scrutiny from regulators as result of its last second trading. NASDAQ issued an automated Regulatory Alert for "Scrutiny on Expiration and Rebalance Days," which provided that "Suspicious orders or quotes that are potentially intended to manipulate the opening or closing price will be reported immediately to FINRA." Athena's CTO forwarded this alert to Manager 1 and Manager 2 and wrote: "Let's make sure we don't kill the golden goose."</p>

Source: US-SEC. (2014)

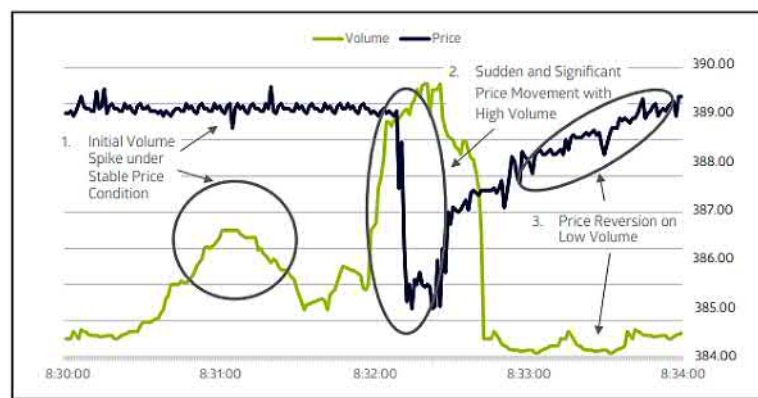
## **Momentum Ignition**

Momentum Ignition typically occurs when a market participant initiates a series of orders or trades with the intent of inducing other market participants to trade in an instrument, so as to accelerate or extend the price trend in the market or a related market. It can be characterized by:

- **An initial spike in the volume under a stable price condition:** Momentum orders are entered by the trader in an attempt to attract other market participants to react or chase the orders.
- **Significant price movement with further spike in volume:** Other market participants enter orders in reaction to the trader's orders, causing a sudden sharp price movement.
- **Price reversion to or near starting price under a lower volume:** The trader trades out his existing position or opens a position at a favorable price and amends or deletes the momentum orders, hence causing the price reversion.

*Figure 5. Market Ignition*

*Source: Addendum to IOSCO Report on Investigating and Prosecuting Market Manipulation, April 2013)*



## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.

- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and fine-tuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

Amjad, M. M., Arshed, N., & Anwar, M. A. (2021). Money Laundering and Institutional Quality: The Case of Developing Countries. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

CFI. (2020). *Front Running*. Corporate Finance Institution. Retrieved from <https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/front-running/>

Comerton-Forde, C., & Putniņš, T. J. (2011). Measuring closing price manipulation. *Journal of Financial Intermediation*, 20(2), 135–158. doi:10.1016/j.jfi.2010.03.003

Dohadwala, B. (2019, April 11). RBI issues directions to prevent market abuse. *Tax Guru*. Retrieved from <https://taxguru.in/rbi/rbi-issues-directions-prevent-market-abuse.html>

DTCC. (2020). *The European Markets Infrastructure Regulation*. Retrieved from <https://www.dtcc.com/about>

Duffie, D., & Stein, J. C. (2015). Reforming LIBOR and other financial market benchmarks. *The Journal of Economic Perspectives*, 29(2), 191–212. doi:10.1257/jep.29.2.191

EC. (2020a). *The European Market Infrastructure Regulation*. European Commission. [https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/post-trade-services/derivatives-emir\\_en](https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/post-trade-services/derivatives-emir_en)

EC. (2020b). *Market Abuse Regulation*. European Commission. [https://ec.europa.eu/info/publications/market-abuse-regulation-mar\\_en](https://ec.europa.eu/info/publications/market-abuse-regulation-mar_en)

ESMA. (2020). *Markets in Financial Instruments Directive*. European Securities and Market Authority Retrieved from <https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir>

Europex. (2020a). *European Market Infrastructure Regulation (EMIR) (EU) No 648/2012*. Association of European Energy Exchanges. Retrieved from <https://www.europex.org/eu-legislation/emir/>

Europex. (2020b). *Market Abuse Regulation (MAR) and Market Abuse Directive (CS MAD)*. Association of European Energy Exchanges. Retrieved from <https://www.europex.org/eu-legislation/mar-and-cs-mad-2/>

FSA. (2011). *David Massey v Financial Services Authority: UKUT 49 (TCC)*. Retrieved from [https://www.fca.org.uk/publication/final-notice/david\\_massey\\_fn.pdf](https://www.fca.org.uk/publication/final-notice/david_massey_fn.pdf)

Garfinkel, J. A., & Nimalendran, M. (2003). Market structure and trader anonymity: An analysis of insider trading. *Journal of Financial and Quantitative Analysis*, 38(3), 591–610. doi:10.2307/4126733

## **Capital Market Frauds**

- Jayasekara, S. F. S. D. (2021). Risk-based AML/CFT Regulations for Effective Supervision. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Kyle, A. S., & Viswanathan, S. (2008). How to define illegal price manipulation. *The American Economic Review*, 98(2), 274–279. doi:10.1257/aer.98.2.274
- MAS. (2020). *Wash Trades*. Singapore: Monetary Authority of Singapore. Retrieved from <https://www.mas.gov.sg/>
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Rafay, A., Sadiq, R., & Mohsan, T. (2016). X-Efficiency in Banking Industry – Evidence from South Asian Economy. *Global Management Journal for Academic & Corporate Studies*, 6(1), 25–36.
- Saeed, S., Mubarik, F., & Zulfiqar, S. (2021). Money Laundering: A Thought-Provoking Crime. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Shah, S. (2021). Compliance Monitoring and Testing Seismometer to Detect Compliquake. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Sinha, A. (2021). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Stafford, P. (2017, September 15). What is MiFID II and how will it affect EU's financial industry? *Financial Times*. Retrieved from <https://www.ft.com/content/ae935520-96ff-11e7-b83c-9588e51488a0>
- Supreme Court of India. (2013, April 26). N. Narayanan versus Adjudicating Officer, Sebi, K.S. Radhakrishnan and Dipak Misra, JJ. Civil Appeal Nos. 4112-4113 of 2013 D.No. 201 of 2013.
- Thomson Reuters. (2020). *Markets in Financial Instruments Directive*. Retrieved from <https://www.thomsonreuters.com/en.html>
- US-SEC. (2014). *Administrative Proceedings File No. 3-16199*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/admin/2014/34-73369.pdf>
- US-SEC. (2018). *Administrative Proceedings File No. 3-18887*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/admin/2018/33-10572.pdf>
- US-SEC. (2020a). *Market Manipulation*. United States Securities and Exchange Commission. Retrieved from <https://www.investor.gov/>
- US-SEC. (2020b). *Administrative Proceeding File No. 3-16316*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/apdocuments/3-16316-event-6.pdf>
- US-SEC. (2020c). *Pump and Dump Schemes*. United States Securities and Exchange Commission. Retrieved from <https://www.investor.gov/protect-your-investments/fraud/types-fraud/pump-and-dump-schemes>
- US-SEC. (2020d). *Litigation Complaints*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/complaints/2020/comp24832.pdf>

US-SEC. (2020e). *Insider Trading*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/>

## **ENDNOTES**

- <sup>1</sup> Major concepts are adapted from the published contents of CFA Institute Investment Foundation.
- <sup>2</sup> Author Compilation.

Section 5

# Taxation and Frauds



## Chapter 19

# Tax Enforcement in the Black Economy: Tackling Disruptive Challenge

**Brendan Walker-Munro**

 <https://orcid.org/0000-0001-5484-1145>

*Swinburne University, Australia*

### ABSTRACT

*The black economy—also called the hidden, covert, underground, grey, illicit, or cash economy—is used to describe the aspect of a country’s economy that is not visibly subject to taxation. However, it is also a useful measure of behavioral disruption to the taxation system, as the scale and tactics of black economy participants vary over time. The purpose of this chapter is to suggest that existing tax policy (where legal constraints alone are used) is insufficient to affect black economy behaviour. It suggests that by adopting responses that are “more than law,” revenue administrations can deploy a more advanced and effective approach to improve tax compliance and can decrease the negative impacts of the black economy.*

### INTRODUCTION

Humankind has been historically inimical to the payment of tax. From the very earliest occasions of human civilization, segments of the population have resisted the payment of taxes, duties and levies even despite obvious legal ramifications (Burg, 2004). In the Bible, Jesus was accused *inter alia* of promoting resistance to the Roman’s poll tax, a crime that was ironically punishable by crucifixion. In 17th century France riots opposing taxes on wine and grain were so violent that tax collectors were lynched, their homes attacked and their families trussed and thrown in the nearest river. And in 2015, austerity measures involving the payment of higher taxes were so violently opposed in Greece that most of the population rallied to the Syriza party’s tax policy of “*Have Not, Pay Not*”, even though Syriza subsequently raised taxes when it came to power (Tsakatika, 2016).

DOI: 10.4018/978-1-7998-5567-5.ch019

## ***Tax Enforcement in the Black Economy***

When parts of a population do not pay the legitimate tax they ought to, a discrepancy arises between tax revenue which theoretically is payable and the tax dollars flowing into the coffers of the government. In OECD countries this discrepancy is referred to as the tax gap and is an important measure that sets the benchmark for tax policy, and more importantly (at least for this chapter) sets a target for tax compliance and enforcement approaches to address. One of the most nefarious contributors to the tax gap is the black economy, the name coming from the covert or hidden nature of the transactions from the revenue authorities that seek to tax it. In other OECD countries it is known by other names, variously called the grey, shadow, hidden, underground, cash, unreported, parallel and/or deviant economy (Bajada, 2017).

This chapter has two main aims. The first is to demonstrate that the black economy is a cause of regulatory disruption for the criminal law regulators that control it. For the purposes of this chapter, regulatory disruption is defined as the disconnection of criminal law regulators from their statutory or political objectives. The predominant cause of this disruption is uncertainty, which acts as a powerful catalyst for disruptive behaviour because it affects how offenders interpret their chances of being caught, the nature of penalization, and the application and legitimacy of the law itself (Walker-Munro, 2020). The second aim of the chapter is that the strategic framework of “more than law” responses might be capable of tackling the black economy, or at least substantial elements of it. Though more research in this area is deeply needed, regulators in the black economy might benefit from adopting such approaches when considering where and how they fit in the enforcement dynamics.

## **BACKGROUND**

Simplistically, tax is revenue paid or collected by a government in exchange for the provision of vital social and community services, such as hospitals, roads, education and defence (ATO, 2020). The most common form of tax is income tax, where a certain percentage of the income of a person is remitted to the Government; however, there are other forms of taxation like duties or excise that may arise from the sale of goods, business transactions, or from the import or export of goods between countries (Rafay & Ajmal, 2014).

In Australia, the Commonwealth Parliament draws legislative power for taxation from section 51(ii) of the *Australian Constitution*, which vests the Commonwealth Parliament with exclusive jurisdiction to make laws relating to taxation matters. Table 1 shows certain other sections of the Constitution which place limits on how the Parliament may enact these laws.

*Table 1. Examples of constitutional limitations of Australia’s taxation power*

Section of the <i>Constitution</i>	Legal and Practical Effect
55	Taxation laws in Australia may only be made with ‘one subject matter’
99	Taxation must be uniform and not favour one State or Territory over another
114	Taxes may not be imposed on property belonging to the Commonwealth, States or Territories

Taxes in Australia are paid on income, certain goods and services, superannuation and pensions, alcohol, luxury vehicles, tobacco, petroleum fuel, and the conduct of certain business and commercial activities (such as capital gains from the sale of assets, shares or securities). The obligations under Australian law also vary depending on whether the taxation is imposed on a natural person, a corporation, or a trust or partnership. Furthermore, under Australia's taxation arrangements each of the States and Territories of Australia also retain some legislative power in relation to so-called "residual" taxes, such as land tax and stamp duty, with each of the States and Territories also receiving payments from the Commonwealth Government from the Goods and Services Tax (GST). Unsurprisingly this has resulted in Australia having one of the most complex tax jurisdictions in the world, and a relatively poor history of completing long-lasting and comprehensive tax reform (Department of the Treasury, 2016). Figure 1 shows how these various taxes have contributed to Australian revenue for the last five years.

Figure 1. Sources of taxation in Australian  
(ABS, 2020)

Total taxation revenue, all levels of government by category						
	2013-14	2014-15	2015-16	2016-17	2017-18	2018-19
	\$m	\$m	\$m	\$m	\$m	\$m
Taxes on income, profits and capital gains						
Income taxes levied on individuals	170 187	183 318	192 054	198 821	212 787	229 749
Income taxes levied on enterprises(a) (b)	76 673	73 568	71 226	80 343	97 705	106 808
Income taxes levied on non-residents	1 566	1 719	1 831	1 976	1 982	2 099
Total taxes on income, profits and capital gains	248 425	258 605	265 111	281 140	312 474	338 656
Taxes on employers' payroll and labour force						
Payroll taxes	20 664	21 297	21 919	22 397	23 573	24 925
Other	844	735	670	605	1 107	1 069
Total taxes on employers' payroll and labour force	21 508	22 032	22 590	23 003	24 680	25 995
Taxes on property						
Land taxes	6 363	6 674	7 237	8 400	9 153	10 712
Municipal rates	15 069	16 009	16 895	17 693	18 407	19 288
Other	2 128	2 333	2 469	2 600	2 689	2 633
Total taxes on property	23 560	25 016	26 602	28 693	30 249	32 632
Taxes on provision of goods and services						
Sales tax	1 302	1 368	1 503	1 524	1 638	1 682
Goods and services tax (GST)	53 409	55 553	59 177	61 505	64 062	65 147
Excises	26 472	24 506	22 540	22 773	23 691	24 574
Taxes on international trade	9 290	10 896	14 057	14 208	15 690	15 944
Taxes on gambling	5 434	5 754	6 053	5 981	6 223	6 876
Taxes on insurance	5 405	5 542	5 718	5 943	6 054	6 348
Taxes on financial and capital transactions	17 360	20 231	22 548	23 353	22 662	20 447
Total taxes on provision of goods and services	118 673	123 850	131 596	135 286	140 020	141 019
Taxes on the use of goods and performance of activities						
Motor vehicle taxes	8 890	9 463	9 902	10 274	10 786	10 986
Other	11 698	4 957	7 834	8 392	10 391	10 546
Total taxes on the use of goods and performance of activities	20 589	14 420	17 736	18 666	21 177	21 532
<b>Total taxation</b>	<b>432 756</b>	<b>443 923</b>	<b>463 635</b>	<b>486 788</b>	<b>528 599</b>	<b>559 833</b>

In Australia, these taxes are administered by the Commissioner of Taxation and the officers and employees of the Australian Taxation Office (ATO). Under Australia's taxation laws, the Commissioner is both the collector of taxation as well as the regulator of the taxation laws, meaning that the Commissioner has responsibility for a broad administrative, civil and criminal jurisdiction relating to the

assessment, collection and enforcement of taxation liabilities. This jurisdiction becomes highly relevant when considering the size, scope and damage caused by the so-called “black economy” in Australia.

## **MAIN FOCUS OF THE CHAPTER**

### **Issues, Controversies, Problems**

#### **The Problem of the Black Economy in Australia**

The ATO defines the black economy problem in Australia as ‘both dishonest and criminal activities that take place outside of or involves misuse or abuse of the tax and regulatory systems’ (ATO, 2019). Such a definition for the black economy subsumes within it other, similarly broad regulatory concepts such as:

- the cash economy – being those portions of the economy where payments are made in cash and taxable amounts not withheld or remitted to the revenue authority (Braithwaite, Reinhart & Job, 2018)
- the grey, shadow or hidden economies – being those portions of the economy relating to specific income generation through tax and other financial crimes (Vousinas, 2017).

The black economy has risen to prominence in Australia over the last decade following investigations by various stakeholders in the regulatory regime including the Australian Taxation Office (ATO), the Board of Taxation and the Treasury. The most recent presentation of these findings was made to Parliament in 2017 by the Black Economy Taskforce (the Taskforce). In their Final Report, the Taskforce provided estimates that indicated the black economy in Australia ‘could be as large as 3 per cent of GDP (roughly \$50 billion)’ and ‘could have increased in size by up to 50 per cent since 2012’, findings which surprised even the Taskforce (Commonwealth, 2017). The Taskforce’s Final Report is important for more than just its identification of the scope and magnitude of the problem – it also frames the contextual challenges the regulators have experienced in bringing the challenge of the black economy to heel.

There are numerous contributors to the black economy. The Taskforce identified eighteen examples of ways in which individual and institutional behaviours could contribute to the size, scope and scale of the black economy, including a variety of various forms of fraudulent over- or under-declaration of tax positions (across numerous revenue streams such as income tax, Goods and Services Tax, pay-as-you-go withholding and superannuation guarantee), illicit business practices (such as sham contracting, manipulating workers visa conditions, “phoenixing” and money laundering (Rafay, 2021), counterfeiting, and evasion of duties and excise (Commonwealth, 2017). Whilst many of these contributors are subject to regulation by one or more government agencies (for example the Department of Home Affairs, the Australian Taxation Office, and the Fair Work Ombudsman), the participants in the black economy themselves clearly underestimate their contribution to it. One comment of the Taskforce is pertinent to this argument: ‘Combating the black economy is not just a matter for governments. We all need to be part of the solution. We need a new social contract: a renewed commitment from the business community and wider public to fight the black economy’ (Commonwealth, 2017). The black economy and the illegal activities that drive it are not just a policing or criminological problem, it is a social problem.

## **Scale and Scope of the Problem**

But how big is this problem to Australia? The estimation of the size, scope and scale of the black economy pose thorny political and social challenges. Warren (2019) describes many of these challenges in his exposition of the tax gap. As was explained earlier in this chapter, the tax gap is a critical part of the setting policy, compliance and enforcement approaches as it frames the discrepancy in collection of taxable amounts from the amounts that might be collectable, but for the failures of either compliance or policy. Citing Donald Rumsfeld, the former US Secretary of Defense, Warren (2019) makes clear that the tax gap in Australia is bounded by the concepts of:

1. 'known unknowns' (what the revenue authority is aware it does not know), and
2. 'unknown knowns' (what the revenue authority is unaware of but could find out if it wanted).

Whilst an in-depth analysis of Warren's (2019) work is beyond the scope of this chapter, his observation of the two forms of unknowns in the black economy serves as a useful introduction to this concept that sits at the heart of regulatory disruption. The biggest stumbling block to the black economy problem is one of uncertainty – uncertainty of size and scope of players in the black economy, uncertainty of regulatory target, and uncertainty of effectiveness of the regulatory controls imposed by regulators required to control it.

The Black Economy Taskforce referred to this uncertainty at several stages of its report. It noted the uncertainty inherent in:

- Identity crimes perpetuated in corporate structures, an uncertainty reinforced by a form of regulatory myopia where ASIC records and ATO records are inconsistent with the controlling mind of the corporation, or where ABN holders failed to lodge tax returns or activity statements (which may or may not have been linked to the holders' earning of assessable income; Commonwealth, 2017).
- Legal and taxation treatment of the status of the gig economy, and the application of mandatory disclosure of income earned by its participants (Commonwealth, 2017); and
- Information shared between regulators (Commonwealth, 2017).

## **How Uncertainty Matters to Black Economy Behaviour: The Rational Choice Model**

In work elsewhere I have already linked the concept of uncertainty with regulatory disruption, wherein I made clear that uncertainty posed by the size and scope of new technological advancements, the uncertainty of application of laws to those advancements, and the uncertainty of the regulator's likely and possible responses all resulted in the displacement and dislocation of regulators from their key policy and statutory objectives (Walker-Munro, 2019). These uncertainties all have influences on the behaviour and conduct that sits at the heart of the black economy challenge because of the underlying influence of the rational choice theory of crime.

This theory stipulates that decisions to engage in a crime or criminal behaviour is driven by a rational calculation of risk versus reward (Pogarsky, Roche & Pickett, 2018). The rational choice model of crime thus recognises three categories of behaviour by which organisations or individuals are incentivised or disincentivised to comply with legal requirements. The first is by reference to economic motivations,

where a person makes a reasoned determination of the likelihood of detection coupled with cost of sanction (generally monetary such as fines or penalties) against the benefits of successful offending (Draca & Machin, 2015). The second is social motivations, where a person wishes to earn the respect and approval of a class or classes of persons in respect of their interactions with them (Dwenger, Kleven, Rasul & Rincke, 2016). Lastly there are normative motivations, where a person feels compelled by a moral duty to comply with a particular regulation, or alternately to disobey a regulation the individual considers is illegitimate or lacking moral authenticity (Parker & Nielsen, 2017).

From the standpoint of regulatory scholarship, tax continues to be a unique environment to explore the rational choice model because revenue administration is a regulatory system that features interactions between both formal rules and informal principles as well as high stakes / high complexity concepts which can sufficiently motivate regulated entities to test, bend or even break the law (Braithwaite, 2005). Professor Valerie Braithwaite has pioneered much of the research in this domain. Building on earlier work from the 1990s she established the concept of motivational postures as behavioural demonstrations of *“the way in which taxpayers controlled the amount of social distance they placed between themselves and the tax office”* (Braithwaite, 2002). She considered that four such postures were evident from research into taxpayers’ behaviour – commitment, capitulation, resistance and disengagement – and that regulators should consider harsher and more serious methods of punishment for non-compliance (Braithwaite, Murphy & Reinhart, 2007). So important is this research that subsequent practitioners examining Professor Braithwaite’s compliance postures have helped guide certain aspects of Australia’s tax compliance policy, such as the work of Wurth (2012) and Wurth & Braithwaite (2016) in the formulation of the teardrop model of tax practitioner compliance (Millane & Stewart, 2019).

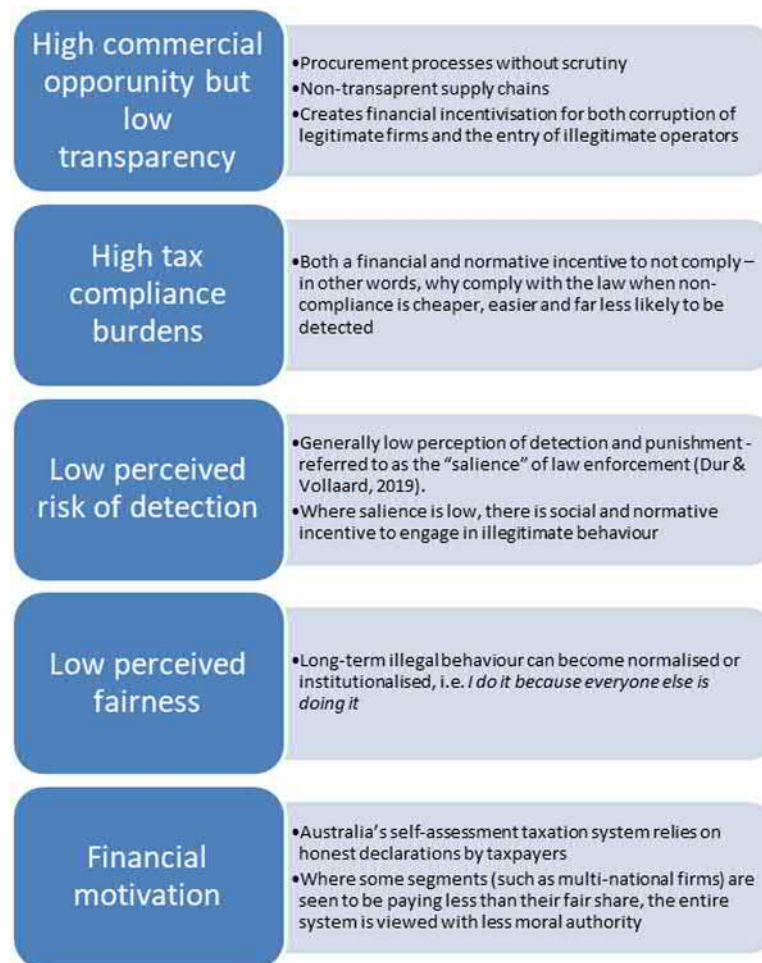
### **Motivational Postures**

Motivational postures become an important consideration of how regulators respond to regulatee conduct, if we accept the previous contention that crimes are based on rational, actuarial decisions of calculated risk. Thus, rational choice becomes a highly relevant window through which to view the various criminal behaviours linked to the black economy. Of the eighteen contributing behaviours identified by the Taskforce, five common themes were identified, and all five have a distinct resonance with rational choice theory (shown in Figure 2).

### **Summary of the Taskforce’s Findings**

Overall, these findings suggest that the Taskforce’s observation that ‘An individual’s decision to engage in the black economy is strongly influenced by their perceived reputation, social norms and their behavioural responses to policy and regulatory settings’ (Commonwealth, 2017) is an accurate one, because it embeds rational choice theory at the heart of the black economy problem and is supported by the findings of the research literature (Dobos & Takacs-Gyorgy, 2018). But we can go further, because the rational choice model does more than just link the observed behaviours in a black economy context with an established criminological model. It offers regulatory scholars, policy administrators and regulatory agencies an opportunity to consider the black economy as a disruptive challenge. This is important because the regulatory responses to technological disruption might then be considered as responses to the black economy.

Figure 2. The common themes of the Black Economy Taskforce



## The Black Economy Is a Disruptive Challenge to Criminal Law Regulators

In their submission to the Taskforce, the Chartered Accountants Australia & New Zealand (CAANZ) summarised the challenge of the black economy succinctly: ‘Just as traditional business models have been disrupted so too have traditional governance models’ (CAANZ, 2017). Yet there exists opportunity as well; the continued and pervasive existence of the similar hallmarks of uncertainty suggests that we might benefit from considering treatments of the black economy in a similar – if not identical – fashion to other disruptive trends with a more technological focus. As a starting point we can examine the work done by other scholars on the effect of technology on regulators (Bennett Moses, 2013; Yeung, 2016; Brownsword, 2019; Rafay, 2019). Brownsword (2018) in particular describes disconnection as occurring when technologies that either create a regulatory void or ambiguity in which the old laws do not apply or facilitate the adoption of norms that modify societal approaches to compliance. Bennett Moses (2013) also defines an important dichotomy between legal and regulatory disconnection: “*Copying digital music is still a breach of copyright—the language of the statute still applies and there is thus no legal*

## Tax Enforcement in the Black Economy

*disconnection—but ease of copying has affected social norms so that rates of copying have increased despite copyright laws, and thus there is regulatory disconnection”*. By applying these concepts to the black economy, we identify that the black economy exhibits all the same hallmarks for regulators as disruption by a more technologically based means:

In short, the black economy is a source of regulatory disruption, as surely as a newly developed technology. Regulators of the criminal laws which might control or limit black economy activities are paralysed by indecisiveness about the best way to proceed, and those proponents of the black economy thrive in such grey and under-enforced markets. Also, the inability to properly enforce the criminal jurisdiction which sits over and above the black economy substantially affects the rational choice of its proponents to engage in unlawful behaviour. So, what can the revenue authorities do in such circumstances?

Table 2.

It modifies the economic incentives for engagement in criminal activity	Decreasing the likelihood of detection and increasing the potential payoffs, all whilst inhibiting the visibility or salience of enforcement activities. In such an environment, the criminal law and its various proponents fails to achieve its objectives of responding to wrongdoing and more importantly, discouraging criminal behaviour (Marks, Bowling & Keenan, 2017)
It nurtures and encourages criminal entrepreneurship	New and varied methods are consistently developed for circumventing or bypassing regulatory controls are developed or exploit existing loopholes and grey areas in laws or legal treatments.
Police are ill-suited to dealing with the black economy	Despite the obvious criminality inherent in certain behaviours observed in the black economy the Police are often ill-equipped (both financially and culturally) to deal with black economy behaviour as a multi-agency, multi-jurisdictional problem. Those regulators better equipped to handle the black economy often struggle with limitations on information sharing, as well as jurisdictional disputes over which agency ought to lead the enforcement response. In a different way, the disruptive effects of technology on terrorism offences led to what some refer to as “hybrid” forms of regulation arising between the military, police and security services, where the regulatory roles and remits of each overlap and become blurred (Bronitt & Donkin, 2012).

## Treating the Risks of the Black Economy

Perhaps the most important finding of the Taskforce was that ‘[m]ore regulation is not the answer... Our responses must be more intelligent and targeted than this, including employing the smart technologies we are seeing in the private sector...the value of visible enforcement has been a consistent message’ (Commonwealth, 2017). The concept of “visible enforcement” that is discussed in the final report is a key one for this chapter because it poses two very substantial questions at the heart of the enforcement challenges posed by the black economy. The first question is how a regulator can enhance the visibility of its enforcement measures that might discourage similar schemes from being enacted in the future, which can be a tall order in a regime so heavily characterised by secrecy and protected by custodial punishments. The second question is how a regulator can ensure the effectiveness of its regulatory controls against targets whose size, connections and net worth may not be fully quantifiable or even estimable. Yet if we recall the rational choice model, we remember that the nature of offending decisions is finite and calculable by reference to economic, social and normative motivations.

Thus, the proper response of regulators to rational crimes (including those represented and fuelling the black economy) is one of “changing the equation”, by incentivising proper behaviour and disincentivising offending, and thus affecting the risk versus reward calculations, increasing social compliance and



institutionalising normative compliance. I have already considered that some of the ways they might do so are by the erection of economic barriers to entry to a criminal market (Walker-Munro, 2019a) and by ensuring prompt, real-time and in-depth surveillance of the regulated environment to identify, quantify and observe the behaviours of the regulated, rather than focusing on legal strictures and punishment before the Courts as sole deterrent (Walker-Munro, 2019b).

## **CURRENT APPROACHES TO TAX ENFORCEMENT**

In one of his seminal works Professor John Braithwaite describes the impact of alternative methods of enforcement in tax administration and enforcement. He notes that the majority of Australian taxpayers who use the service of tax agents demand an ‘honest, low fuss preparer’ – thus demand for virtue ought to drive a competition dynamic that rewards honesty and integrity in the tax planning industry. For those taxpayers who self-prepare, Braithwaite suggests that revenue authorities benefit when their compliance models utilise four core elements (Braithwaite & Hong, 2015):

- An understanding of taxpayer behaviour and risks so that ‘prevention can loom larger than cure’.
- Building of partnerships to address risks.
- Creativity in the building and utilisation of multiple toolsets.
- ‘Responsive escalation up enforcement pyramids’ with a focus on problem solving.

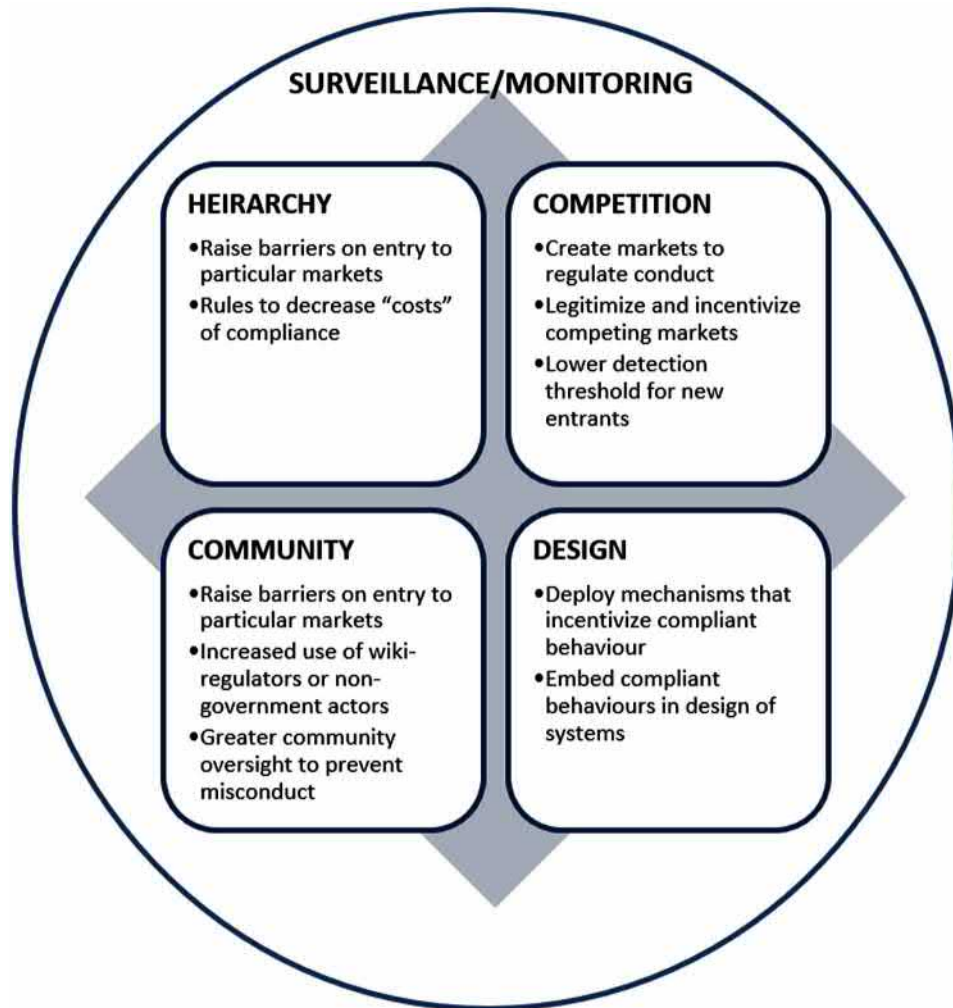
Wurth and Braithwaite echo these sentiments. To them, tax compliance may be an individual choice, but it is a choice influenced by a set of networks involving workplaces, professional relationships, other taxpayers and friends and family (Wurth & Braithwaite, 2016). One comment of the Taskforce is pertinent to this argument: ‘Combatting the black economy is not just a matter for governments. We all need to be part of the solution. We need a new social contract: a renewed commitment from the business community and wider public to fight the black economy’ (Commonwealth, 2017). The holistic focus of compliance and enforcement policy and responses by a revenue authority must therefore be aimed at eliminating uncertainty and promoting a credible narrative.

In applying the concepts of regulatory responses to disruptive technologies, Figure 3 demonstrates how the disruption calculus from earlier work I have completed in this area might provide a useful conceptual framework for such approaches by revenue authorities looking to treat the black economy. We will deal with each of the areas in Figure 3 in further detail.

## **Surveillance/Monitoring**

Given the levels of uncertainty we have identified as being inherent in the black economy, perhaps one of the most underestimated regulatory activities relevant to the black economy is the immediate need for surveillance and monitoring mechanisms to identify, quantify and assess participants in the black economy. Such mechanisms are important to give revenue authorities more certainty about both the size and scale of the problem as well as the quantifiable risks to better target individual compliance responses, but their utility extends far beyond merely satisfying Rumsfeld’s knowns and unknowns. Under both Bayesian economics and game theoretical models, black economy behaviours have been shown to be driven by the possession of both incomplete and imperfect information by the regulatory authority, lim-

*Figure 3. The disruption calculus*  
(Walker-Munro, 2019)



iting their freedom of action and permitting unlawful actors a greater scope in which to operate (Fedeli & Forte, 2012; Chiarini & Marzano, 2016). Such information asymmetry has also been borne out as a substantial driver in academic and Parliamentary reports on the black economy in both highly developed economies (UK, USA and Australia) as well as developing nations such as India, Pakistan and Nigeria.

However, such proposals are not without their own unique problems. It is a long-established fact that the mere act of governmental surveillance can have a chilling effect on behaviour and conduct (especially where that conduct is contentious or sanctionable), with the Law Reform Commissions of both Australia and New Zealand considering a range of harms that result from inappropriately broad State-sponsored surveillance activities (NZLC, 2010; Australian Law Reform Commission, 2014). In the United States the chilling effect has been recognised by Supreme Court decisions as affecting not only the rights of the populace under the Fourth Amendment to the *US Constitution* (protecting citizens’ right against arbitrary search and seizure) but also under the rights of association and free speech protected by the

First Amendment (*NAACP v Alabama*, 1958; *Bates v City of Little Rock*, 1960; *Dombrowski v Pfister*, (1965); *Zweibon v Mitchell*, (1975)). The former Supreme Court Chief Justice, Earl Warren, said of such cases that '[i]t would indeed be ironic if, in the name of national defense, we would sanction the subversion of...those liberties...which makes the defense of the Nation worthwhile' (*USA v Robel*, 1967). Such cases have only increased as policymakers have sought to increase surveillance mechanisms and powers, both as a result of the post-9/11 threat of ubiquitous terrorism but also our increasingly digitised modern society (Richards, 2012; Hughes, 2012; Lightfoot & Wisniewski, 2014; De Zwart, Humphries & Van Dissel, 2015; Memdani, Kademi & Rafay, 2021; Sambo & Sule, 2021).

In stark contrast to these suggestions the Taskforce published a consultation paper in which it identified that access to substantial amounts of banking, telecommunications and other third-party data was absolutely crucial to understanding the full picture of black economy conduct, as well as to appropriately identify various players in the black economy space (including for example, straw directors; Department of the Treasury, 2018). Internationally there abounds both Parliamentary and scholarly literature which identifies numerous mechanisms whereby proposed increased access by revenue authorities to banking records, employment databases and insurance registers, company registration information, and other electronic or financial sources are considered substantial tools in the fight against the black economy (Murphy, 2014; CRA, 2017; Ernst & Young, 2017; Dobos & Takacs-Gyorgy, 2019).

In conclusion, the surveillance and monitoring of black economy type behaviours is highly relevant and extremely important for embedding any form of policy and compliance response. As envisioned in Figure 3, this effectively sets the background for the deployment of other forms of social control (Hierarchy, Competition, Community and Design) that can better perfect and incentivise rational choices to comply with the tax laws.

## **Hierarchy**

The concept of hierarchy includes not only existing statutes and the enforcement tools that flow from them (such as the imposition of penalty notices or fines, the concepts of charges and imprisonment) but also softer tools designated under the broad concept often referred to as 'command and control' regulation such as agency threats, policy guidance and adjudications (Wu, 2010; Brit, 2014; Schwarcz & Zaring, 2017). In the taxation space the concept of hierarchy is thus not only comprised of the tax laws and codes, but also specific tax rulings and interpretation policies. Unfortunately, hierarchy is perhaps the most ill-fated tool to choose to combat the black economy.

## **Competition**

The compliance dimension of competition can be leveraged against black economy participants by affecting how consumers of a free-market economy choose to engage with the incumbents in the market, by making the incumbents more or less visible, more or less expensive and more or less accessible (Walker-Munro, 2019a). As a result, incumbents' behaviour can move to being self-regulating. Consumers who dislike a particular service or company – for example, because of their environmental record – “vote with their feet” by patronizing other suppliers (Henriksen & Ponte, 2018). Where a large number of incumbents compete for market share, there is a financial incentive in obtaining new customers – therefore any regulatory decision that links potential customers to compliant conduct or an increase in salience is more likely to increase compliance (Baumann & Friehe, 2016).

## **Community**

The third modality of compliance we suggest ‘sets normative requirements by reference to both internal and external influences of a given community grouping’ (Walker-Munro, 2019a) and can both incentivise and disincentivise compliant taxpayer behaviour by affecting their perceptions of broader behaviours being engaged in by other classes of taxpayers, or by society as a whole (Farrar, Massey, Osecki & Thorne, 2018). These perceptions can be:

1. objectively based (i.e., the taxpayer is certain, based on credible evidence, that another class of taxpayers are gaining an unfair or unlawful advantage); or
2. subjectively based (i.e., the taxpayer *thinks* another class of taxpayers are gaining an unfair or unlawful advantage, even where this perception is skewed or untrue).

## **Design**

The last of the four modalities, design, differs from the preceding three in that design-based controls preclude or foreclose the possibilities of non-compliance by virtue of some inherent feature in the structure or process. A design-based control to prevent speeding for example would be a technological or mechanical limiter placed on the vehicle engine, physically preventing it from exceeding a speed limit.

Within the tax administration space, revenue authorities are employing design controls by removing the need for individual and some classes of small business taxpayers to lodge annual tax returns (Wilson, 2017). In the UK, HMRC leads this approach, anticipating that the need to submit annual returns for individual taxpayers should be removed by the end of 2020. New Zealand’s Internal Revenue Department (IRD) has also eliminated the need for “simple” tax returns for individual taxpayers who earn wages or salaries (Veit, 2019). Unfortunately, in this regard Australia lags well behind the rest of the world. In part, this is because the Australia income tax provisions permit a wide variety of work-related expense deductions to be claimed by nearly all individual taxpayers, resulting in quantifying, assessing, defining and claiming such deductions. The Inspector-General of Taxation (IGT) has joined many others in calling for the work-related expense regime to be overhauled or removed, as it stands as a substantial impediment to future tax reform (IGT, 2018).

## **SOLUTIONS AND RECOMMENDATIONS**

Taking the above framework outlined in Figure 3, we can now propose some opportunities of practical significance for taxation authorities to consider. For example, in Australia, surveillance by algorithm, trusted tax status and overseas income-matching are substantial tools taken from these methodologies which have been successful in leveraging increased tax compliance (Veit, 2019).

### **SURVEILLANCE**

One such mechanism which the author considers warrants further exploration is Hatfield’s (2015) suggestion of a ‘tax surveillance system’. He suggests that the revenue administrations of future years will

invest in systems in which the existing data streams entering their databases are quickly and continuously monitored by artificial intelligence (AI) routines looking for mismatches and anomalies between declared tax positions and both actual and potential positions. Hatfield's (2015) mechanism has a great degree of promise for the black economy, but there are a number of compliance concerns that remain unaddressed, such as concerns with privacy, fairness, bias and due process. Though an examination of these concerns in taxation surveillance is beyond the scope of this chapter, it is enough to observe that there exist real tensions around the application of such principles to the concept of continuous AI assessments of regulatory databanks (including their use by tax or revenue authorities).

For example, the use of algorithms to assess data holdings in a continuous fashion may be considered by privacy advocates to constitute ongoing surveillance and thus offending both international law on arbitrary interferences with privacy and the generally adopted principles of data privacy around limiting uses to those which are reasonable, adequate, relevant and necessary (Regulation (EU) 2016/679). Yet there are numerous counters to this argument. The first is that the ongoing analysis of digitised records by an algorithm is not an interference with privacy because the searches are not being conducted by a human being (Casey & Niblett, 2016). The second is that the searches by algorithms of massed data for anomalies and links is not factually different to those conducted by a person, only faster (O'Reilly, 2013). The third is that decisions made by a computer are still subject to various forms of administrative and judicial review (Crawford & Schultz, 2014); indeed, in some jurisdictions, decisions made by a computer program are not considered decisions at all (see for example *Human Rights Watch and others v Secretary of State for the Foreign and Commonwealth Office and others*, 2016; *Pintarich v Deputy Commissioner of Taxation*, 2018). The fourth and final counter is that there are often substantially compelling public policy reasons for regulators of certain fields (including taxation, but also counterterrorism, organised crime and money laundering) to have ongoing and real-time analytical capabilities of the kind envisioned by Hatfield (Margulies, 2014; Margulies, 2016).

## **HIERARCHY**

One approach is to consider the actions taken by other revenue authorities that treat the source of black economy activities, not their effects or symptoms. This involves analysis of, and understanding, the specific behavioural drivers that shift taxpayer behaviour towards the illegal, and act to disincentivise the behaviour. By way of example, the National Taxation and Customs Authority (NAV) in Hungary is given legislative powers to close 'the premises of a taxable activity' if it employs an unregistered employee. The sanction available also increases from 12 to 60 days of closure if the offence is repeated. Obviously, there is a noticeably clear financial disincentive attached to this kind of enforced closure; however, much more of the regulatory control comes from the 'loss of prestige' as the NAV then publishes the name and tax number of employment relationship offenders on its website (Dobos & Takacs-Gyorgy, 2019).

Another possibility is to posture the hierarchy of the tax system to promote principles over formal rules. One of the most strident criticisms of the tax laws in the digital economy is that they lack the speed of adjustment, flexibility and scope of application to successfully and meaningfully be applied to new business models, even if the revenue authority applying them demonstrates adaptability (Grinberg, 2018; Bentley, 2019). This lack of speed and reactivity can be particularly exacerbated by the challenges of the black economy – technological innovation is very often one or more steps ahead of tax policy, compliance and enforcement frameworks. By embedding of what Wurth and Braithwaite describe as

a hybrid system of tax regulation, rigid rules are designed to be subservient to the principle which the rule seeks to enforce. Principles have the benefit of promoting flexibility and certainty, as well as being reactive to new innovations in schemes and structures (Gribnau, 2015). It is for this reason that many of the OECD jurisdictions have adopted principle-based approaches to assessing tax avoidance (Prebble & Prebble, 2010; Taboada, 2015). Though there are some criticisms of these rules as unfairly penalising those who comply with the letter but not the spirit of the law, these cases are broadly considered to be in the minority in a system where ‘[i]n a contest between a rule and an overarching principle, it is the principle that is binding on taxpayers’ (Wurth & Braithwaite, 2019).

The final proposal is to consider a greater use of surveillance and monitoring to inform the principal compliance tool in the armoury of the revenue administration: the tax audit. Whilst some early research in the tax space suggested that the audit “*can backfire by teaching tax cheats how much they can get away with*” (Braithwaite, 2018), there are more recent studies suggesting that “*uncertainty of the probability and regularity of audit activity is key in encouraging voluntary compliance*” (Dai, Galeotti & Villeval, 2017). Tax audits can also promote trust in the integrity of the tax system and more widely act as a deterrent (OECD, 2017), as well as encouraging taxpayers to remain in more secure, unchallenged tax positions. The ATO (like many OECD revenue authorities) have no obligation under statute or common law to inform taxpayers how they were selected for audit, and indeed can conduct audits at random or on the basis of “fishing” for non-compliance (Bazart, Beaud & Dubois, 2020); however, they do appear to rely on a wide variety of macro- and micro-economic data to conduct case selections (Memon & Lorenz, 2016). Therefore, the use of Hatfield’s (2015) tax surveillance model to inform audit case selection appears far less likely to draw adverse criticism for privacy and due process concerns when the reasoning for such selections is not provided.

## **COMPETITION**

When examining the competition methodology, certification is a useful method. Although this process might seem more suited to coffee producers and organic vegetable farms, there is a place for these kinds of non-law systems in other regulatory systems by providing a publicly viewable “badge” that enhances the repute of its bearer (Swierczynska, 2016). The Internal Revenue Service (IRS) of the United States and Her Majesty’s Revenue and Customs (HMRC) in the UK already employ such a system to combat aggressive tax planning. Under these systems, promoters must register any “potentially abusive shelters” for taxation and taxpayers must declare a registration number of that shelter when claiming or deducting tax based on investments to that shelter. Such a system enables cross-checking of disclosures and the taking of enforcement action becomes much easier (Alstadsæter, Kopczuk & Telle, 2019). So effective is reputational influence and brand certification that the Taskforce suggested tax compliance certification as a method of enhancing the integrity of procurement, building and construction, and noting that the UK, South Africa and Ireland all have similar certification processes.

Certification can also be applied to the advisors and agents within the tax system who assist taxpayers with their lodgements. By “certifying” certain trusted taxation advisors, the regulator can enhance the commercial capital and client base of that advisor in exchange for the promotion of lawful and compliant tax advice by that advisor amongst their client bases. Afield (2014) provides a fulsome description of how such a market would work in the US by encouraging the IRS to structure an incentives-based certification and compliance program around tax advisors, including by lowering the rate and scale of

any imposed penalties when errors are detected, decreased scales of compliance costs in producing information or records whilst under audit and decreasing the audit rates of certified individuals. Promoting advisors also has a highly legitimising effect on external perceptions of the revenue authority (Farrar, Kaplan & Thorne, 2019). Murphy (2019) suggests coupling this with audits by the regulator to target tax preparers whose clients – as a holistic population – have the worst compliance record. Similar to other mechanisms proposed in this chapter, a certification approach was also endorsed by the Taskforce as a valid mechanism for dealing with advisors who facilitate the black economy (Commonwealth, 2017). The concept of ‘trusted taxpayers’ was also explored by the Taskforce from a small business perspective as a way to incentivise non-cash operating models, by promoting compliance through competitive means such as by reducing or eliminating the need to file tax returns for appropriately e-linked businesses.

Competition is a valid compliance tool for revenue authorities to mobilise compliance in response to the black economy. The financial incentives for increased or more developed clientele are powerful ones for many small businesses who may be competing in tight markets or with small margins (especially given these markets are often the prime targets of black economy participants). In addition, they can be highly flexible to technological change and innovation and can also be a strongly legitimising force for revenue authorities seeking to build capacity within tax advisor populations to influence downstream behaviour.

## **COMMUNITY**

There are a number of different mechanisms whereby revenue authorities can engage the community modality in treatment of the black economy. One method is by virtue signalling in the sense described by Etienne (2013), where regulators ‘making certain behaviours meaningful and others less so’. This can be as simple as tailoring correspondence of the revenue authority to better reward compliant behaviours and more explicitly call out unlawful ones (Faulkner *et al.* 2018). Though the publicity (and therefore signalling effect) of such correspondence is limited, there is a pressure on the taxpayer’s self-interest to engage in compliant behaviour and a concomitant increase in perceptions of the revenue authority’s legitimacy and fairness (Demin, 2018).

Virtue signalling can also be leveraged through the use “naming and shaming” programs. Shaming has a very long history in the administration of tax revenue. In Rome, the roughhewn stones outside the Ducal Palace in Piazza San Marco still carry the names of those Venetian citizens alleged to be hiding taxable income from Republican authorities (Tanzi, 2017). Indeed, the disclosure of corporate (as opposed to individual) tax information in Australia is not new but has been demonstrated benefits in the disclosure of corporate tax return information that improves transparency and legitimises the tax authority. It also encourages a degree of self-regulation such as the adoption of voluntary tax transparency codes and self-recognition by companies of the importance of reputational influence on corporate behaviour (Hoopes, Robinson & Slemrod, 2018).

But community compliance levers can be pulled further. Two enforcement strategies with distinctly community-based incentives were reported in Pakistan (Slemrod, Ur Rehman & Waseem, 2019). In that study the authors analysed the compliance effects of a public register for tax reporting – in which the amount of tax paid by every taxpayer in the country was made available online and free of charge in a searchable PDF – and a Taxpayers Privilege and Honours Card (TPHC). They identified that both mechanisms together:

## **Tax Enforcement in the Black Economy**

*...can encourage whistleblowers to come forward, increasing the expected costs of evasion through the conventional channel of the deterrence framework. The shame and guilt resulting from the disclosure can also induce greater tax compliance. On the other hand, the programs may stimulate feelings of pride and positive self-image if one is revealed to be a compliant or top taxpayer.*

Afield (2014) also embeds shaming as a key enforcement tool in his proposed market for tax compliance. Certified preparers can be publicly named, resulting in both a competition and community benefit (deriving from their increase in status and the desire for taxpayers to be associated with a certified preparer) that, through shaming, prompts those preparers who are not certified to join the program. However Afield (2014) is quick to caution that ‘the shaming effect could backfire if preparers see that the vast majority of their peers are not seeking certification and are thus not necessarily furthering compliance norms’.

Lastly, community modalities can be implemented to incentivise and legitimise relationships with the revenue authority to the exclusion of the participants in the black economy. These incentives may be for unlawful participants to admit wrongdoing before they are “dobbed in” by a member of their community or close network, in which case the revenue authority will consider various forms of immunity or lesser sanctions than might otherwise be the case (Braithwaite, 2013). Community partnerships can also be linked with financial incentives, though revenue authorities need to be careful that the access to such financial incentives is not perceived as a right in cases where scant, unnecessary or inaccurate (or even wildly untrue) disclosure is made to achieve a financial benefit. Incentives can also be levied as a function or percentage of the amount of taxes recovered from evasive or illegal behaviour, similar to the “bounty hunting” provisions in the US Dodd-Frank Act (Sampson, 2019). Finally, some countries such as Romania, Korea, Hungary and Poland have all reduced black economy behaviours by incentivising relationships with the tax authorities through the use of taxpayer lotteries – though the mechanics differ, these lotteries all award a monetary prize to random taxpayers selected from a pool of those who have been deemed to be compliant with their various obligations, such as record keeping or accuracy of tax disclosure in returns (Ungureanu & Dascalu, 2015; Sung, Awasthi & Lee, 2017; Pauch, 2018).

## **DESIGN**

A specific design control that could apply to the black economy is demonetisation. Given that much of the black economy behaviours observed by the Taskforce involved physical cash changing hands, the removal of reliance on cash payments was dedicated to an entire chapter in the Taskforce final report and included the introduction of a New Payments Platform (NPP), a limit of \$10,000 on cash payments, a legal requirement for wages to be paid into bank accounts and reducing the fees for bank card transactions (Commonwealth, 2017).

However, demonetisation suffers a serious number of drawbacks. Firstly, empirical evidence from India’s experiences with demonetisation demonstrates that a push for digital currencies is pointless if the supporting education, infrastructure and support for the digital infrastructure is poor or improperly resourced (Singh & Panwar, 2017; Beyes & Bhattacharya, 2017). Secondly, even though global cash use has declined in favour of digital alternatives there remains a desire to retain cash use even in well-developed industrial economies such as the United Kingdom, United States, the Netherlands and Japan (Khiaonarong & Humphrey, 2019). Secondly, digital or cryptocurrencies *can* be more secure and traceable, but does not always mean they are. Many of the current alternatives in the market (such Bitcoin, Litecoin



and Ripple) offer anonymization of participants and/or peer-to-peer encryption as standard (Tasca, 2015; Iqbal *et al.*, 2019)). Though ostensibly offered for privacy and security of financial details, such features are also highly prized by criminal offenders seeking to either shield their sales and purchases from law enforcement, or to launder money derived from illicit activities (Caytas, 2017).

A third mechanism of potential use in the tax administration and black economy space is an adoption of the *lex cryptographia* (Wright & De Filippi, 2015). By charting the rise of both mercantile and informatics law over the last several centuries, Wright and De Filippi (2015) suggest that emphasising design/architecture solutions could inevitably displace judicial enforcement of the law dependent on contractual provisions built into smart contracts, web interfaces and the use of cryptographically activated assets. Under the *lex cryptographia* regulators are able to access smart contracts executed between various parties and exert their influence by arbitrating conditions in an online ecosystem.

Because the regulatory decisions made under smart contracts are effectively “built in” to the rights that flow from the contracts, they are instantly and irrevocably binding on service providers and intermediaries. Non-compliance with a contract becomes impossible because the benefits (such as a payment of money only releases once the precedent conditions are met). The NPP considered by the Taskforce (Commonwealth, 2017) is a powerful example of the *lex cryptographia* at work, where:

1. a building tradesman issues an electronic quote to a householder,
2. the householder makes a digital payment and receives an e-receipt, and
3. the tradesmen receive an income notification from their bank.

As a regulator, the Australian Taxation Office has visibility of the entire transaction and can calculate the taxes payable in real-time and at point-of-service. Unfortunately, the *lex cryptographia* at present remains conceptually nascent – there are several existing types of conduct which contractual parties engage in (such as consensual non-enforcement for technical breach, or vague/unenforceable terms) which the *lex* does not currently allow for or address (Levy, 2017).

## CONCLUSION

The purpose of this chapter was to examine the black economy as a disruptor, in a manner similar to the emergence of novel technologies. In considering the black economy we can identify that much of the financial, social and normative motivations for engaging in illicit or underground tax behaviour are driven by uncertainty – both uncertainty of the regulator’s approach and reach, but also uncertainty around the conceptual and legal treatment of certain tax arrangements. Where a revenue authority seeks to treat this uncertainty, a usual policy response is the implementation of new rules and laws (a hierarchical response). However, as we have demonstrated in this chapter, there is a substantial degree of benefit in considering the drivers of compliance in competition-, community- and design-based controls. The black economy in particular, being a compliance problem with a distinctly social background, is highly susceptible to these forms of controls and the prospects of future research in this area appears highly exciting.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the author in his personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## **REFERENCES**

- ABS. (2020). *5506.0 - Taxation Revenue 2018-19*. Australian Bureau of Statistics. Australian Government Printer.
- Afield, W. E. (2014). A Market for Tax Compliance. *Cleveland State University Law Review*, 62(2), 315–341.
- Alstadsæter, A., Kopczuk, W., & Telle, K. (2019). Social networks and tax avoidance: Evidence from a well-defined Norwegian tax shelter. *International Tax and Public Finance*, 26(6), 1291–1328. doi:10.1007/10797-019-09568-3
- ATO. (2019). *Black Economy*. Australian Taxation Office. Retrieved from <https://www.ato.gov.au/general/black-economy/>
- ATO. (2020). *Tax in Australia: What you Need to Know*. Australian Taxation Office. Australian Government Printer.
- Australian Law Reform Commission. (2014). *Serious Invasions of Privacy in the Digital Era* (Report No. 1). Retrieved from <https://apo.org.au/node/41124>
- Bajada, C. (2017). *Australia's Cash Economy: A Troubling Issue for Policymakers: A Troubling Issue for Policymakers*. Routledge. doi:10.4324/9781315187372
- Bates v City of Little Rock*, 361 US 516 (1960).
- Baumann, F., & Friehe, T. (2016). Competitive pressure and corporate crime. *The B.E. Journal of Economic Analysis & Policy*, 16(2), 647–687. doi:10.1515/bejeap-2015-0064

- Bazart, C., Beaud, M., & Dubois, D. (2020). Whistleblowing vs. Random Audit: An Experimental Test of Relative Efficiency. *Kyklos*, 73(1), 47–67. doi:10.1111/kykl.12215
- Bennett Moses, L. (2013). How to Think about Law, Regulation and Technology: Problems with “Technology” as a Regulatory Target. *Law, Innovation and Technology*, 5(1), 12.
- Bentley, D. (2019). Timeless principles of taxpayer protection: how they adapt to digital disruption. *eJournal of Tax Research*, 16(3), 679-713.
- Beyes, P., & Bhattacharya, R. (2017, March). *India’s 2016 demonetisation drive: A case study on innovation in anti-corruption policies, government communications and political integrity*. Paper presented at OECD Global Anti-Corruption & Integrity Forum, Paris, France.
- Braithwaite, J. (2002). Rules and Principles: A Theory of Legal Certainty. *Australian Journal of Legal Philosophy*, 27, 47–82. doi:10.2139srn.329400
- Braithwaite, J. (2005). *Markets in Vice, Markets in Virtue*. Federation Press.
- Braithwaite, J. (2013). Flipping markets to virtue with qui tam and restorative justice. *Accounting, Organizations and Society*, 38(6-7), 465. doi:10.1016/j.aos.2012.07.002
- Braithwaite, J. (2018). Minimally Sufficient Deterrence. In M. Tonry (Ed.), *Crime and Justice: A Review of Research*. University of Chicago Press.
- Braithwaite, J., & Hong, S. H. (2015). The iteration deficit in responsive regulation: Are regulatory ambassadors an answer? *Regulation & Governance*, 9(1), 16–29. doi:10.1111/regg.12049
- Braithwaite, V. (2002). *Taxing Democracy*. Ashgate.
- Braithwaite, V., Murphy, K., & Reinhart, M. (2007). Taxation threat, motivational postures, and responsive regulation. *Law & Policy*, 29(1), 137–158. doi:10.1111/j.1467-9930.2007.00250.x
- Braithwaite, V., Reinhart, M., & Job, J. (2018). Getting on or getting by? Australians in the cash economy. In C. Bajada & F. Schneider (Eds.), *Size, Causes and Consequences of the Underground Economy* (pp. 55–69). Routledge. doi:10.4324/9781351149044-4
- Brito, J. (2014). Agency Threats and the Rule of the Law: An Offer You Can’t Refuse. *Harvard Journal of Law & Public Policy*, 37, 553–577.
- Bronitt, S., & Donkin, S. (2012). Australian Responses to 9/11: New World Legal Hybrids? In A. Masferrer (Ed.), *Post 9/11 and the State of Permanent Legal Emergency* (pp. 223–239). Springer. doi:10.1007/978-94-007-4062-4\_10
- Brownsword, R. (2018). Law and technology: Two modes of disruption, three legal mind-sets, and the big picture of regulatory responsibilities. *Indian Journal of Law and Technology*, 14, 1–40.
- Brownsword, R. (2019). *Law, Technology, and Society – Re-imagining the Regulatory Environment*. Routledge. doi:10.4324/9781351128186
- Burg, D. (2004). *A World History of Tax Rebellions*. Taylor & Francis. doi:10.4324/9780203500897

## ***Tax Enforcement in the Black Economy***

CAANZ. (2017). *Submission to the Black Economy Taskforce*. Chartered Accountants Australia and New Zealand. Retrieved from <https://www.charteredaccountantsanz.com/-/media/b28ef2c51a1d42daaf-9517d689d8e6a5.ashx>

Casey, A. J., & Niblett, A. (2016). The death of rules and standards. *Indiana Law Journal (Indianapolis, Ind.)*, 92, 1401.

CaytasJ. (2017). *Regulatory Issues and Challenges Presented by Virtual Currencies*. Retrieved from <https://ssrn.com/abstract=2988367>

Chiarini, B., & Marzano, E. (2016). *Is the Severity of the Penalty an Effective Deterrent? A Strategic Approach for the Crime of Tax Evasion* (CESifo Working Paper No. 6112). Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2867304](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2867304)

Commonwealth. (2017). *Black Economy Taskforce: Final Report*. Australian Government Printer.

CRA. (2017). *Tax Assured and Tax Gap for the Federal Personal Income Tax System*. Canada Revenue Agency.

Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review. Boston College. Law School*, 55, 93.

Dai, Z., Galeotti, F., & Villeval, M. C. (2017). Cheating in the lab predicts fraud in the field: An experiment in public transportation. *Management Science*, 64(3), 1081–1100. doi:10.1287/mnsc.2016.2616

de Zwart, M., Humphreys, S., & Van Dissel, B. (2014). Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK. *The University of New South Wales Law Journal*, 37(2), 713.

Demin, A. (2018). New model of tax administration: Change of paradigm. *Financial Law Review*, 10(2), 11–29. doi:10.4467/22996834FLR.18.008.9138

Department of the Treasury. (2016). *White Paper: Taxation Reform*. Australian Government Printer.

Department of the Treasury. (2018). *Improving black economy enforcement and offences* (Consultation Paper). Retrieved from <https://treasury.gov.au/sites/default/files/2019-03/Consultation-Paper-Improving-black-economy-enforcement-and-offences.pdf>

Dobos, P., & Takacs-Gyorgy, K. (2018). The Factors Influencing the Emergence of Unethical Business Behaviour. *International Journal of Contemporary Management*, 17(3), 51–75. doi:10.4467/24498939IJCM.18.025.9621

Dobos, P., & Takacs-Gyorgy, K. (2019). Possible Smart City Solutions in the Fight against Black Economy. *Interdisciplinary Description of Complex Systems*, 17(3, 3-A), 468–475. doi:10.7906/indexs.17.3.5

*Dombrowski v Pfister*, 380 US 479 (1965).

Draca, M., & Machin, S. (2015). Crime and Economic Incentives. *Annual Review of Economics*, 7(1), 389–408. doi:10.1146/annurev-economics-080614-115808

Dwenger, N., Kleven, H., Rasul, I., & Rincke, J. (2016). Extrinsic and intrinsic motivations for tax compliance: Evidence from a field experiment in Germany. *American Economic Journal. Economic Policy*, 8(3), 203–232. doi:10.1257/pol.20150083

Ernst & Young. (2017). *Reducing the Shadow Economy through Electronic Payments* (Report for Mastercard, 2017). Retrieved from [https://www.ey.com/Publication/vwLUAssets/Report\\_Shadow\\_Economy/\\$FILE/REPORT\\_ShadowEconomy\\_FINAL\\_17.pdf](https://www.ey.com/Publication/vwLUAssets/Report_Shadow_Economy/$FILE/REPORT_ShadowEconomy_FINAL_17.pdf)

Etienne, J. (2013). Ambiguity and Relational Signals in Regulator-Regulatee Relationships. *Regulation & Governance*, 7(1), 35. doi:10.1111/j.1748-5991.2012.01160.x

Farrar, J., Kaplan, S. E., & Thorne, L. (2019). The effect of interactional fairness and detection on taxpayers' compliance intentions. *Journal of Business Ethics*, 154(1), 167–180. doi:10.1007/10551-017-3458-x

Farrar, J., Massey, D. W., Osecki, E., & Thorne, L. (2018). Tax fairness: Conceptual foundations and empirical measurement. *Journal of Business Ethics*, 162(3), 487–503. doi:10.1007/10551-018-4001-4

Faulkner, N., Borg, K., Bragge, P., Curtis, J., Ghafoori, E., Goodwin, D., Jorgensen, B. S., Jungbluth, L., Kneebone, S., Smith, L., Wright, B., & Wright, P. (2018). The INSPIRE Framework: How Public Administrators Can Increase Compliance with Written Requests Using Behavioral Techniques. *Public Administration Review*, 79(1), 125–135. doi:10.1111/puar.13004

Fedeli, S., & Forte, F. (2012). A Game Theoretic Approach to Cross-Border VAT Evasion within EU Member States and its Relationship with the Black Economy. *Economic Analysis and Policy*, 42(2), 209–220. doi:10.1016/S0313-5926(12)50021-4

Gribnau, H. (2015). Corporate social responsibility and tax planning: Not by rules alone. *Social & Legal Studies*, 24(2), 225–250. doi:10.1177/0964663915575053

Grinberg, I. (2018). International Taxation in an Era of Digital Disruption: Analyzing the Current Debate. *Taxes*, 3, 85–118. Retrieved from <https://scholarship.law.georgetown.edu/facpub/2145>

Hatfield, M. (2015). Taxation and Surveillance: An Agenda. *Yale Journal of Law & Technology*, 17, 340–349.

Henriksen, L. F., & Ponte, S. (2018). Public orchestration, social networks, and transnational environmental governance: Lessons from the aviation industry. *Regulation & Governance*, 12(1), 23–45. doi:10.1111/rego.12151

Hoopes, J., Robinson, L., & Slemrod, J. (2018). Public Tax-Return Disclosure. *Journal of Accounting and Economics*, 66(1), 142–162. doi:10.1016/j.jacceco.2018.04.001

Hughes, S. (2012). US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program. *Canadian Journal of Law and Society*, 27(3), 399–425. doi:10.1017/S0829320100010577

*Human Rights Watch and others v Secretary of State for the Foreign and Commonwealth Office and others* [2016] UKIPTrib 15\_165-CH.

IGT. (2018). *The Future of the Tax Profession*. Inspector-General of Taxation. Australian Government Printer.

Iqbal, S., Hussain, M., Munir, M. U., Hussain, Z., Mehrban, S., Ashraf, A., & Ayubi, S. (2019). Crypto-Currency: Future of FinTech. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 1–13). IGI Global. doi:10.4018/978-1-5225-7805-5.ch001

Khiaonarong, T., & Humphrey, D. (2019). *Cash Use Across Countries and the Demand for Central Bank Digital Currency* (IMF Working Paper WP/19/46). International Monetary Fund.

Levy, K. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Emerging Science. Technology in Society*, 3, 1–15.

Lightfoot, G., & Wisniewski, T. (2014). Information Asymmetry and Power in a Surveillance Society. *Information and Organization*, 24(4), 214–235. doi:10.1016/j.infoandorg.2014.09.001

Margulies, P. (2014). Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden. *The Hastings Law Journal*, 66, 1–13.

Margulies, P. (2016). Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights. *Florida Law Review*, 68(4), 1045–1117.

Marks, A., Bowling, B., & Keenan, C. (2017). Automatic Justice? Technology, Crime, and Social Control. In R. Brownsword, E. Scotford, & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation and Technology*. Oxford University Press.

Memdani, L., Kademi, T. T., & Rafay, A. (2021). Effect of Terrorism Financing on selected Global Indices: The Case of 2015 Paris Attacks. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Memon, N., & Lorenz, C. (2016). Does selecting a taxpayer for audit violate civil rights—a critical analysis of the Pakistani High Court’s decision? *eJournal of Tax Research*, 14(3), 766–785.

Millane, E., & Stewart, M. (2019). Behavioural insights in tax collection: getting the legal settings right. *eJournal of Tax Research*, 16(3), 500–535.

Murphy, K. (2019). Moving towards a more effective model of regulatory enforcement in the Australian Taxation Office. Centre for Tax System Integrity (CTSI). Canberra: ANU Press.

Murphy, R. (2014). *In the Shade: Research on the UK’s missing economy*. University of London. Retrieved from <https://openaccess.city.ac.uk/16563/>

*NAACP v Alabama*, 357 US 449, 462 (1958).

NZLC. (2010). *Invasion of Privacy: Penalties and Remedies Report* (Report No. 113). New Zealand Law Commission.

O’Reilly, T. (2013). Open Data and Algorithmic Regulation. In B. Goldstein & L. Dyson (Eds.), *Beyond Transparency: Open Data and the Future of Civic Innovation* (pp. 289–300). Code for America Press.

- OECD. (2017). *The Changing Tax Compliance Environment and the Role of Audit*. Organisation for Economic Cooperation and Development. Retrieved from <https://www.oecd.org/ctp/the-changing-tax-compliance-environment-and-the-role-of-audit-9789264282186-en.htm>
- Parker, C., & Nielsen, V. L. (2017). Compliance: 14 questions. In P. Drahos (Ed.), *Regulatory theory: Foundations and applications* (pp. 217–232). ANU Press.
- Pauch, D. (2018). Gray Economy as Part of Tax Gap. *European Journal of Service Management*, 27(1), 197–210.
- Pintarich v Deputy Commissioner of Taxation* [2018] FCAFC 79.
- Pogarsky, G., Roche, S. P., & Pickett, J. T. (2018). Offender Decision-making in Criminology: Contributions from Behavioral Economics. *Annual Review of Criminology*, 1, 379–400.
- Prebble, R., & Prebble, J. (2010). Does the Use of General Anti-Avoidance Rules to Combat Tax Avoidance Breach Principles of the Rule of Law? A Comparative Study. *Saint Louis University Law Journal*, 55(1), 21–46.
- Rafay, A. (Ed.). (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global.
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Rafay, A., & Ajmal, M. M. (2014). Earnings Management through Deferred Taxes Recognized under IAS 12: Evidence from Pakistan. *Lahore Journal of Business*, 3(1), 1–19.
- Richards, N. M. (2012). The dangers of surveillance. *Harvard Law Review*, 126, 1935.
- Sambo, U., & Sule, B. (2021). Financing as a Livewire for Terrorism: The Case of North-Eastern Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Sampson, S. (2019). Citizen duty or Stasi society? Whistleblowing and disclosure regimes in organizations and communities. *Ephemera*, 19(4), 792–798.
- Schwarcz, D., & Zaring, D. (2017). Regulation by threat: Dodd-frank and the nonbank problem. *The University of Chicago Law Review. University of Chicago. Law School*, 84, 1813.
- Singh, D. B., & Panwar, S. (2017). Study of Effects of Demonetization on the Informal Economy of India. *International Journal of Engineering Technology. Management and Applied Sciences*, 5(5), 552–561.
- Slemrod, J., Ur Rehman, O., & Waseem, M. (2019). *Pecuniary and Non-Pecuniary Motivations for Tax Compliance: Evidence from Pakistan* (Working Paper 19/08). Oxford: University of Oxford.
- Sung, M. J., Awasthi, R., & Lee, H. C. (2017). Can Tax Incentives for Electronic Payments Curtail the Shadow Economy? Korea's Attempt to Reduce Underreporting in Retail Businesses. *Korean Journal of Policy Studies*, 32(2), 85–134.
- Swierczynska, J. (2016). The Reduction of Barriers in Customs as One of the Measures Taken by the Customs Service in the Process of Ensuring Security and Safety of Trade. *Studia Ekonomiczne*, 266, 212–222.

## ***Tax Enforcement in the Black Economy***

Taboada, C. (2015). OECD Base Erosion and Profit Shifting Action 6: The General Anti-Abuse Rule. *Bulletin for International Taxation*, 69(10), 602–608.

Tanzi, V. (2017). Corruption, complexity and tax evasion. *eJournal of Tax Research*, 15(2), 144.

Tasca, P. (2015). *Digital Currencies: Principles, Trends, Opportunities, and Risks* (ECUREX Research Working Paper). Retrieved from [https://faculty.fuqua.duke.edu/~charvey/Teaching/898\\_2016/Readings/Tasca.pdf](https://faculty.fuqua.duke.edu/~charvey/Teaching/898_2016/Readings/Tasca.pdf)

Tsakatika, M. (2016). SYRIZA's electoral rise in Greece: Protest, trust and the art of political manipulation. *South European Society & Politics*, 21(4), 519–540.

Ungureanu, D., & Dascalu, E.-D. (2015). Improving VAT Compliance in Romania by Implementing a New Tool – Tax Lottery Receipts. *Journal of Economic Development. Environment and People*, 4(4), 47–57.

*USA v Robel*, 389 US 258 (1967).

Veit, A. (2019). Swimming upstream: leveraging data and analytics for taxpayer engagement – an Australian and international perspective. *eJournal of Tax Research*, 16(3), 478.

Vousinas, G. (2017). Shadow economy and tax evasion: The Achilles heel of Greek economy. Determinants, effects and policy proposals. *Journal of Money Laundering Control*, 20(4), 386–404.

Walker-Munro, B. (2019a). Regulating Disruption and Development of the Disruption Calculus. *University of Western Australia Law Review*, 46(1), 111–143.

Walker-Munro, B. (2019b). Disruption, regulatory theory and China: What surveillance and profiling can teach the modern regulator. *Journal of Governance and Regulation*, 8(2), 23–40.

Walker-Munro, B. (2020). A Case for Systemic Design in Criminal Law Techno-Regulation. *Criminal Law Journal*, 43(5), 306–324.

Warren, N. (2019). Estimating tax gap is everything to an informed response to the digital era. *eJournal of Tax Research*, 16(3), 536–546.

Wilson, E. (2017). Point of No Return. *EY Tax Insights*, 17, 46–48.

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of *Lex Cryptographia*. Retrieved from <https://ssrn.com/abstract=2580664>

Wu, T. (2010). Agency threats. *Duke Law Journal*, 60, 1841–1857.

Wurth, E. (2012). *A will and a way: An analysis of tax practitioner preparation compliance* (Unpublished PhD thesis). Australian National University.

Wurth, E., & Braithwaite, V. (2016) *Tax practitioners and tax avoidance: gaming through authorities, cultures and markets* (RegNet Research Paper No. 119). Australian National University.

Yeung, K. (2016). Algorithmic regulation and intelligent enforcement. In M. Lodge (Ed.), *Regulation scholarship in crisis?* (LSE Discussion Paper No. 84, pp. 50–62). Academic Press.

*Zweibon v Mitchell*, 516 F.2d 594 (1975).



## ADDITIONAL READINGS

Dur, R., & Vollaard, B. (2019). Salience of Law Enforcement: A Field Experiment. *Journal of Environmental Economics and Management*, 93, 208.

European Parliament. (2016). *Regulation (EU) 2016/679*. General Data Protection Regulation.

## KEY TERMS AND DEFINITIONS

**Black Economy:** Dishonest and criminal activities that take place outside of or involves misuse or abuse of the tax and regulatory systems.

**Regulatory Disruption:** The disconnection of criminal law regulators from their statutory or political objective.

**Tax:** The revenue collected by a government on income, sales, goods and services, or other transactions to fund public spending initiatives.

# Chapter 20

## The Role of Tax Systems in Preventing Corruption

Simla Güzel

Namık Kemal University, Turkey

### ABSTRACT

*The determinants of corruption have long been an important subject for research in the fields of economics and political science. Corruption was not deemed as a significant issue in the pre-democratic era and has become a serious issue later on. Corruption can be defined as “exploitation of public power to gain private gain.” It is a problem that occurs for various reasons and causes various effects. It may occur due to the occurrence of illegal activities in the political and economic system, as well as due to social and individual moral issues. Corruption has disruptive effects on the functioning of the economic, political, and social system. The aim of this study is to determine the duties of states towards a tax system to combat financial corruption. Corruption in the tax system affects the investment environment negatively, which slows down economic growth.*

### INTRODUCTION

The issue of corruption is not a new problem as it has become more popular since the 1990s. Although it is defined in various ways, the most widely used definition of corruption was made by the World Bank. Accordingly, corruption; “*is the exploitation of public power for the sake of private interests*”. Corruption can be considered as an indicator of many problems in society. Therefore, a multidimensional approach needs to be adopted in combatting corruption. Countries that want to fight corruption seriously should pay attention to redefining the role of government in the economy, particularly in the areas entitling officials with discretionary power which are hotbeds for corruption in addition to implementing law and law enforcement actions (Wei, 1999).

In addition to the claims on the positive effects of corruption in terms of facilitating commercial activities, it can be suggested that there are also many negative effects, especially social corruption. Other effects of corruption are the macroeconomic cost to national economic income and/or growth, microeconomic costs to businesses, inequality impacts on the poor, public service delivery impact, state

DOI: 10.4018/978-1-7998-5567-5.ch020

legitimacy impact, stability and the environment impacts (Department for International Development, 2015).

As demonstrated in every state activity, taxation is one of the areas where corruption frequently takes place. Corruptions in taxes, which constitute the most important source of income of the state, may disrupt public services, and inequalities for taxpayers; thus adversely affect voluntary compliance of honest taxpayers. This will shake confidence in the state.

The government has to undertake important duties in fighting corruption. This study evaluates the measures to be taken against the struggles in the tax system. In the study, firstly, the background and main focus of the chapter sections are included, then the concept of corruption is explained and the causes of corruption are discussed, and the effects of corruption are addressed in the next section. Later, the corruption types encountered in the tax system and the effective measures to be taken are explained. Following the section of solutions and recommendations, and future research directions, conclusions are reported in the end.

## **BACKGROUND**

Tanzi (1998) reported that corruption is often associated with state corruption, and in particular, the monopolistic and discretionary authority of the state. Accordingly, such aspects of governmental activities ensure a suitable ground for corruption.

One of the areas where corruption is encountered is tax systems. Tax corruption increases “black money,” which refers to the concealed income used for bribery in relation to other government regulations, procurement, and informal economic activities (Rahman, 2009). In a more corrupt society, tax evasion could be higher since corrupt public servants would increase their income through bribes, while higher tax evasion could lead to higher corruption levels by exacerbating bribe opportunities (Alm, Martinez-Vazquez, & McClellan, 2004). Tax administration and tax system reforms are two key components of revenue generation (Brondolo *et al.*, 2008).

In every economy, tax administration is a key topic. One of the fundamental requirements of a country for substantial development and economic stability is to be able to domestically raise resources that are sufficient to meet the budget needs (Magumba, 2019). A properly functioning tax administration is important to promote economic performance (Rahman, 2009). Establishing an effective taxation system is among the hardest problems for economies. In a study, Liu & Mikesell (2018) reported that complex tax systems lead to higher public corruption levels, higher tax burden, and rely heavily on indirect taxes. Arif & Rawat (2018) recommend that countries should implement policy reforms such as establishing an efficient judicial system is so important for broaden the tax base. In this way, tax administration can function and consequently, tax revenue will improve.

## **MAIN FOCUS OF THE CHAPTER**

Corruption is a versatile concept. This study examines corruption encountered in many activities of the state in the field of taxation. Corruptions in the taxation area, which is the most important source of income of the state, may increase depending on the features of the tax system. In this study, reforms to be applied in fighting tax corruption are evaluated.

## **The Concept of Corruption and Its Reasons**

Having existed for thousands of years, corruption has become a more focused concept in recent years. Although this cannot be directly related to more corruption cases than before; Tanzi (1988) suggests that it can be related to the fact that the state started to play more roles in the economy after the 1960s. The higher level of inclusion of the state in the economy causes more taxes to be collected, increased public spending and the impact of the state on the economy through economic regulations and controls in many countries. Besides, depending on the traditional habits of a country, the bureaucracy's stance against corruption is also important. In addition, due to economic changes, increasing international trade relations and particularly the emergence of transition economies with privatizations are among the other factors that increase corruption.

Corruption is a concept that can be defined in several ways. The most widely used definition of corruption was made by the World Bank. In this definition, corruption is the exploitation of public power for private interests (Wei, 1999). With the purposes of obtaining private gain, public office is exploited if an official accepts, solicits, or extorts bribe. The same abuse of power can be encountered if private agents directly offer bribes to evade public policies and processes for the sake of a competitive advantage and gain. Even without any bribery cases, patronage and nepotism, the theft of state assets, or the diversion of state revenues can be used as a way of exploiting public office for personal benefit. (WorldBankGroup, 2020).

In addition, McMullan (1961) defines corruption as cases when a public official is assigned with doing or not doing any activity, but s/he is doing/not doing the given duty or trying to legitimize the violated duty without valid reasons and accepting money or monetary values against these acts. Leff (1970) defines corruption as the presence of illegal factors that affect the activities of individuals or groups of bureaucracy. Fullerton (2000) also reports that corruption is very dangerous for the systemic existence of a government. Corruption is an infectious, socio-political, economic and moral discomfort that can affect all networks of administration.

Corruption can take place in many ways. Corruptions can occur in the procurement of goods and services, distribution of subsidies, and the privatization of state enterprises. Individuals or companies may want to pay government officials for various reasons. These reasons may include a desire to be included among the bidders on a contract, modification of contract specifications to benefit themselves, to win a contract, to win the contract with inflated prices for the associated goods or services, or for the ability to skimp on the quality of these goods and services (Bhargava, 2005).

Bribes are considered as the most common corruption instruments. Private entities may resort to bribes to "purchase" services provided by central or local governments, or public servants may seek bribes when procuring these services (WorldBank, 2020):

- Government contracts: The government's decision on companies to supply goods, services, and works, along with the terms of their contracts can be changed through bribes. Companies may resort to bribes to win the tender or to make government tolerate the contractual breaches.
- Government benefits: The distribution of government supports, can be affected through bribes.
- Lower taxes: The amount of taxes from private sector can be reduced through bribes. The tax collector or the taxpayer may offer such bribes. In fact, the tax bill is negotiable in many countries.
- Licenses: The issuance of a license, can be ensured through bribes. Politicians and bureaucrats may also deliberately put policies in action to create control rights and profit by selling them.

- Time: States granting permission for certain activities can be accelerated by offering bribes. To extort bribes, the threat of inaction or delay may also be used.
- Legal outcomes: The outcome of a legal process can be altered through bribes for private parties.

However, it is important to distinguish bribes from gifts. From time to time, these two concepts can be confusing. A bribe refers to reciprocity while a gift does not. Despite the importance of defining them, it can be very hard to do so. What turns a gift into a bribe? Is it the size of the gift? What are the cultural factors being effective on the size of such a gift? What if a large gift is not given to a relative of a person who provides the favour rather than the person himself? Is there a distinction between giving the gift obviously or privately? In any case, such questions reveal that it is not always easy to identify a bribe (Tanzi, 1998).

*Nepotism*, another type of corruption, is the assignment of relatives or friends of public servants to positions that the same public servants have the authority of appointment. *Clientelism* is a regime based on patronage relations. Clientelism is characterized by the relations between the “client” and the “patron,” where powerful and rich patrons such as government, members of parliament, political candidates promise incentives for relatively poor clients in return for their votes. *Embezzlement* is the act of stealing money or property by a public servant. Innocent citizens are affected by this act since public employees inappropriately channel resources that are actually meant for public services. It is a form of corruption and abuse of power and could occur in limited settings close to public scrutiny or under impunity. It is a form of rapid acquisition of wealth and a threat in corrupt nations. *Fraud*, on the other hand, occurs when an individual cheats another individual by deception, and usually considered a financial crime (Khan *et al.*, 2020). It is conducted by manipulating individuals or distorting information and facts. Another corrupt behavior, *extortion* is a type of corruption where an individual offers financial gain to another individual for completion of a task more rapidly, preventing the access of the public to the associated service. *Rent seeking* is associated with activities conducted to receive an artificial economic transfer from the state. Such activities could lead to significant economic consequences. Certain factors play a role in prevalent corruption. The factor of *uncertainty of laws and regulations* leads to loopholes for individuals or corporations to benefit from the state that they might not be entitled otherwise. *Opportunity for official misconduct* is another factor. All governments have the authority to enforce the laws and regulations, levy taxes, and apply sanctions against the lawbreakers. Public officials could abuse their duties in levying taxes, duties, etc. and they could discriminate against certain citizens by imposing these duties selectively. *Low income per capita* is another factor. It could be suggested that corruption and poor governance occurs in countries with high poverty and low income per capita. *Poor enforcement of property rights and the rule of law* is another factor. The lack of clear property rights definition could lead to problems by introducing uncertainty to the limits of public and private property rights. This could adversely affect both domestic and foreign investments. Excessive bureaucratic red tape and inefficient justice system lead to higher corruption levels. Another factor is the heightened inclination of the *closed economic and political systems* to social inequality that contributes to high levels of corruption. Political competition, an effective and well-organized political opposition, an independent judiciary system, and freedom of expression (including free media) are important factors that increase social transparency and accountability. These factors could also help reduce the prevalence and magnitude of corruption. The final factor that affects corruption is the historical and cultural factors. Specific historical and cultural structure could be an element in the discussion of cross-country variances in corruption. For example,

## ***The Role of Tax Systems in Preventing Corruption***

gifts could be commonly accepted in certain cultures, while they could be considered corruption in others (Bhargava, 2005).

Although poverty generally leads to public corruption, it may also be associated with corruption among individuals in the private sector. Private sector corruption includes organized crime or even a small tip to the busboy to get the best available table in a restaurant (WorldBank, 2020).

### **Effects of Corruption**

Corruption has many effects on both social and economic senses. Despite views on the positive effects of corruption, it is generally the negative effects which are discussed.

According to those who believe that corruption has positive effects; positive effects can be aroused by bribery under certain circumstances since it enables firms and individuals to avoid burdensome regulations and ineffective legal systems (Gray & Kaufmann, 1998). The idea of positive effects of corruption is based on the perception of it as a factor which facilitates trade flow. Acceleration of the commercial process, which would normally take place more difficultly, is considered as facilitating transactions. Corruption leads to the emergence of free markets in limited freedom situations (Berksoy & Yıldırım, 2017).

Gray & Kauffman (1998) list the negative effects of corruption as follows:

- It escalates transaction costs and leads to economic uncertainty.
- It generally leads to adverse economic outcomes. It prevents long-term international and domestic investments, leads to displacement of talent via rent-seeking efforts, industrial priorities and technological preferences. It amplifies the attraction of grey economy, reduces public revenues, and leads to the levy of ever-higher tax rates on a reduced number of taxpayers. Thus, it reduces the ability of the state to provide significant public goods and services, in addition to corruption and grey economic activities.
- Bribery disrupts fairness. It leads to an increased tax burden particularly on trade and services conducted by small enterprises.
- Corruption cripples the legitimacy of the state.

Corruption hampers economic performance as reported by Sumah (2018). In the report issued by the Department of International Development of the UK, negative effects are suggested as follows (Department for International Development, 2015):

1. The macroeconomic burden to national economic income and/or growth since corruption causes unprofitability and adverse effects on growth.
2. Microeconomic costs to businesses: Ample evidence revealed the impact of corruption on corporate profitability, commercial behaviour, and individual and corporate preferences. It was strongly suggested that corruption has adverse effects on productivity, investment, overall profitability and growth.
3. The effects on the poor via inequality: The economic development of a nation could be exacerbated due to corruption via increased income inequality and could affect the poor disproportionately.
4. The effects on the delivery of public services: The perception of corruption about a government may lower tax revenues and finally adversely affect the delivery of public services.
5. The effects on the legitimacy of the state: It reduces public trust in public institutions.

6. The effects on stability: Corruption often leads to national instability. Highly corrupt states are fragile, and public perception of high corruption levels exacerbates dynamics of conflict in the long run.
7. The effects on environment: Corruption leads adverse environmental outcomes such as high pollutant emissions, depletion of natural resources, illegal trafficking, high deforestation, or high regulation of environmental products such as wildlife and wood.

## **Tax System and Corruption**

In this framework, one of the key areas is taxation institutions, which take place among the main interfaces between the private and public sectors of a country. Fair tax treatment may bring a significant competitive advantage to a taxpayer while unfair tax treatment may hinder success. Taxation is used as a way to encourage and discourage particular economic activities by a good number of countries. In such a case, the administrative process surrounding taxation is more likely to be corrupted (Sharkey & Fraser, 2017).

Corruption is frequently encountered in taxation as in many other fields. Taxes constitute the most important source of income for states, therefore it is important to combat corruption, which may hamper tax collection with sufficient amounts. Because corruption in taxation will lead to insufficiency in public services based on insufficient income.

Tax revenues ratios have been at different levels in developed and developing countries from past to present. The ratio of tax revenues to GDP in developing countries is around 10-20% while it reaches 40% in developed countries. The reason for tax revenues being low in developing countries is related to many factors. Along with the economic structure of a country, political factors such as poor institutions, disintegrated polities, and non-transparency affiliated with weak news media may also lead to low tax revenues. Furthermore, a weak sense of national identity and a poor norm for compliance and other sociological and cultural factors may restrain the collection of tax revenue (Besley & Persson, 2014).

Despite various reasons for low tax revenues; many studies have reported that tax evasion and corruption reduce tax revenues. Besides, tax evasion is considered a corruption activity, and the concept of corruption includes tax evasion as well (Akdede, 2006). As reported by Nawaz (2010) corruption both reduce the collection of tax revenue from the present economy and also damages economic growth, which affects future tax revenue collection.

Table 1 represents CPI which is widely used to determine the ratio of tax revenues of OECD countries to GDP and worldwide corruption level. Countries/territories are scored and ranked by the CPI depending on experts' and business executives' perception of corruption in the public sector of the given country. This composite index consists of 13 surveys and assessments of corruption, which are collected by various trustworthy institutions. CPI values range between 0 and 100. The value 0 indicates the lack of corruption while 100 indicates high-level corruption (<https://www.transparency.org>). As for countries; it can be suggested that the rate of tax revenues is generally high in countries with the least corruption. Denmark, where the level of corruption is the lowest with its CPI value (88), is the country having the highest tax income rate (44.9%). In New Zealand where the CPI value (87) is high, the tax rate is 32.7. In Finland, where the CPI value (85) is, it can be seen that the tax rate is quite high with 42.7. On the other hand, it can be stated that tax rates are low in countries such as Mexico (28), Turkey (41), Slovak Republic (50), Korea (57), Chili (67), which are among the countries with the high level of corruption.

## The Role of Tax Systems in Preventing Corruption

Table 1. Corruption and Tax Revenue in OECD Countries

Countries	Tax Rev.	CPI	Countries	CPI	Tax Rev.
Austria	42,2	76	New Zealand	32,7	87
Belgium	44,8	75	Norway	39,0	84
Canada	33,0	81	Poland	35,0	60
Czech Rep.	35,3	59	Portugal	35,4	64
Denmark	44,9	88	Slovak Rep.	33,1	50
Finland	42,7	85	Spain	34,4	58
France	46,1	72	Sweden	43,9	85
Germany	38,2	80	Switzerland	27,9	85
Greece	38,7	45	Turkey	24,4	41
Hungary	36,6	46	United Kingdom	33,5	80
Iceland	36,7	61	USA	24,3	71
Ireland	22,3	73	Chili	21,1	67
Italy	42,1	52	Estonia	33,2	73
Korea	28,4	57	Israil	31,1	61
Luxemburg	40,1	81	Slovenia	36,4	60
Mexico	16,1	28	Latvia	30,7	58
Netherlands	38,8	82	Lithuania	30,3	59

Source: Corruption Perceptions Index (2019).

Note: The ratio of Tax Revenue to GDP is formed using the data of OECD tax revenue.

Denmark has been preserving its status as a country with the highest CPI and lowest corruption for long years. This is due to the advanced press freedom, accessible information about public expenditure, better standards for integrity for public officials, and autonomous judicial systems in the country (Ministry of Foreign Affairs of Denmark, 2020).

A good body of research in the literature report that corruption has a negatively impacts tax incomes. In a study analysing the effect of institutional and structural variables on tax revenues, Ajaz and Ahmad (2010) used a panel data set for 25 developing countries over the period 1990-2005. The findings of the study show that corruption adversely affects tax collection, on the other hand, successful governance bring along better performance in terms of tax collection. Nawaz (2010) states that tax evasion and corruption have always been an important problem. Tax evasion and corruption can generally ambiguously affect entrepreneurial activities. Therefore, negative consequences may occur in economic growth. According to Aghion *et al.* (2016), lessening corruption brings along the largest potential impact on welfare gain by affecting the uses of tax revenues. Orucu, Aysu & Bakırtaş (2012) analysed the relationship between corruption and corporation tax incomes based on the data of 16 OECD countries between 1996 and 2010. In this analysis, it was found that corporation tax incomes increase as corruption decreases. In addition, Atilla (2008) reports that decreasing corruption contributes to a better governance and more transparency in public finance management, thus increases public resources (Rafay, 2021).



A broad tax base and acceptable tax compliance have been supported by economic institutions, political institutions, and social and cultural norms. Citizens who are aware of the importance of ensuring wise spending of tax revenues demand for accountable and transparent government. (Besley & Persson, 2014). Swanepoel & Meirng (2017) report that economic crimes such as money laundering, corruption, fraud, and tax evasion often lead to some apparent financial and moral consequences (Lokanan & Chopra, 2021). In this study, a survey was applied to 140 people in South Africa on corruption, fraud, and tax evasion and it was found that the most effective factor in reducing these economic crimes in a society is the existence of moral values in a society.

Paying bribes to public officials to reduce tax obligations directly affects the revenues of a state and hampers voluntary compliance with tax laws and regulations. Seeing that paying taxes would only further lead to inequities by transferring tax due to a corrupt and inefficient tax administration, an honest taxpayer would prefer avoiding this competitive disadvantage and seeking to either evade taxes or bribe an official to pay less (Bridi, 2010).

Tax administration, which is an important element of a state's development and economy, significantly affects the state's capacity to spend on public goods hence worsening the consequences of inefficiency and revenue leaking. In the field of tax administration, corruption also deters honest taxpayers by attracting their attention to the black-market Tax administration is an appropriate sector for corruption to take place since there are numerous opportunities and incentives to engage in illegal activity (Bridi, 2010).

Many factors may lead to corruption in tax administration. These are listed as follows (Purohit 2007; Asher n.d.):

*The complexity of tax laws and procedures:* The corruption in the tax system is higher as a result of the complex tax laws and procedures. In a highly corrupt environment, it is more possible to encounter tax evasion. Taxpayers would not be aware of their rights and would be more exposed to discriminatory actions and exploitation.

*Monopolistic and Discretionary Power of Tax Officials:* Tax officers perform significant functions in tax collection operations. Thus, the tax officer represents the tax authority for a particular taxpayer. This monopolistic authority allows tax officers to persuade taxpayers to conduct corrupt practices. *Lack of Monitoring and Supervision:* The asymmetrical information makes it difficult for the central administration to supervise officers and hold them accountable. The lack of supervision and accountability may prevent the public servants from conducting their public duties. *Unwillingness of Taxpayers to Pay Taxes:* In some developing countries, significant results of corruption include the extreme unwillingness in taxpayers' compliance and thus their readiness to bribe tax collectors with the purpose of reducing their tax liability. In cases of an obvious gain, many taxpayers are ready to provoke tax collectors. This phenomenon is familiar for a good number of middle-income countries.

*Political Leadership:* Corruption is sustained, created and protected by political leaders most of the time. Various corrupt transactions are typically associated with a hierarchy of administrative levels.

*Overall Government Environment:* The corruption level in tax administration is usually in parallel with the one in the administrative environment as a whole. Fewer opportunities are offered in liberal economic systems for corruption compared to socialist systems.

## **How to Fight Corruption in Tax System?**

One of the areas where corruption is frequently observed in both developed and developing countries is tax systems. Corruption weakens the will of honest tax officers, reducing the sense of guilt, increasing the number of bribery officers and reducing the quality of management (Gediz Oral, 2011).

Tanzi (1998) reported that corruption is never a simple phenomenon that could be explained by a single factor. If it was easy to explain it by a single factor, the solution would also be simple. Tax reform measures should tackle not only corporate corruption, but also those induced by tax administration. There is a close correlation between poor administration and pervasive corruption and they mutually reinforce one another. Rahman (2009) reported six reasons to reform the tax administration as follows:

- Tax administration provides a crucial motive for investments. Improvements in tax administration may attract higher investments, leading to higher growth and lower poverty rates.
- Tax reforms reduce tax costs. Independent of implemented tax policies, the revenues increase with a functional policy when compared to a non-functional one.
- A well-functioning administration raises tax revenue.
- In an environment of mistrust, tax policy reform would not be a remedy without an administrative reform; neither the tax officers nor the businesses are trusted by each other.
- Tax corruption drives corruption to different paths; reform is crucial in blocking the “supply lines” of corruption.
- A modern tax administration is required to cope with the sophistication of corporate operations in the current global economy.

Tax administration, which is an important element of a state’s development and economy, significantly affects the state’s capacity to spend on public goods and services, hence worsening the consequences of inefficiency and revenue leaking. In the field of tax administration, corruption also deters honest taxpayers by attracting their attention to the black-market since it is a more attractive alternative. Tax administration is an appropriate place for illegal activity (Bridi, 2010).

Rahman (2009) states that short- to medium-term and medium- to long-term reforms can be implemented in fighting corruption in taxation for the tax office.

Short- to medium-term reforms can be explained as follows: Being simpler processes, *simplify, standardize, and harmonize tax procedures* reduce the discretionary power of tax officers and abuse of tax laws, lessening the burden for companies to comply (Rahman, 2009). The important condition for taxpayers to comply with the law is that the legislation is simple, simple and understandable. Laws, which are constantly changing and having a complex structure, may cause taxpayers to fail to pay their taxes, even unintentionally due to the confusion. In addition, the complexity of laws poses difficulties for supervisors and judicial bodies. (Gediz Oral, 2011; İşler & Kutluay Tutar, 2019). Liu & Feng (2014) indicated that the nations with more complex tax systems were more susceptible to higher levels of corruption when compared to those with less complex tax systems. Efforts should be made to create as clear and understandable texts as possible, while preparing tax-related regulations, in order to find solutions to the problems caused by the complex tax legislation for taxpayers in consideration of the principle of “legal certainty”. In this way, the tax becomes understandable and the taxpayers’ problems arising from uncertainty are eliminated. (Uyumez, 2016).

A lower tax burden can be effective to ensure compliance only with an effective enforcement mechanism. Record-keeping, filing tax returns, voluntary registration, and debt collection should be enforced by law. Based on the self-assessment principle, regular taxpayers could conduct their businesses without excessive auditing, and non-compliant taxpayers should be prosecuted (Rahman, 2009). A proper regulatory framework, speedy enforcement of laws, and prosecution of the offenders are required to ensure a functional anti-corruption strategy in tax administration. This is also true for the justice system and could be considered an external function of the reforms (Zuleta, 2008). *Conduct taxpayer outreach and education.* Providing information for the taxpayers reduces corporate misconceptions and confusions on tax policies and procedures and raises awareness on the advantages of legal record-keeping such as rapid evaluation and lower probability of an audit. *Institutionalize an effective control and audit system.* Experience suggests that a higher number of corporations would comply with tax payments when they recognize their obligations and consider the tax administration as fair in non-compliance procedures. The risk-based auditing system leads to effective auditing and efficient management of the resources (Rahman, 2009). Middle- and long-term reform policies include the following: *Institutionalize e-services and automation:* Limiting face-to-face interactions between businesses and tax officers would lead to lower corruption opportunities. Information could be effectively collected from taxpayers and other parties (such as banks and government agencies) and clerical functions are minimized through electronic applications. It would also allow the businesses to file returns, declare and pay taxes rapidly and easily. Another significant benefit of risk-based management approaches is automation (Rahman, 2009; Sinha, 2021; Jayasekara, 2021).

The advances in information and communication technologies (ICT) reward good and effective work. Therefore, one of the most significant obstacles to tax reform is the development of strategic, historical, and politically correct tax reform knowledge base in the constitution and the level of development (Zuleta *et al.*, 2007). *Introduce an effective human resource management policy:* A transparent and fair tax administration and streamlined policy for recruitment, performance appraisal, career development for officers is very important (Rahman, 2009). Tax officers need not only high wages but also opportunities to career development (Zuleta, 2008). A good number of tax administrations are top-down organisations associated with the term obedience. Promotion is usually based on seniority. Younger staff members are given fewer opportunities to improve their skills. *Institutionalize a streamlined and transparent appeal procedure:* An impartial, rapid, and transparent appeal process helps companies earn trust in the whole system. *Reorganize tax administration by type of taxpayer:* Rational and streamlined tax authority headquarters and local office network should be established based on the number of taxpayers to improve efficiency. Most revenue administrations are endeavouring for such an institutional restructuring. The tax authority can better understand each category of companies by means of segmented service delivery allowing for informed monitoring of taxpayers and tax officers. *Ensure the tax authority's autonomy:* Despite the fact that the tax authority is usually under the auspices of the Ministry of Finance, it is necessary to take precautions to empower the administrative autonomy of tax services. Autonomy improves the transparency, budget of the tax administration along with the increased effectiveness and efficiency of the expenses (Rahman, 2009).

It can be suggested that in addition to these reforms, tax structure also will be effective on corruption. The design of the tax structure, for instance, tax base should be as wide as possible. When the number of taxpayers is below potential, the tax burden per individual would increase considerably and would be too heavy (Purohit, 2007). High tax burden not only negatively affects voluntary tax compliance, but also leads to inequality among taxpayers. Besides, Zuleta *et al.* (2007) report that more focus on direct

## ***The Role of Tax Systems in Preventing Corruption***

and progressive income and property taxes will be more fruitful. For Liu & Maksel (2018), indirect taxes are more common in countries with high corruption. In indirect taxes, it is regarded that such taxes cause financial illusion. Fiscal illusion reflects “systematic, persistent, recurring and consistent” citizen misperception on key fiscal parameters since the citizens would not be aware of the most important fiscal elements. This idea underlines the significant and regular underestimation of the government program costs by the citizens. Public servants will be regarded as “self-serving.” They would be perceived to design and manipulate fiscal systems to create a fiscal illusion. Thus, leading to the underestimation of the actual financial burden by the taxpayers and support of large public revenues and expenditures in the end by the same. Finally, the efforts of private entities to model the tax structure would be welcomed even further.

Taxpayers may systematically underestimate the tax burden, leading to increased indirect tax volume instead of direct taxation since indirect taxes are incorporated into (and therefore ‘hidden’ in) the prices (Sausgruber & Tyran, 2005). Asher (n.d.) reported that this would lead to the preference of withholding provisions, especially in capital revenues. This could be associated with a significant transformation towards the self- assessment of taxes. However, the self-assessment system should be assisted by a tax office or administration with effective auditing facilities to function properly.

## **SOLUTIONS AND RECOMMENDATIONS**

Being a situation that adversely affects countries in many respects, corruption especially in the field of taxation is widespread and negatively affects the inability of states to obtain sufficient income and the principle of justice in taxation. Accordingly, some regulations are needed in tax administration and tax system. Policies for combatting tax evasion and bribes are important in the tax field. Rahman (2009) lists these policies as follows: *Simplify, standardize, and harmonize tax procedures, conduct taxpayer outreach and education, institutionalize an effective control and audit system, institutionalize e-services and automation, introduce an effective human resource management policy, institutionalize a streamlined and transparent appeal procedure, reorganize tax administration by type of taxpayer, ensure the tax authority’s autonomy.*

Mechanisms to monitor tax practices and punish corrupt practices could be strengthened through various ways such as (Asher n.d.):

- Parliamentary oversight, independent audit and investigative organisations.
- The presence of a tax ombudsman in addition to special tax tribunals and courts to rapidly resolve the tax disputes.
- Investigation of fiscal responsibilities and resources at different government levels.
- The employment of indirect regulators such as credit-rating agencies, insurance companies, and ensuring the availability of instruments for numerous economic agents and the availability of public information on government finances and tax policies.
- Implementation of particular country- and context-specific methods to expand the number of taxpayers in the country.

It is important that the reforms to be implemented, on one hand, facilitate taxpayer’s compliance with tax obligations, and on the other hand, improve the efficiency of tax audits and improve administration.

## **FUTURE RESEARCH DIRECTIONS**

This study evaluates the measures to be taken against corruption in the financial field, which has an important place among all corruption types and may arise from the flaws in the tax systems. Further studies, including comprehensive empirical analysis to identify the relationship between tax structure and corruption, will contribute to the literature.

## **CONCLUSION**

It is quite difficult to identify both the definition and the causes of corruption, which is a versatile concept, and to find solutions to overcome. Therefore, many countries today are in search of ways to fight corruption. Corruption, which can be seen in many areas, is evaluated especially in terms of tax systems in this study.

Corruption in the field of taxation, which is the most important source of income of the state, means that the state has to give up such income. In this case, the government may be obliged to perform the public services below the optimal level. Corruption shakes the confidence of the state, causing honest taxpayers to question this situation and bringing an adverse impact on their voluntary tax compliance. Corruptions in the tax system affect the investment environment negatively, which slows down economic growth. Measures to be taken for tax compliance will mitigate the tax cost and increase the amount of income to be included in the budget as a tax.

Tax evasion and related bribes are also generally high in countries with a high tendency to corruption. It can be suggested that the measures to be taken for tax administration and taxpayers are very important. The reasons of corruption in tax systems are; the presence of factors such as the complex tax laws and taxation procedures, the insufficient audit of tax officers working in tax administrations, insufficient accountability in the tax system, the unwillingness of taxpayers to pay taxes, and suitable environment prepared by the political administration for corruption. In this regard, it is important to simplify tax laws, not to make frequent changes in the laws, to increase accountability, and to tighten audits for both tax administrations and taxpayers. In order to improve the trust in the state, it will be effective to take precautions to minimize tax evasion and tax avoidance by means of the tax bureaucracy control, independent audit and tax ombudsmen, to use tax courts more efficiently for the rapid resolution of tax disputes, to control the allocation of resources, at every level of the state, to use economic institutions such as credit rating agencies and insurance companies to inform the public, to develop tax base considering specific features of the given country.

Even though the main purpose of taxation is to generate income, it is also important to ensure fair taxation. However, in countries where there is a high tendency to corruption, indirect taxes, which undermine the principle of justice and the power of financial solvency, are higher in taxation since sufficient income cannot be obtained directly from taxes. Therefore, withholding provisions is used more particularly for capital income. This can be supported with a sound shift towards self-assessment of taxes, which needs to be supported with an efficient audit system.

In addition, countries with low corruption are developed in terms of economic and political institutions as well as having developed social and cultural norms. Budget accountability and transparency regarding public expenditures are required to increase the trust of individuals to the state. Only through this way of improving volunteer compliance with taxation, corruption can be eliminated.

## DISCLAIMER

The contents and views of this chapter are expressed by the author in her personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## REFERENCES

- Aghion, P., Akcigit, U., Cagé, J., & Kerr, W. R. (2016). *Taxation, corruption, and growth* (Working Paper Series, No. 21928). NBER.
- Ajaz, T., & Ahmad, E. (2010). The effect of corruption and governance on tax revenues. *Pakistan Development Review*, 49(4), 405–417. doi:10.30541/v49i4Ipp.405-417
- Akdede, S. H. (2006). Corruption and tax evasion. *Doğuş Üniversitesi Dergisi*, 7(2), 141–149. doi:10.31671/dogus.2019.247
- Alm, J., Martinez-Vazquez, J., & McClellan, C. (2014). *Corruption and Firm Tax Evasion*. (Working Paper, 14-22). International Center for Public Policy.
- Arif, I., & Rawat, A. S. (2018). Corruption, governance & tax revenue: Evidence from EAGLE countries. *Journal of Transnational Management*, 23(2), 119–133. doi:10.1080/15475778.2018.1469912
- Asher, M. G. (n.d.). The design of tax systems and corruption. Public Policy Programme, National University of Singapore.
- Atila, G. (2008). *Corruption, taxation and economic growth: theory and evidence* (Working paper E 2008.29). CERDI.
- Berksoy, T., & Yıldırım, N. E. (2017). Yolsuzluk kavramına genel bir bakış: Problemler ve çözüm önerileri [An overview of the concept of corruption: Problems and solutions]. *Journal of Awareness*, 2(1), 1–18.
- Besley, T., & Persson, T. (2014). Why do developing countries tax so little? *The Journal of Economic Perspectives*, 28(4), 99–120. doi:10.1257/jep.28.4.99

Bhargava, V. (2005). *The cancer of corruption*. World Bank Global Issues Seminar Series. Retrieved from <http://siteresources.worldbank.org/EXTABOUTUS/Resources/Corruption.pdf>

Bridi, A. (2010). *Corruption in tax administration* (U4 Expert Answer No. 229). Transparency International. Retrieved from <https://www.u4.no/publications/corruption-in-tax-administration.pdf>

Brondolo, J., Bosch, F., Borgne, E. L., & Silvani, C. (2008). *Tax Administration reform and fiscal adjustment: The case of Indonesia (2001-07)* (Working Paper No: WP/08/129). International Monetary Fund.

Corruption Perceptions Index. (2019). Retrieved from <https://www.transparency.org/en/cpi/2019/results/table>

Department for International Development. (2015). *Why corruption matters: understanding causes, effects and how to address them Evidence paper on corruption*. Retrieved from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/406346/corruption-evidence-paper-why-corruption-matters.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/406346/corruption-evidence-paper-why-corruption-matters.pdf)

Fullerton, R. (2000). Political leaders must be held accountable for corruption. *Crossroads*, 6(4), 5–6.

Gediz Oral, B. (2011). Mali yolsuzlukla mücadele stratejileri: Türk vergi sistemi [Anti-financial corruption strategies: Turkish tax system]. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(3), 403–431.

Gray, C. W., & Kaufmann, D. (1998). Corruption and development. *Finance & Development*, 35(1), 7–10.

Işler, K., & Kutluay Tutar, F. (2019). Yolsuzluk ve ekonomik etkileri: Türkiye örneği [Corruption and economic impacts: In Turkey]. *Atlas International Refereed Journal on Social Sciences*, 5(17), 32–59.

Jayasekara, S. F. S. D. (2021). Risk-based AML/CFT Regulations for Effective Supervision. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2

Leff, N. H. (1970). Economic Development through bureaucratic development. In *Political Corruption: Readings in Comparative Analysis*. Transaction Books.

Liu, C., & Mikesell, J. L. (2018). Corruption and tax structure in American States. *American Review of Public Administration*, 49(5), 585–600. doi:10.1177/0275074018783067

Liu, Y., & Feng, H. (2014). *Tax structure and corruption: Cross-country evidence* (Working Paper 14-27). International Center for Public Policy.

Lokanan, M., & Chopra, G. (2021). Money Laundering in Real Estate (RE): The Case of Canada. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Magumba, M. (2019). Tax administration reforms: Lessons from Georgia and Uganda (ICTD African Tax Administration Paper 5). Institute of Development Studies.

McMullan, M. (1961). A theory of corruption. *The Sociological Review*, 9(2), 181–201. doi:10.1111/j.1467-954X.1961.tb01093.x

## ***The Role of Tax Systems in Preventing Corruption***

Ministry of Foreign Affairs of Denmark. (2020). *Denmark is the least corrupt country in the World*. Retrieved from <https://studyindenmark.dk/news/denmark-is-the-least-corrupt-country-in-the-world>

Nawaz, F. (2010). *Exploring the relationships between corruption and tax revenue* (U4 Expert Answer No. 228). Transparency International. Retrieved from <https://www.u4.no/publications/exploring-the-relationships-between-corruption-and-tax-revenue/>

Orucu, A. I., Aysu, A., & Bakırtaş, D. (2012). Yolsuzluğun kurumlar vergisi gelirleri üzerine etkisi: OECD ülkeleri analizi [The impact of corruption on corporate tax revenues: Analysis of OECD countries]. *Maliye Dergisi*, 163, 539–556.

Purohit, M. C. (2007). Corruption in tax administration, performance accountability and combating Corruption. In A. Shah (Ed.), *World Bank Public Sector Governance and Accountability Series*. Academic Press.

Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Rahman, A. (2009). *Tackling corruption through tax administration reform* (Note Series No. 48312). Investment Climate Department, World Bank Group.

Sausgruber, R., & Tyran, J. R. (2005). Testing the Mill hypothesis of fiscal illusion. *Public Choice*, 122(1-2), 39–68. doi:10.1007/11127-005-3992-4

Sharkey, N., & Fraser, J. (2017). Applying foreign anti-corruption law in the Chinese tax context: Conceptual difficulties and challenges. *eJournal of Tax Research*, 15(2), 312-332.

Sinha, A. (2021). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Sumah, S. (2018). Corruption, causes and consequences, trade and global market. In *Trade and Global Market*. Retrieved from <https://www.intechopen.com/books/trade-and-global-market/corruption-causes-and-consequences>

Swanepoel, B., & Meiring, J. (2017). Morality associated with fraud, corruption and tax evasion in South Africa. *eJournal of Tax Research*, 15(2), 333-358.

Tanzi, V. (1998). *Corruption around the world: Causes, consequences, cope, and cures (WP/98/64s)*. International Monetary Fund.

Uyumez, M. E. (2016). Vergi mevzuatının karmaşıklığı ve uzlaşma yöntemi bağlamında vergi uyumunun değerlendirilmesi [Assessing tax compliance in the context of the complexity of tax legislation and method of settlement]. *Ekonomi Bilimleri Dergisi*, 8(1), 75–92.

Wei, S.-J. (1999). *Corruption in economic development beneficial grease, minor annoyance, or major obstacle?* (Working Paper No. 2048). World Bank Group. Retrieved from <https://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-2048>

Worldbank. (2020). Retrieved from <http://www.worldbank.org>



Worldbank Group. (n.d). *Helping Countries Combat Corruption: The Role of the World Bank*. <http://www1.worldbank.org/publicsector/anticorrupt/corruptn/cor02.htm>

Zuleta, J. C. (2008). *Combating corruption in the revenue service: the case of VAT refunds in Bolivia* (U4 Brief No. 14). Transparency International. Retrieved from <https://www.u4.no/publications/combating-corruption-in-the-revenue-service-the-case-of-vat-refunds-in-bolivia>

Zuleta, J. C., Leyton, A., & Fanta, E. (2007). Combating corruption in revenue administration: The Case of VAT refunds in Bolivia. In J. E. Campos & S. Pradhan (Eds.), *The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level*. The World Bank Group.

## ADDITIONAL READINGS

Ali, A. M., & Isse, H. S. (2003). Determinants of economic corruption: A cross-country comparison. *The Cato Journal*, 22(3), 449–466.

Barreto, R. A., & Alm, J. (2003). Corruption, optimal taxation, and growth. *Public Finance Review*, 31(3), 207–240. doi:10.1177/1091142103031003001

Del Monte, A., & Papagni, E. (2001). Public Expenditure, corruption, and economic growth: The case of Italy. *European Journal of Political Economy*, 17(1), 1–16. doi:10.1016/S0176-2680(00)00025-2

Glaeser, E., & Saks, R. (2006). Corruption in America. *Journal of Public Economics*, 90(6-7), 1053–1072. doi:10.1016/j.jpubeco.2005.08.007

Goel, R. K., Nelson, M. A., & Naretta, M. A. (2012). The Internet as an indicator of corruption awareness. *European Journal of Political Economy*, 28(1), 64–75. doi:10.1016/j.ejpoleco.2011.08.003

Hauner, D., & Kyobe, A. (2010). Determinants of government efficiency. *World Development*, 38(11), 1527–1542. doi:10.1016/j.worlddev.2010.04.004

## KEY TERMS AND DEFINITIONS

**Bribes:** Dishonestly persuade someone to act in one's favour by a gift of money or other inducement.

**Corruption:** Dishonest or fraudulent conduct by those in power, typically involving bribery.

**Tax Administration:** A unit of government that collect all tax revenues an efficient way.

**Tax Evasion:** It is an illegal activity in which a person or company avoids to pay tax.

**Tax Officer:** Tax officers are civil servants, working for tax administration.


**Tax Payer:** A taxpayer is a person or organization subject to pay a tax.

**Tax System:** A type of official unity government system connected to unity government policy created to control, collate, manage tax law and tax legislation.

# Chapter 21

## Tax Disclosures in Financial and CSR Reporting as a Deterrence for Evasion

**Fábio Albuquerque**

 <https://orcid.org/0000-0001-8877-9634>  
*Instituto Politécnico de Lisboa, Portugal*

**Julija Cassiano Neves**

*Instituto Politécnico de Lisboa, Portugal*

### ABSTRACT

*This chapter is about the mandatory disclosure of income tax as required by international financial reporting standards (IFRS) and standards issued by Portuguese regulatory bodies. The chapter also elaborates the most relevant disclosures from the perspective of corporate social responsibility (CSR). Furthermore, it highlights the most influential CSR reporting standards to answer the question that whether these standards adequately address the issue of income tax payment as a factor of CSR. Finally, it also reviews the international and Portuguese theoretical and empirical academic research available about income taxes and related subjects, such as disclosures, corporate tax as a CSR matter, and tax aggressiveness of corporations. Future research may be conducted geographical reporting of income tax expense and its relationship with the effective tax rate (ETR) and other independent variables.*

### INTRODUCTION

If one looks at the whole known history of humankind, corporate social responsibility (CSR) is a relatively new phenomenon (Wells, 2002). There are many views on what exactly constitutes CSR and whether one should apply any limits to this phenomenon (Garriga & Melé, 2004). We are living in a world where technology is rapidly developing (Rafay, 2019), taking all other aspects of human life with it, including the phenomena which emerged with the industrial revolution and subsequent globalisation.

DOI: 10.4018/978-1-7998-5567-5.ch021

As CSR is a part of our life subject to constant change, we hardly can set any limits to it and the concept will take different shape each time there is a significant change in the corporate world. In this way, CSR has been developing and is changing over the time of its existence (Jusoh, 2020). From environmental concerns, human rights, health, and safety we see the development to respecting the legal order and, lately, we see that paying taxes is already being looked at as an element of CSR.

On one hand, income taxes are an element of financial reporting, virtually always present since public finances and tax is a constitutive element of the most of modern societies and states. Contributing to the public finances is clearly part of how business contributes to society, its sustainability, its development, and well-being. The other perspective, which is also embedded in the financial reporting, is that tax appears to be and may feel like a cost. In line with the basic laws of commerce and business, there is an effort to reduce the costs in search of more efficient profit-making.

These two approaches are being discussed in media and at the academic level. The debate has been even more prominent after the global financial crisis of 2008, conditioned by the slow economic recovery and the budgetary needs of many countries. As Avi-Yonah (2008) puts it, the question is “whether publicly traded U.S. corporations owe a duty to their shareholders to minimize their corporate tax burden through any legal means, or if instead, strategic behaviours like aggressive tax-motivated transactions are inconsistent with CSR” (2014). According to Scheiwiller and Symons (2014), who are discussing tax and CSR in an article published the OECD Observer online, “the groups campaigning on tax would like to see a change in reporting standards to require companies to report their tax affairs in much more detail in their accounts, essentially a profit and loss account, assets and tax charge for every country where they operate, known as country-by-country reporting”.

These two leading forces give an impetus to the debate, scientific research, and development in the field. As will be clear from further discussion, it looks that nowadays there seems to be already an agreement that paying tax has already started to develop as a CSR issue. Some companies have started to include tax payments as one of the issues discussed in their CSR reports. Scheiwiller and Symons (2014) give the example of the mining giant Anglo American: the total tax contribution by country is reported in CSR reports as part of their economic dimension, including all the different taxes paid and collected and explaining how all these taxes are generated across the life-cycle of a mining project, showing that two thirds of their tax payments are made in developing countries.

The inclusion of tax as an aspect for CSR reporting is indeed presenting tax information in a way that is easy to understand. Notwithstanding, considering that no international and/or mandatory standards effectively exist in this regard, the information highlighted in CSR reports might be selective information cherry-picked by the reporting entity. The financial reporting standards, on the other hand, provide for certain minimum mandatory reporting and disclosure on income tax matters.

The objectives of the research shall be to evaluate the existing accounting standards and social responsibility reporting rules in terms of whether these rules provide for sufficient disclosure in order to enable the users of the information to evaluate (i) the financial position of a company from the tax exposure perspective and (ii) assess the corporate responsibility of a company from the perspective of paying its “fair share” of tax bill, both items capable of eventually influencing the decisions of the users of financial information and decisions and opinions of the widest range of stakeholders.

Due to the limitations inherent in the requirements applicable to a book chapter, the object of the research is not to provide an exhaustive research of all perspectives that are related to the issue of accounting and reporting of corporate and deferred taxes, corporate taxation itself, or corporate disclosures. On the one hand, the present research will be limited to the identification and analysis of the income tax

reporting disclosure requirements relevant from the CSR standpoint. On the other hand, and from the CSR reporting perspective, the chapter will only focus on the disclosure requirements related to taxation (if any). Consequently, the research of any social aspects of the reporting for income taxes that touch upon business ethics, concurrent international scandals on profit shifting, tax planning or tax avoidance concepts, national tax and accounting rules in different countries other than Portugal, falls outside of the scope of the present work.

In this way, the research of accounting rules will be limited to the research of international standards and interpretations issued by International Accounting Standards Board (IASB, 2009), Financial Accounting Standards Board (FASB) and the standards and interpretations issued by the Portuguese Accounting Standards Board (*Comissão de Normalização Contabilística* or CNC, in the Portuguese acronym). Here, the objective will be to provide an overview of disclosure requirements and to identify those requirements that are most relevant from the CSR perspective.

Next, the research of CSR reporting rules will focus on the main standards used by enterprises worldwide, namely United Nations (UN) Global Compact, Global Reporting Initiative (GRI, 2013a, 2013b) G4 Sustainability Guidelines (GRI G4 Guidelines) and the Organisation's for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises (OECD Guidelines). The objective of this part of the research will be to ascertain whether any of these organisations considers income tax as a matter of CSR and if, as a consequence, there are any standards related to reporting on income tax as one of the sustainability factors.

Further, there is the aim of exploring the national and international academic literature about reporting for income taxes and the disclosure of such information from the CSR standpoint.

Based on the foregoing, the overall purpose of the present work is to contribute to and develop, on the one hand, the existing national research on the disclosure of income tax matters and CSR reporting. As will be demonstrated further by the review of the academic literature, the current research is more specific in comparison to the previous more general national research available both on the income tax disclosure and reporting and CSR reporting. Namely, taking into consideration the CSR angle of the present research, this work presents a novelty at the level of national academic research by putting income tax reporting and disclosure as a subject of CSR.

## **BACKGROUND**

There is a conflict between the purpose of fiscal activities reported on CSR from the view of shareholders and society in general, which is clearly highlighted by Christensen and Murphy (2004) as it follows:

*“It is therefore curious that tax minimization through elaborate and frequently aggressive tax-avoidance strategies is regarded as one of the prime duties that directors are required to perform on behalf of their shareholders. It is more curious still that the debate about CSR, which has touched on virtually every other area of corporate engagement with broader society has scarcely begun to question companies in the area where their corporate citizenship is most tangible and most important: the payment of tax.”*

The companies' dilemma between optimizing shareholders wealth and the social responsibility associated with paying a fair share of taxes, from the view of external stakeholders, such as tax authorities and the general public, is also stressed by Huseynov and Klamm (2012). According to these authors,

while the “reductions of tax expense can be viewed as economically necessary”, on the other hand, the tax avoidance, “for any reason, may be viewed by some as socially irresponsible”.

That conclusion comes from an evidence gathered by the authors through their informal studies of CSR statements published by a wide selection of multinational corporations, allowing the authors to conclude that “company directors do not regard tax payment as a part of the CSR agenda”, which is in the opposite way of the ethical behaviour that is expected to be reported there (Christensen & Murphy, 2004).

More specifically, Jenkins and Newell (2013) state that, despite the recognition of the importance of taxation to financing the policy-makers social actions and, additionally, the tax issues, including tax strategy, as part of the CSR matters, there is still a “surprising lack of attention to tax avoidance and evasion as a CSR issue (...), even among those companies that pride themselves on being CSR leaders”. The evidence leads authors to conclude that voluntary actions or commitments are not enough to eliminate the problem of tax avoidance, also considering that public pressures to solve them tend to be uneven.

The empirical analysis performed by Preuss (2012), while examining a sample of large firms that are headquartered in two off-shore finance centers, suggested this inconsistency when the author suggested that “the duplicity inherent in a tax haven-based company professing social responsibility throws open a range of challenges regarding the conceptualization of CSR”.

However, the findings and perspectives are not necessarily consensual. Then, further researches in this area, given its relevance, seem to be necessary, and they are indeed progressively arising to solve the several issues and conflicts associated with the relation between tax avoidance and CSR from different perspectives of analysis.

Huseynov and Klamm (2012), from a different perspective of analysis, have found empirical evidence that general tax management fees within the auditor-provided tax services are associated with lower effective tax rate (ETR). Notwithstanding, there were cases when tax management fees had no effect, i.e., the service is mainly for compliance (Ramzan, *et al.*, 2020), or the effect was even positive (expense and/or payments increase).

Kim and Im (2017) state that this is dependent on how engaged firms are as regards the CSR activities. Then, if CSR activities “deter tax avoidance, specifically in firms that are actively engaged”, they also found that, on the other hand, a “passive involvement in CSR does not have any influence on tax avoidance”. Then, and oppositely to beliefs of Jenkins and Newell (2013), these authors suggested that voluntary methods can “reduce corporate tax avoidance in firms, which is by encouraging them to engage in CSR activities. By encouraging social responsibility in firms, tax authorities can motivate firms to refrain from tax avoidance.”

More recently, using a legitimacy theory framework to examine how managers of companies who have been subject to specific criticism of their alleged tax avoidance respond to that, and based on content analysis from reports for the 11 year period 2004–2005 to 2014–2015, Holland, Lindop and Zainudin (2016) concluded differently that “governments cannot rely on managerial attitudes or voluntary frameworks if they wish to change the behaviour of managers in relation both to tax avoidance or to tax more widely”.

Tax, fair share, transparency, and tax avoidance issues have been increasingly debated during the recent years. Tax and Base Erosion and Profit Shifting (BEPS) are constantly on the agenda of the Group of Twenty (G20), OECD, the European Commission, non-governmental organisations (NGOs) and of the national governments, to name a few. The international and national effort against income tax avoidance and tax minimisation strategies employed by multinational corporations in the increasingly global world has grown into the important political issue and news topic nationally and globally.

The fruit of the joint effort is emerging: the European Commission has opened in-depth investigations to examine the corporate income tax payments of several multinationals and has recently declared illegal the arrangements in place for Starbucks (in the Netherlands) and Fiat (in Luxembourg) (European Commission, 2015a, 2015b); Apple case still to be decided (European Commission, 2014); Belgian excess profit regime has been also condemned with millions of euros to be paid back in tax by multinationals (European Commission, 2016). In the United States of America (US) the discussion of the international tax policy reform is on-going. The US authorities have been recently reported to be more harsh in the tax audits of the multinationals, including the recent 2015 Coca-Cola assessment (Bloomberg, 2015).

Tax paid by companies operating globally and their tax planning has been also a topic in Portugal (Pedro, 2013; Venâncio, 2012a, 2012b) on several occasions. In 2015, the Portuguese government adopted a plan to combat tax evasion, in which the international tax evasion is specifically noted (Governo de Portugal, 2015).

In this context, the need for transparency and social responsibility are the cornerstone topics within this global debate. The OECD through its Global Forum on Transparency and Exchange of Information created in the early 2000ties, the various national examples of mandatory disclosure of tax schemes and arrangements (the Portuguese Decree-Law no.º 29/2008 on mandatory disclosure of schemes targeted on obtaining tax advantages is an example of this global trend), the OECD BEPS project and the effort at the European Union (EU) level are all directed to improve the ability of governments and, in some cases, the society, to access information on taxpayers transactions and potential tax planning. However, it seems that currently the international effort directed to transparency has missed the financial and social aspect of transparency, which could to a certain extent be covered in the financial statements or CSR reports.

Transparency is directly related to disclosure. As far as transparency in financial statements is concerned, the existing most influential financial standards are International Financial Reporting Standards<sup>1</sup> (Rafay, Yasser & Khalid, 2019). Other important standards are US Statements of Financial Accounting Standards (SFASs), require certain disclosures while reporting for income taxes, which should provide the users of the financial statements with the most relevant and significant information regarding income tax obligations of an entity. It must be noted that the FASB Statement no. 109 (SFAS 109) and its interpretation FIN 48 “Accounting Uncertainty in Income Taxes” adopted in 2006, discussed in the Chapter 2 below, is viewed as a first step undertaken in the US to further increase transparency and information given to the users of financial statements on more sensitive information regarding income tax obligations, which could indicate on the degree of the corporate income tax aggressiveness of a given corporation. Tax aggressiveness, in its turn, is generally negatively viewed from the CSR standpoint.

Following the example of the US, the IFRS Interpretations Committee is currently discussing a Draft Interpretation “The Impact of uncertainty when an entity recognises and measures a current tax liability or asset” (IFRS, 2015). As of this date, the IASB Draft Interpretation has been already released (in October 2015) with numerous comments received and already available of the organisation’s website. The Draft Interpretation is discussed in due detail in the section devoted to the IFRSs below, but it does not impose any additional disclosure obligations and the potential effects of the adoption of the interpretation are discussed further.

There have been several other suggestions for improvements in disclosure on relevant corporate tax matters (namely, regarding tax strategies, facilitating understanding of the effective tax rate, statutory and effective rate reconciliation) by European Financial Reporting Advisory Group (EFRAG) and the United Kingdom Accounting Standards Board in their joint discussion paper “Improving the Financial Reporting of Income Tax” (EFRAG, 2011). The purpose of the discussion paper was to stimulate debate

on the issues presented and to assist the IASB in making progress with its income tax project, which, however, has been put on hold by the IASB in 2009.

In Portugal, although the financial statements of the Portuguese companies have come under the scrutiny of the NGOs (Fernandez, McGauran & Frederik, 2013) and the press (Pereira, 2012; Venâncio, 2012a) from the perspective of potential tax avoidance, no national academic discussion has arisen yet as regards their transparency in financial or CSR reporting.

In this context, it appears novel to undertake a comparative research of the existing and draft FASB, IASB and the Portuguese national mandatory standards and interpretations on information disclosure as regards income tax, focusing on the disclosure requirements that would be most important from the CSR and transparency perspective, or in other words, which could give the users of the financial information the necessary data to make a judgement on the CSR behaviour of a given company in terms of income tax responsibility. Such information could include, for example, effective income tax due or paid, prior year adjustments of income tax charge, reconciliation of the statutory and effective tax rates, reporting income tax geographically, disclosure of income tax contingencies, uncertainty in income tax and other aspects, which will be examined in the analysis of the referred financial standards.

Next, as far as CSR reporting is concerned, the academic research on whether corporate income tax is a subject for CSR reporting, on the payment of fair share of tax and tax avoidance as an irresponsible CSR activity is yet emerging (Dowling, 2013; Hoi, Wu, & Zhang, 2013; Preuss, 2012; Ylönen & Laine, 2014). As will be shown in the theoretical background, throughout the review of the financial standards referred to above and academic literature, the studies undertaken until now have indeed discussed the aspects of existence of the potential tax avoidance and empirical CSR reporting for income tax (Avi-Yonah, 2008; Dowling, 2013; Jenkins, J. G., & Sawyers, 2002; Preuss, 2012). However, possibly for the reason of income tax at this stage being still labelled as an “emerging” CSR matter, no general and comprehensive overview has been so far undertaken to ascertain whether any of the most influential CSR reporting standards published by the UN, GRI and OECD recognise and/or mention income tax as a social responsibility item in their recommendations for CSR reporting.

In this sense and considering the issues mentioned before, it would not be justified to require income tax to be a matter of CSR reporting if income tax is not an item noted in the recommendations of the most influential bodies issuing guidelines for CSR reporting worldwide. Therefore, first theoretical analysis of the existing CSR reporting guidelines (UN Global Compact, the GRI G4 Guidelines and the OECD Guidelines) is indispensable for the purposes of the topic chosen for this chapter.

Based on the topics previously mentioned, the main reasons for the choice of the topic may be summarised as follows:

1. First, corporate income tax payments, tax planning and tax avoidance is an issue that has been taken from national to international level. There are a lot of changes going on regarding increasing transparency and combatting BEPS at the G20, OECD, EU, and generally international level.
2. Second, income tax is increasingly becoming to be viewed as a CSR matter.
3. Third, perhaps considering that these developments are recent, the academic research has lagged in terms of linking income tax or CSR reporting and income tax payment as a CSR factor on a comprehensive basis.

These reasons provide compelling and sufficient background for conducting theoretical research in this field.

## REGULATORY FRAMEWORK AND LITERATURE REVIEW

The focus of this chapter is the regulatory and academic background on the issue of income taxes, including the perspective of this topic as a CSR matter.

In this context, this chapter first explores corporate tax disclosure requirements under the mandatory financial reporting standards of most relevance internationally and in Portugal: (i) disclosure of income tax related items under the IFRSs; (ii) SFASs issued by FASB; (iii) the Portuguese accounting standards *Normas Contabilísticas e de Relato Financeiro* (NCRFs).

After highlighting and comparing the relevant income tax disclosure requirements in the above-mentioned standards, the non-mandatory CSR reporting guidelines will be scrutinised to find relevant guidance for reporting on income taxes as on an aspect of CSR. Also here, the scope will be limited to the CSR reporting standards recognised and most used or referred to at the international and national level: (i) the UN Global Compact; (ii) the GRI G4 Guidelines; (iii) the OECD Guidelines.

Finally, the subject-matter of the third section of this chapter will be the national and international academic research.

### Corporate Tax Disclosures Under the Financial Reporting Standards

As stated above, this section will describe and will provide a brief comment on the requirements set for disclosure of corporate tax, tax strategy and some aspects related to uncertainties in tax matters. Considering their scope, IFRSs published by IASB represent one of the most influential financial reporting guidance on an international scale, including Portugal. Naturally, NCRFs, i.e. the Portuguese national standards, which are partially based on the IFRSs, are also discussed. Additionally, and taking into account its influence and the more recent work for convergence between the two standards bodies the IASB and the FASB, the standards and interpretations issued by the US FASB (SFASs) on these topics will be also analysed.

### Income Tax Disclosures Under IFRSs Disclosures Under IAS 12

It is generally accepted that tax effects, however they are calculated, should be presented separately from the items or transactions to which they relate (PriceWaterhouseCoopers, 2008). For this reason, most of disclosure requirements related to income tax under IFRSs are primarily found in IAS 12 *Accounting for Income Taxes*. Some general nature disclosures applicable to accounting and reporting, which may also impact income tax reporting and disclosure, are found in IAS 1 *Presentation of Financial Statements*. Furthermore, in June 2015, IFRS Foundation published the draft proposal for its interpretation *Impact of Uncertainty When an Entity Recognises and Measures a Current tax Liability or Asset* (IFRS, 2015). These rules are discussed in more detail below.

As regards IAS 12, it requires the disclosure of the main components of tax expense (or tax income) [IAS 12.79]. The purpose of the disclosures is to provide the information on the relationship between the entity's pre-tax accounting profits and related tax effects (MacKenzie *et al.*, 2011). It should be noted that this aspect is directly relevant for CSR, as it allows measuring the relationship between the profits reported (earned), if any, and the income tax contribution of a reporting entity.

IAS 12 [IAS 12.79 and 12.80] requires the following disclosures:



### ***Tax Disclosures in Financial and CSR Reporting as a Deterrence for Evasion***

1. current tax expense or income, together with recognised adjustments of prior periods.
2. amount of deferred tax expense (income) relating to: (i) the origination and reversal of temporary differences (ii) changes in tax rates or the imposition of new taxes.
3. amount of the benefit arising from a previously unrecognised tax loss, tax credit or temporary difference of a prior period.
4. write down and reversals of a deferred tax asset.
5. amount of tax expense (income) relating to changes in accounting policies and corrections of errors.

It is clear from the applicable standard that the tax expense related to profit or loss from ordinary business activities is presented on the face of the statement of profit and loss and other comprehensive income. It is required to be presented separately and, in this way, it is the first information available on income tax liability of the reporting entity. It will give information on the amount of the estimated income tax expense of the reporting entity, which would be used, by the users of the financial statements, as one of the references for further analysis from the CSR perspective.

Furthermore, disclosure of tax expense related to changes in accounting policies may directly or indirectly indicate the existence of tax planning, including aggressive tax planning, which is viewed negatively from the CSR standpoint (see under 2.2. *Corporate tax disclosures under social responsibility guidelines* below). For instance, the implementation of tax strategies for the use of deferred tax assets (such as loss refreshment), as demonstrated by the example of the impact of qualifying tax strategy on deferred asset realization (MacKenzie *et al.*, 2011) may be evidenced by unusual recognition of such assets from year to year and analysis of other items of financial statements.

Next, IAS 12.81 and IAS 12.82 deal with disclosure (and explanation) of items related to income taxes of more technical nature, namely:

1. aggregate current and deferred tax relating to items recognised directly in equity [IAS 12.81].
2. tax relating to each component of other comprehensive income [IAS 12.81].
3. explanation of the relationship between tax expense (income) and the tax that would be expected by applying the current tax rate to accounting profit or loss (presented either as a reconciliation of amounts of tax or a reconciliation of the rate of tax) [IAS 12.81];
4. changes in tax rates [IAS 12.81].
5. amounts and other details of deductible temporary differences, unused tax losses, and unused tax credits [IAS 12.81].
6. temporary differences associated with investments in subsidiaries, branches and associates, and interests in joint arrangements [IAS 12.81].
7. for each type of temporary difference and unused tax loss and credit, the amount of deferred tax assets or liabilities recognised in the statement of financial position and the amount of deferred tax income or expense recognised in profit or loss [IAS 12.81];
8. tax relating to discontinued operations [IAS 12.81].
9. tax consequences of dividends declared after the end of the reporting period [IAS 12.81].
10. information about the impacts of business combinations on an acquirer's deferred tax assets and recognition of deferred tax assets of an acquirer after the acquisition date [IAS 12.81].
11. details of deferred tax assets [IAS 12.82].
12. tax consequences of future dividend payments [IAS 12.82A].

## ***Tax Disclosures in Financial and CSR Reporting as a Deterrence for Evasion***

From the CSR perspective, another important disclosure requirement is the reconciliation between the statutory tax rate and the actual tax expense as listed under (c) above. The difference between tax expense and accounting profit or loss depends on a variety of factors, such as the existence of tax-exempt income (e.g. dividends or capital gains), of recognized expense not deductible for tax purposes, of tax use of previous losses, different rates of taxation if entity operates in more than one jurisdiction, etc.

Notwithstanding, the reconciliation would help the user of the financial statements “to understand whether the relationship between tax expense and accounting profit is unusual and to understand the significant factors that could affect that relationship in the future” (PriceWaterhouseCoopers, 2008). Consequently, it may allow for a certain explanation of why the income tax contribution is higher or lower compared to the accounting profit or loss, which may be useful for the assessment of CSR of the reporting entity.

The remaining disclosure items are of rather technical nature and requires a closer look to relate them to CSR. For example, the amount of deferred tax liabilities due to items recognized in equity (item (a) above) and details of the deferred tax assets (item (k) above) may indicate whether the reporting entity performs transactions and uses certain techniques that allow for a deferral of tax liabilities (Rafay & Ajmal, 2014).

Although a variety of different views exist on this subject, IAS 12 has been criticized. Specifically, it has been argued that despite requiring a range of disclosures “these tend to focus on accounting technicalities [...] rather than on aspects that are of real concern to users such as tax cash flows and implications for future tax cash flows” (EFRAG, 2011). EFRAG (2011) has identified “the following categories of tax information that could be relevant to investors and creditors:

1. Tax strategies and objectives.
2. Clarity on tax risk position.
3. Cash tax and future tax cash flows.
4. A clear explanation of the difference between the taxes paid and the charge made in the income statement.
5. A clear explanation as to why the current tax charge is not equivalent to the accounting profit at the statutory rate of tax (tax rate reconciliation).
6. Improved understanding of the effective tax rate.
7. A reasonable value of losses carried forward (or other deferred tax assets).”

It may be referred that currently reporting entities may cover all or some of the items listed by EFRAG. However, the users have pointed out to “struggle to use the information available”. IASB Exposure Draft ED/2009/2 Income Tax (paragraphs 40-49) (IASB, 2009) contained improved disclosure requirements, which could partially reflect the above items, but further discussion and adoption of the Draft was set aside for an indefinite period of time.

## **Disclosures Under Other IFRSs**

In addition to the disclosures required by IAS 12, some important general disclosures relating to income taxes are required by other standards.

For example, IAS 12 does not specifically require any disclosure of accounting policies in relation to current and deferred tax. However, IAS 1 *Presentation of Financial Statements* does oblige reporting

entities to disclose significant accounting policies relevant to understanding of the entity's financial statements [IAS 1.117]. IAS 1 gives certain freedom to choose which accounting policies should be disclosed and which should not, the basis for the decision (to disclose or not) being utility for the users of financial statements. The management of a reporting entity will exercise its judgement as regards the disclosures and the extent of the disclosures, except for mandatory disclosure items under the IFRSs (see the above analysis of IAS 12 requirements). Notwithstanding, the IFRSs mention that an entity subject to income taxation would be expected to disclose "its accounting policies for income taxes, including those applicable to deferred tax liabilities and assets" [IAS 1.120].

Furthermore, IAS 1 obliges an entity to disclose the judgements made by the management in the process of applying the entity's accounting policies and that have the most significant impact on the financial statements [IAS 1.121]. This rule equally relates also to judgements exercised in accounting for income taxes.

This leads us to another area relevant for income taxes, which is tax contingencies, governed by IAS 37 *Provisions, contingent liabilities, and contingent assets*. Any tax contingency should be properly reported in the financial statements and may be relevant for judgements regarding the CSR of an entity.

In this regard, the IAS 37 requires including reporting the provisions and contingent liabilities by classes [IAS 37.84 and IAS 37.86] and requires to report the brief description of the nature of the liability, the economic outflow and the uncertainties. Tax matters are not specifically set by IAS 37 as a class of provisions or contingent liabilities. Instead, IAS 37 gives certain freedom for division of such liabilities into classes, the criterion being the sufficient similarity in the nature of the items [IAS 37.86]. As an example, the standard explains that "it would not be appropriate to treat as a single class amounts relating to normal warranties and amounts that are subject to legal proceedings" [IAS 37.86].

As regards contingent tax assets, these are merely to be disclosed in the notes to the financial statements if an inflow of economic benefits is probable, avoiding misleading indications of a likelihood of the income arising [IAS 37.89-37.90].

Consequently, tax contingencies may or may not be classified as a class of provisions or contingent liabilities, and it is possible that the financial statements therefore do not provide this information, useful for the assessment of CSR of a firm. However, according to the author's view, if an income tax contingency met the materiality threshold, it would be appropriate to disclose it as a separate class of contingent liabilities, for instance. This information would be useful for the users of the financial statements and would be relevant for those who would like to know more about the CSR standards of the reporting entity, giving relevant information as regards to the reporting entity's tax compliance, tax aggressiveness and social responsibility as regards tax payments.

Finally, it should be noted that the draft International Financial Reporting Interpretations Committee's (IFRIC) Interpretation DI/2015/1 *Uncertainty over Income Tax Treatments* (the Draft IFRIC Interpretation) is being discussed by IASB and will provide guidance on the recognition and measurement of income taxes payable (recoverable) when there are uncertainties for income taxes (IFRS, 2015). The Draft IFRIC Interpretation was released in October, with the call for comments by 19 January 2016.

It appears that, despite for the time being IASB and FASB have abandoned plans for a joint convergence project for the topic of income taxes, this initiative seems to support the aims of bilateral convergence program between the two standard bodies as it covers the issues already dealt with by FASB interpretation FIN 48 under the US SFASs. As discussed further (see under 2.1.2.1. *Disclosures under ASC 740* below), the FIN 48 adopted in 2006 has been criticized for its complexity and excessive reporting burden, together with the prevailing research showing that the new reporting and disclosure

requirements introduced by the said interpretation had an effect of diminishing the aggressiveness as regards tax planning, and improving general tax compliance. These are naturally the factors directly relevant to CSR and income tax; disclosures that would be produced as a result of the adoption of the Draft IFRIC Interpretation might contribute to the information useful as regards assessing the level of the social responsibility of the reporting entity.

However, it should be noted that the Draft IFRIC Interpretation is rather different from FIN 48. In contrast to FIN 48, it does not require any additional disclosures to those that are required under the general rules for disclosure of significant judgements of management in the preparation of the financial statements under IAS 1.

More specifically, in the situation of uncertainty over tax treatment, the Draft IFRIC Interpretation, similarly to FIN 48, requires an entity to assume that the tax authorities would have the knowledge of all relevant information (§13 of the Draft IFRIC Interpretation). Next, the entity weights the probability of that the tax treatment being accepted by the tax authorities in such circumstances (§14 of the Draft IFRIC Interpretation). Depending on the probability test, the taxable profit or loss, the tax bases, unused tax losses and tax credits are determined and accounted for accordingly (§15-§16 of the Draft IFRIC Interpretation). Furthermore, if it is not probable that certain tax treatment is accepted, the entity may use the most likely amount method or the expected value method to reflect the uncertainty. Finally, as regards disclosure, the Draft IFRIC Interpretation refers to the general rule of IAS 1.122, which requires an entity to disclose the judgements of the management that have the most significant effect on the statements.

Thus, in contrast to FIN 48, the Draft IFRIC Interpretation merely provides clearer guidance on the issue of uncertainty in income taxes, without imposing new disclosure and compliance requirements. It appears also that, in many cases, and unlike under FIN 48, the uncertainty is reflected immediately and directly in the accounts related to current and deferred tax assets and liabilities, with no recourse to additional provisions.

Overall, it appears that the Draft IFRIC Interpretation may contribute to more clarity on the issue of reporting uncertain tax position but would not mean an overhaul in reporting for income taxes, as it was in the case when FIN 48 was introduced in the US and which might have led to the change in the tax policies of the US entities (see discussion in the following section below).

## **Income Tax Disclosures Under SFASs**

### **Disclosures Under ASC 740**

The SFAS 109 *Accounting for Income Taxes* was replaced by the FASB-released Accounting Standards Codification (ASC), the rules relevant to accounting for income taxes being codified under ASC 740 (FASB, 2011). General disclosure matters related to income taxes are dealt with by the standard ASC 740-10-50. For Income Statement related disclosures, the standard lists the following items as examples of the significant components [ASC 740-10-50-9]:

1. Current tax expense (or benefit).
2. Deferred tax expense (or benefit) (exclusive of the effects of other components listed below).
3. Investment tax credits.
4. Government grants (to the extent recognized as a reduction of income tax expense).
5. The benefits of operating loss carry forwards.

6. Tax expense that results from allocating certain tax benefits directly to contributed capital.
7. Adjustments of a deferred tax liability or asset for enacted changes in tax laws or rates or a change in the tax status of the entity.
8. Adjustments of the beginning-of-the-year balance of a valuation allowance because of a change in circumstances that causes a change in judgment about the readability of the related **deferred tax asset** in future years. For example, any acquisition-date income tax benefits or expenses recognized from changes in the acquirer's valuation allowance for its previously existing deferred tax assets because of a business combination [...].

Further, numerical reconciliation of the reported income tax expense and an expected amount based on statutory rates is required only for public entities (i.e. quoted or otherwise regulated, as defined), whereas IFRSs (specifically, IAS 12) always require numerical reconciliation, with no distinction. It is also important to notice that, under the SFASs, the effective tax rate reconciliation is presented using the statutory tax rate of the parent company, whereas the IFRSs additionally allow using the weighted average tax rate applicable to profits of the consolidated entities. The disclosure of significant reconciling items, however, is required under ASC 740-50-10 for both public and non-public entities.

There are additional total deferred tax asset and liability disclosure requirements in the balance sheet, alongside with the total valuation allowance recognized for deferred tax assets [ASC 740-10-50-2]. Finally, SFASs explicitly require a disclosure of policies on classification of interest and penalties and investment tax credit recognition [ASC 740-10-50-18/19].

Comparing the SFASs and IFRSs in terms of disclosure requirements, the first main components of disclosure (income tax expense, reconciliation, deferred tax entries on the balance-sheet) are rather similar. However, SFASs seem to require less technical disclosure and appear to be focused more on information useful to investors, such as disclosing the valuation allowance.

An important aspect presenting a major difference between SFASs and IFRS reporting remains the accounting and disclosures related to tax uncertainties, which became mandatory in the US with the adoption of FIN 48 in 2006, now codified in ASC 740-10-50. As mentioned above, IASB is currently working on the Draft IFRIC Interpretation to similar effect, the first draft of which has been already released and is discussed in the subsection devoted to IFRSs, under 2.1.1.2. *Disclosures under other IFRSs* above.

In the US, the FIN 48 has been referred as an interpretation “universally reviled by client management, financial statement preparers and auditors” (Bragg, Epstein & Nach, 2009). It requires to identify and measure the uncertain tax positions. In brief, the reporting entity must examine if a certain tax position can be sustained. A tax benefit cannot be recorded and an adjustment must be made, including applicable penalties, if, assuming all the relevant information and facts are known to the tax authorities, it is “more-likely-than-not” (i.e., more 50% threshold [ASC 740-10-50-5]) that the position is not sustained in the tax examination.

In this regard, a FAS reporting entity is required to disclose [ASC 740-10-50-15]:

1. the accounting policy classification of interest and penalties.
2. a roll-forward of all unrecognized tax benefits presented as a reconciliation of the beginning and ending balances of the unrecognized tax benefits on a worldwide basis.
3. the amount of unrecognized tax benefits that, if recognized, would affect the effective tax rate.

### ***Tax Disclosures in Financial and CSR Reporting as a Deterrence for Evasion***

4. the amount of interest and penalties that have arisen during the year and are cumulatively accrued on the balance sheet.
5. a discussion of reasonably possible changes to the balance of unrecognized tax benefits that could occur within 12 months after the reporting date.

These disclosures would certainly give the users additional information on the tax aggressiveness of the reporting entity as far as income tax positions are concerned, including easier access to information from the tax authorities side. The disclosures could provide information useful to evaluate a firm's CSR behaviour, which would be demonstrated by the size of the reserves created for unrecognized tax benefits and the amount of penalties related to tax. IFRSs in its current version do not require disclosure of such information and it is doubtful that information on penalties, being sensitive information that may impact firm's reputation, would be voluntarily disclosed by firms following IFRSs for financial reporting.

There is a research (discussed in more detail further in section 2.3. *Literature review*) finding that FIN 48 likely increased larger companies' tax burdens, reducing the appeal of more aggressive tax minimization strategies (Tomohara, Lee, & Lee, 2012). It is confirmed by a later research finding that the state income tax burden reported increased, linked to the adoption of FIN 48 (Gupta, Mills, & Towery, 2014). Another research on FIN 48 and tax compliance finds that, first, some taxpayers are more likely to be audited or, second, deterred from transactions generating uncertain tax benefits just because of implementing FIN 48 (Mills, Robinson, & Sansing, 2010). The research available demonstrates that the disclosure requirements increase the responsibility regarding income tax compliance, reporting and payment, and change the tax compliance behaviour of the reporting entities in the US.

### **Disclosures Under Other SFASs**

As with IFRSs, SFASs include the standard FAS 5 *Accounting for Contingencies*, now codified in ASC 450 *Contingencies*, equivalent to IAS 37 *Provisions, Contingent Liabilities and Contingent Assets*, which is relevant for accounting for income tax contingencies as well. Not going into the study of differences between the two standards, as it is not the purpose of this chapter, the US standard also requires the disclosure of the nature of the accrual for contingency and disclosure of an estimate of a possible loss.

As regards accounted income tax liability, the risks and uncertainties related to income taxes, these are governed in the US by the SFAS rules on uncertain tax positions discussed in detail in the previous section. In addition, ASC 275 *Risks and Uncertainties* requires to disclose risks and uncertainties that could significantly affect the amounts reported in the financial statements in the near term [ASC 275-10-05-02]. Thus, ASC 275 *Risks and Uncertainties* and ASC 450 *Contingencies* require to disclose, provided there could reasonably be a change in the estimate of tax liability for unrecognized income tax benefits within one year from the reporting date, the nature of uncertainty and potential events triggering the change, as well as the estimates of the change (Bragg, Epstein & Nach, 2009).

Other contingencies are to be reported under the general framework. Whether an accrual is recorded or not, the US standards require to disclose the nature of the accrual, and, in some circumstances the amount accrued, or an estimate of possible loss for non-recordable accruals (PriceWaterhouseCoopers, 2014).

## Portuguese NCRFs

Before examination of the contents of the Portuguese NCRFs, it should be noted that the Portuguese standards adopted in 2008 have been recently amended, with effect from 1 January 2016 (Secretário do Estado dos Assuntos Fiscais, n.d.). The amendments were adopted to implement the new European rules further harmonising accounting regulations in EU Member States, whose primary aim was simplification and reduction of the administrative burden related to financial reporting by small and medium-sized enterprises. For simplification purposes, virtually most of the more detailed disclosure requirements that are currently incorporated into each separate NCRF were deleted from the texts of the standards and transferred into the new Annex 6 to the Models of Financial Statements (Ministério das Finanças, 2015). At the same time, in some cases, the volume of mandatory disclosures appears to be slightly reduced by the amendments in comparison to the disclosures required by the previous version of NCRFs. Below, the current NCRFs will be discussed together with the impact of the amendments applicable from 1 January 2016.

### Disclosures Under NCRF 25

The Portuguese standards applicable as from 1 January 2016 deal with income tax matters related to income taxes in NCRF 25 *Income Taxes* in paragraphs 72-84, which, similarly to most NCRF standards, are largely based on the IAS 12 (Rodrigues, 2012) before the last amendments of the latter standard in 2008 (effective 2009). In contrast to IAS 12 *Income Taxes*, it has been stated that NCRF 25, as in force before 1 January 2016, required mandatory disclosure of all elements of the tax expense recognised as major components of such expense in IAS 12.80 [NCRF 25.72] (Morais & Lourenço, 2013).

The amended Portuguese disclosure requirements regarding income taxes effective 1 January 2016 are set out in point 27 *Income Taxes* of the Annex to the models of financial statements (i.e. Annex 6). The wording of the rules has not changed so it may be suggested that the disclosure items listed continue to remain mandatory.

It should be further noted that the new disclosure requirements are virtually the same, except for the following differences:

- the current Portuguese standard, similarly, to its previous version in force before 1 January 2016, omits the disclosure of the effects of business combinations on tax expense, required under IAS 12.81(j)-(k).
- the amendments in effect from 1 January 2016 eliminated the disclosure of tax expense related to discontinued operations, corresponding to IAS 12.81(h) and the previous NCRF 25.74(g).
- the reference to the [numerically expressed] amounts of the potential income tax consequences of payment of dividends to shareholders, corresponding to the second sentences of IAS 12.82A and previous NCRF 25.76 was equally eliminated.

Henceforth, it may be concluded that IAS 12 and NCRF 25 disclosure elements are almost identical, except for the differences noted above. These differences might not be important for accessing CSR related to income tax payments in all cases. However, the recognition of deferred income tax assets because of business combinations, which does not have to be disclosed under the Portuguese NCRFs, may indicate on potential existence of tax planning, including aggressive tax planning. Overall, however,

the comment regarding the importance of the reporting of the major tax expense elements under IAS 12 as well as the critiques expressed regarding the IAS 12 standard (see under 2.1.1.1. *Disclosures under IAS 12* above) apply equally here.

## **Disclosures Under Other Portuguese Standards**

The relevant disclosure requirements of NCRF 1 *Structure and Contents of Financial Statements* and of NCRF 21 *Provisions, Contingent Assets and Contingent Liabilities* are almost identical to the corresponding rules of the IFRSs, with several minor differences.

Similarly to IAS 1, NCRF 1 also obliges an entity to disclose the judgments made by the management in the process of applying the entity's accounting policies that have the most significant impact on the financial statements [NCRF 1.47 and 1.48 current and amended versions].

Additionally, NCRF 21 likewise requires the division of provisions into classes and presenting respective amounts accounted for each class of provisions [NCRF 21.81 in current version corresponding to point 23.1 of the Annex 6 to the Models of the Financial Statements]. In contrast to IFRSs, however, NCRFs (after 1 January 2016, the new Annex 6) do not require any further information revealing the nature of the obligation and other details about each class of provision, as required by IAS 37.85. The disclosure requirements in the IFRSs and NCRFs (Annex 6) are coincident regarding the contingent assets and liabilities.

Logically, as NCRF 21 does not require details on the classes of provisions, apart from numerical information, it allows not disclosing contingencies in the circumstances in which it is not appropriate [NCRF 21.86]. The Portuguese standard does not explain in which cases the disclosure is deemed inappropriate, leaving this to the full consideration of the reporting entity. In this way, unlike IAS 37 in this regard [IAS 37.92], NCRFs give much more opportunities for non-disclosure: IAS 37 allows not disclosing the details of the provisions or contingencies only in extremely rare cases, in which a disclosure would be to the prejudice of the reporting entity.

Overall, it would be appropriate to note that as far as provisions and contingencies for tax matters are concerned, the Portuguese standard requires less disclosure as compared to the IFRSs, allowing the information relating to provisions and contingencies related to tax not to be disclosed clearly in the financial statements. This leads to a conclusion that the users of financial statements looking for information on tax contingencies may not find the essential information sought.

## **Corporate Tax Disclosures Under Social Responsibility Guidelines**

Although it may still be debated whether corporate tax is or is not a social responsibility item, it appears useful to research whether the existing CSR guidelines touch upon corporate taxation matters, and if so, then to which extent. Hence, the description and analysis will highlight the existing relevant guidelines, if any, in the UN, GRI and OECD issued guidelines for CRS reporting.

### **UN Global Compact**

The Ten Principles of the UN Global Compact do not deal with tax issues directly (UN Global Compact, 2014). Furthermore, the “Business for the Rule of Law Framework” developed to assist businesses to “support the rule of law and build lives of dignity for all” (UN Global Compact, 2015:4) does not ad-



dress any specific legal areas apart of the areas covered by the Ten Principles, which do not include any tax matters. Finally, the search in the on-line library of the UN Global Compact by “tax” keyword produced no hits.

Consequently, tax is not on the agenda of the UN Global Compact directly, the primary role being given to human rights and basic respect for environment, state, and legal order. This can be explained by the focus of the UN Global Compact on the matters of primary concern, such as basic human rights, tax being the secondary issue fitting secondarily into the general sphere of action of the UN Global Compact. Thus, the UN Global Compact standards will not be referred to or discussed further.

## GRI

In 2013, GRI launched the fourth generation of its sustainability reporting guidelines “GRI G4 Sustainability Guidelines” (GRI G4 Guidelines), to apply to sustainability reports published after 31 December 2015 (GRI, 2013a). The GRI G4 Guidelines organize sustainability reporting in three main categories of economic, environmental, and social aspects. These categories are divided into material topics, or “Aspects”.

Similarly, to the UN Global Compact, taxation specifically and directly is reflected in none of the GRI G4 Guidelines’ material aspects. However, the GRI G4 Guidelines link to the other international standards, such as the mentioned UN Global Compact’s Ten Principles and the OECD Guidelines. Taking into account that Chapter XI of the OECD Guidelines is explicitly dedicated to taxation (see the discussion below), in explaining the link between both standards, the GRI G4 Guidelines state that taxation is dealt with by the Economic Performance Aspect and by the Anti-Competitive Behaviour and Compliance Aspects under the Society sub-category.

For the Economic Performance Aspect, the relevant GRI G4 Guidelines standard is G4-EC1 standard on “Direct Economic Value Generated and Distributed”. It requires to report the basic components of the organization’s global operations and lists payments to government, by country, as one of the reportable components. The GRI G4 Guidelines Implementation Manual further explains that the report should state that “all organization taxes (such as corporate, income, property) and related penalties paid at the international, national, and local levels”, stressing that “for organizations operating in more than one country, report taxes paid by country” (GRI, 2013b).

For the Compliance Aspect, the focus of GRI G4 Guidelines in the relevant G4-EN29 standard are monetary and non-monetary sanctions for non-compliance. Not addressing taxation separately, this standard requires to report the total amount of significant fines and several non-monetary sanctions. As this normally presents a sensitive area that organisations would be reluctant to disclose in any further details, the G4-EN29 standard does not present any value for sustainability reporting as regards tax compliance.

Thus, in respect of taxation as a CSR matter, the GRI G4 Guidelines not only recognise it as such, but also link to the financial reporting disclosure requirements reviewed previously (namely, those issued by IASB, FASB and CNC), in what concerns reporting of tax expense geographically, as the possibility of such reporting provided in all the financial reporting standards, but is mandatory under neither of those. Sanctions may also be reported in financial reports; however, it is the mandatory reporting item only in the US under FIN 48.

## **OECD Guidelines for Multinational Enterprises**

The OECD Guidelines for Multinational Enterprises (OECD Guidelines) were first published in 1976 for promoting appropriate business conduct by companies, which operate in different jurisdictions and face a variety of cultural, legal, and regulatory environments (OECD, 1976). The very first original version of the OECD Guidelines already contained a two-paragraph section on taxation, stating that the enterprises should provide the required information to the tax authorities and refrain from abusive transfer pricing practices (OECD, 1976).

The latest version of the OECD Guidelines and its commentary include a slightly more extensive chapter XI on taxation (OECD, 2011). It requests the multinational enterprises to:

- contribute to the public finances by making timely tax payments.
- comply with both the letter and spirit of the tax laws.
- ensure tax compliance by providing information required for tax determination and by complying with the arm's length principle.
- place tax governance and tax compliance as a part of general risk management and as a board item.

The Commentary calls on co-operation with the tax authorities, transparency in tax matters and recognizes the existence of major financial, regulatory and reputation risk for an enterprise in tax matters. The Commentary elaborates extensively (in four paragraphs out of seven paragraphs of the commentary in total) on the necessity to comply with the OECD Transfer Pricing Guidelines for Multinational Enterprises and Tax Administrations.

The OECD Guidelines is the only instrument on CSR focusing extensively on tax matters and recognizing tax as being important aspect of CSR. This may be explained by the fact that tax is one of the main areas of the OECD's work. OECD has launched and has been promoting various projects aiming on making sure that the "fair share" of tax revenues are received by the governments, and is working on raising awareness of the necessity of fair contributions by the multinational corporations at the highest levels. The main streams of work in this area is the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes operating since 2000, the work on Base Erosion and Profit Shifting project endorsed by G20 member countries in July 2013 and in progress from then on, as well as work on the developing of legal basis for international co-operation and exchange of information in tax matters.

## **LITERATURE REVIEW**

The academic and accounting literature linking the financial reporting disclosures of corporate tax and CSR has been emerging in the past years. Within the recent years, the scandals about the widespread use of tax planning schemes resulting in payment of disproportionately low corporate taxes by multinational corporations like Amazon, Google and Starbucks, have gained worldwide dimension and are raising awareness of the issue, resulting in academic studies and research on the issue. According to Jenkins and Newell (2013), "the issue of corporate responsibility towards taxation has moved to centre stage" and "it is likely to become an increasingly important item on the CSR agenda in the foreseeable future".

It should be noted that tax avoidance has been always a topic for academic discussion mostly among tax law specialists, even though without establishing a relationship between this matter and the CSR or the financial reporting. This literature is not the focus of the present research and thus will not be reviewed here, except for the Portuguese academic literature on this subject.

The existing academic literature may be divided into two blocks and will be organized in the following way:

- firstly, the review will start with international academic literature, which aims to explore the link between taxation and CSR, backed by empirical studies and specially focused on studies covering US firms and FIN 48;
- finally, the second part will focus on Portuguese literature relevant for the subject-matter of this work.

## **An International Perspective**

The views on taxation as a CSR matter put forward in the academic literature may diverge, but there is a predominant trend of considering taxation as being an item for CSR rather than excluding it from responsibility framework.

As far as purely theoretical studies are concerned, Avi-Yonah (2008) discusses the three main theoretical views of the corporation and concludes that tax minimization strategies are unacceptable under any of these theories discussed. Dowling (2013) equally examines the “fair share of tax” issue as a matter of CSR from business ethics standpoint and scrutinises it under stakeholder group theories, concluding that taxation is a boundary condition for CSR. He notes that businesses have resisted the discussion of taxation as a moral issue and that the complexity of tax regulations and modern accounting rules, together with global scale of operations make it almost impossible for a member of general public to understand whether a company pays its fair share of tax.

Christensen and Murphy (2004) argue that “taxes are the lifeblood of the social contract, vital to the development and maintenance of physical infrastructure and to the sustenance of the infrastructure of justice that underpins liberty and the market economy. Besides that, these authors advocate reaching an intergovernmental agreement at a global level to define minimum standards of transparency and disclosure by companies, in which IASB is given one of the leading roles.

Preuss (2012) discusses the issue of CSR of companies domiciled in tax havens, namely Bermuda and Cayman Islands. The author rejects the utilitarian perspective of considering tax haven companies as wealth generators for their shareholders or tax haven governments, undoubtedly placing taxation as the CSR category. The study argues that, although offshore-headquartered companies cannot isolate themselves completely from the global CSR awareness, incorporation off-shore suppresses one important aspect of its responsibilities to society (i.e., taxation) and shows that the CSR of such companies is mostly mere window-dressing.

Finally, Zhang (2010) approaches tax and CSR from the tax policy and Marxist ideology standpoints, advocating for introduction of tax incentives in China to stimulate socially responsible corporate activities, such as public welfare donations, environmental protection and employment.

US was the first country which formally linked financial reporting and uncertainties in tax position, by means of adoption of FIN 48 by FASB and introducing mandatory disclosure requirements, as discussed in the section describing SFASs under 2.1.2.1. *Disclosures under ASC 740 above*. Since then,

research has been emerging in the US as regards the impact of FIN 48 and tax behaviour and disclosures of multinational corporations. The research in the US has relevance and will be briefly reviewed here.

Thus, before adoption of FIN 48, Jenkins and Sawyers concluded that tax shelters are unlikely to be disclosed unless they result in a material contingent liability (Jenkins & Sawyers, 2002). Hope, Ma & Thomas (2013) tested the relation between corporate tax avoidance and disclosure of geographical earnings by US firms. These authors find that firms opting not to disclose geographical earnings in their financial reports have lower effective tax rates, in line with the perception that non-disclosure of geographical earnings helps masking tax avoidance.

The empirical research made by Mills, Robinson and Sansing (2010) investigates how FIN 48 changed the strategic interaction between the corporations and the government. Their research shows that taxpayers with stronger positions obtain higher expected payoffs post-FIN 48. Also, the research finds that liability disclosed under FIN-48 can be overstated or understated relative to the expected cash payment. Those authors additionally conclude that some taxpayers are more likely to be audited because of the disclosures or they are deterred from taking more aggressive tax positions because of FIN 48.

Another research finds that implementation of FIN 48 possibly increased larger companies' tax burdens, due to the prohibition of recording any tax benefit which does not pass "more-likely-than-not" test (Tomohara *et al.*, 2012). In line with Mills *et al.*, this research concludes that FIN 48 appears to have reduced the appeal of more aggressive tax minimization strategies (*ibid.*:4239). McKinley and Owsley (2013) assert that inter-group transfer pricing often falls into the category of uncertain tax positions and is likely to increase the tax charge as well as lower the valuation allowance under FIN 48. Finally, the study of Lisowsky, Robinson and Schmidt (2013) link public disclosures of tax reserves with mandatory private disclosures of tax shelter participation as made to the Internal Revenue Service. The authors find strong evidence that the tax reserve is positively associated with tax shelters, accounting 48% of its value to the benefits of tax shelters, while other commonly used measures of tax avoidance are not valid.

The reviewed research on FIN 48 implementation effects does not directly link the findings to the CSR. Indeed, as noted by a number of authors (Dowling, 2013; Fisher, 2014; Jenkins & Newell, 2013), taxation is hardly mentioned in CSR reports and tax avoidance is rarely discussed in the context of CSR. Notwithstanding, the academic research on this subject is emerging at a considerable pace, which may be caused, for instance, by the tax avoidance scandals of the recent years, discussed globally, the increasing public awareness and the work of G20 and OECD on tax transparency, tax competition and combating BEPS (OECD, 2013).

The existing research combining theoretical and empirical discussion examines various aspects of taxation and CSR. Lanis and Richardson (2012), by adopting a wider view of corporation and considering a larger range of stakeholders beyond management and shareholders, put taxes into the CSR framework, arguing that tax aggressiveness is socially irresponsible. In the empirical part of their research, the authors examine the relationship between CSR and tax aggressiveness in Australia. The authors demonstrate that the higher the level of CSR disclosure, the lower the tax aggressiveness, and their further analysis additionally shows that existence of social investment commitment and corporate and social responsibility strategy reduce tax aggressiveness. Laguir, Staglianò and Elbaz (2015) examine how the CSR dimension influences corporate tax aggressiveness of the French quoted firms. In line with previous research, the authors conclude that the higher level of the social dimension of the CSR, the lower the tax aggressiveness. Hoi, Wu and Zhang adopt a broader perspective to evaluate CSR activities and examine association between CSR and tax avoidance, additionally using FIN 48 as a natural quasi-experiment to further explore this link (Hoi *et al.*, 2013). More specifically, partially relating to empirical research

methods used by Lanis and Richardson (2012), the research conducted by these authors collectively suggests that firms with excessive irresponsible CSR activities are more aggressive in avoiding taxes.

Ylönen & Laine (2014) also argue that corporate tax payment is an issue of CSR and explore transfer pricing strategy of a Finnish corporation as the case for implementing aggressive tax minimization strategies but not disclosing tax matters in its numerous corporate responsibility publications. Huseynov and Klamm (2012) explore the relationship between auditor-provided tax services and the impact of CSR. They conclude that tax fees are always associated with lower effective tax rate (i.e., percentage of income tax charge in relation to pre-tax earnings). However, the relationship between fees paid for auditor-provided tax services and tax avoidance is affected by levels of CSR, tax fees associated with higher effective tax rate for firms with stronger CSR.

Finally, there are qualitative studies that may be used for the discussion of links between CSR as risk management tool: Hardeck and Hertl (2013) investigate the effects of media reports on aggressive and responsible tax strategies on corporate consumer success, Desai and Dharmapala (2004, 2008) investigate the links between corporate tax avoidance and corporate governance, Kenyon (2008) surveys tax avoidance practices in Brazil and Lenter, Slemrod and Shackelford (2003) discuss the pros and cons of public disclosure of corporate tax return information, as a means to increase transparency and accountability.

## **A National Perspective**

Portuguese academic literature about taxation and CSR is virtually inexistent. It appears that more attention has been paid to the subject of tax avoidance and evasion, which has been discussed mainly by the Portuguese tax law academia and economists, and to the CSR reporting in general terms, but not to the link between income taxation and CSR. There are also studies on reporting for income taxes in Portugal. These studies, similarly, to the literature available on CSR, do not link the conclusions to CSR.

As regards the duty to pay taxes and tax avoidance problem, Sanches (2006) in his monograph discusses the legal aspects of tax planning. Several conferences resulted in publication of collection of the conference reports and articles, such as the Conference on the Enterprise Restructuring and the Boundaries of Tax Planning held in Lisbon in 2008 (Sanches, Câmara, & Gama, 2009) and Accounting and Taxation Conference organised by ISCAP in Oporto, in the Special Topic of Tax Planning and Avoidance in 2009 (Amorim, 2010). Borrego and Lopes (2013) make a review of literature on tax non-compliance in an international perspective.

As regards discussion of taxation in a more sociological perspective, Nabais (1998) in the publication of his doctoral thesis discusses the fundamental duty to pay tax, rejecting the existence of the right not to pay taxes and asserting that the modern state is a fiscal state (*estado fiscal*). Carvalho (2010) elaborates on social solidarity in taxation, discussing the balance between excessive and just amount taxation and their effects. Pires (2011) reflects upon the issues of ethics and taxation, stating that in the contemporary society, taxation rests on the idea of solidarity, which appeals to equality in what is contributed to and received from the community. Poço, Lopes and Silva (2015) investigate the sociological aspects of tax evasion in Portugal.

Finally, Catarino and Monteiro (2013) study the tax treatment of environmental provisions, focusing on technical aspects and surveying the PSI 20 practice, with no discussion of CSR issues.

Next, as far as the academic research on CSR is concerned, most of the studies on the topic of CSR have been conducted within the institutions of higher education and research, even though not necessarily related to accounting for income taxes and associated matters.

Fernandes, Monte and Afonso (2013) analyse the CSR of the Euronext PSI 20 entities between 2005 and 2009 and construct the CSR index, based on the total of 239 CSR items. These authors find that most of the Portuguese PSI 20 entities show medium performance about CSR, with EDP – Energias de Portugal, S.A. leading the high-performance cluster. Also, the human rights dimension was found to be the most important for the Portuguese companies in terms of CSR (ibid.).

Next, Domingos (2010) examines the general evolution of sustainability reporting by companies quoted on Euronext Lisbon between 2006 and 2008, Carvalho (2008) studies the influence of GRI standards on CSR reporting by quoted Euronext Lisbon companies in 2006, whereas Silva (2014) concludes that CSR reporting has reduced dimensions in Portugal, and is restricted mainly to environmental and social indicators. Lopes (2015) notes general significant progress of voluntary disclosures related to CSR in Portugal, in line with Pinto (2014) who proves that Portuguese companies have been increasing investment into ethics and social responsibility, the largest enterprises being the largest investors. Roque (2012) conducts a research into environmental accounting and its impact and practices in Portugal.

As regards reporting for income taxes in Portugal, a number of authors study accounting and disclosure related to deferred taxes in Portugal by listed and unlisted companies, the interrelations between the size of companies and styles of reporting, and draw various conclusions about the existing practices in reporting for deferred taxes in Portugal (Aracchande, 2010; Ferreira, 2014; Fonseca, 2011; Lopes, 2014; Pereira, 2013). Lopes (2014) constructs an information compliance index for IAS 12 and studies the relation of the index to performance and control indicators, whereas Silva (2013) repeats and further develops the study by studying each type of disclosure requirement and its disclosure, as well as links compliance to other factors (Lopes, 2014).

## **CONCLUSION**

This section presents, in a concise form, the main conclusions based on the review of the financial standards and CSR guidelines.

All the most influential financial standards reviewed, namely IAS 12 on accounting for income tax, IAS 1 on presentation of financial statements and IAS 37 on provisions and contingencies, FAS 109 on income tax, FAS 5 on contingencies and FIN 48 on tax uncertainties, as well as the Portuguese NCRF 25 on income tax, NCRF 1 on presentation of financial statements and NCRF 21 on provisions and contingencies require mandatory disclosure of certain information related to corporate income tax. Specifically, all the standards require disclosure of the current and deferred tax expense, which are potentially the first main points that the users of the financial information would pay their attention if looking for the tax information from the CSR standpoint. Also, the standards require the disclosure of uncertainties, which would include disclosure of provisions or contingencies as regards potential uncertainties related to tax payments.

Although all the standards, along with annual tax charge disclosure, require the tax charge reconciliation with statutory corporate income tax rate as a numerical or percentage reconciliation, none makes percentage reconciliation mandatory, making the assessment of tax charge less transparent. Furthermore, the degree of detail as regards explaining the differences between the actual tax charge and the statutory rate is not defined, giving the companies an opportunity not to expose the more sensitive data and thereby making the essential information unavailable for those users of financial information, who seek to assess the CSR of the companies in tax field. Also, the geographical earnings and consequently geographical

tax charge disclosure is not mandatory, making the information how much corporate tax has been paid in each particular jurisdiction of operation (and useful to assess CSR tax behaviour) often unavailable based on the financial statements.

It should be noted, however, the US SFAS (more specifically, FIN 48) require to report uncertain tax positions, the information that is certainly interesting to evaluate the company's behaviour as far as tax payments and aggressiveness in application of tax rules are concerned. In relation to FIN 48, the existing research provides evidence that tax aggressiveness of the US entities has diminished after the introduction of mandatory reporting of uncertain tax positions. As for the IASB issued standards, there is a draft IFRIC Interpretation on the matter. The Draft IFRIC Interpretation is designed to deal with tax uncertainties. However, in contrast to its US counterpart, the Draft IFRIC Interpretation in its current version does not impose any additional reporting and disclosure but is designed to merely provide clarification to existing rules of IAS 12 and IAS 37. If this is not changed, the effects of its adoption, in the author's view, would be different compared to the introduction of FIN 48, which had been reported to have a big impact on the reporting practices of the US companies. Here, it should be noted that the Portuguese NFRCs remain silent on the topic, save for the general requirement to disclose contingencies.

Among the CSR standards analysed, namely the GRI G4 Guidelines, the UN Global Compact and the OECD Guidelines, only the latter directly addresses taxation as CSR matter extensively, stressing tax compliance behaviour and placing tax topic on the table of the board. The GRI G4 Guidelines nevertheless recognise payments to government as a reportable item, recommending reporting the amounts of tax payment to each government (geographically) as well as separately the number of fines and penalties related to tax. In this way, the GRI 4 Guidelines contain the recommendation, which could provide for the main information on tax as CSR-related subject and certainly remedy the absence of mandatory recognition geographical of tax expense in the financial statements.

The academic literature on tax as a CSR matter is emerging, with the authors accepting that tax is a matter of CSR. A significant body of research has developed as regards the US FIN 48 rules, demonstrating various aspects of its impact and the change in the tax behaviour of US corporations. International research provides evidence that more socially responsible firms are less tax aggressive, whereas, to the author's knowledge, no similar research has yet been conducted in Portugal. The Portuguese academic literature and research has focussed mainly on the issues of tax, tax avoidance, tax reporting and CSR reporting separately.

## **FUTURE RESEARCH DIRECTIONS**

This research is about the issue of income taxes from the perspective of CSR, outlining the financial and CSR reporting rules apply as well as providing the insight into the existing available research on the subject. It may be also applied with the purpose of identifying any differences in tax-related CSR reporting as well as ETR for entities operating in different sectors of a broader sample of the Portuguese non-financial corporations' sector. Furthermore, future researches may be further developed by focusing on the matter of reporting for income taxes solely in the CSR reports or by examining the more narrowly selected CSR-related reporting items in financial and CSR reports of the entities or constructing the weighted indices, which would particularly emphasize the CSR-related income tax reporting elements. Finally, another separate topic for further research could be geographical reporting of income tax expense and its relationship with the ETR and other independent variables as well as CSR reporting.

## DISCLAIMER

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication;
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter;
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

- Amorim, J. C. (Ed.). (2010). *Planeamento e Evasão Fiscal - Jornadas de Contabilidade e Fiscalidade*. Vida Económica.
- Aracchande, V. (2010). *O impacto dos impostos diferidos nas demonstrações financeiras das empresas não financeiras incluídas no PSI 20: ano de 2009*. ISCAL. Retrieved from <http://hdl.handle.net/10400.21/3419>
- Avi-Yonah, R. S. (2008). Corporate Social Responsibility and Strategic tax Behaviour. In P. D. W. Schoen (Ed.), *Tax and Corporate Governance* (pp. 183–198). Springer. doi:10.1007/978-3-540-77276-7\_13
- Bloomberg. (2015). *Coca-Cola Fights \$9.4 Billion Transfer Pricing Adjustment*. Retrieved April 11, 2016, from <http://www.bna.com/cocacola-fights-94-n57982065115/>
- Borrego, A. C., & Lopes, C. M. da M. (2013). Tax Noncompliance in an International Perspective: a Literature Review. *Contabilidade E Gestão*, (14), 9–43
- Bragg, S. M., Epstein, B. J., & Nach, R. (2009). Income Taxes. In *Wiley GAAP 2010. Interpretation and Application of Generally Accepted Accounting Principles* (pp. 875–952). John Wiley & Sons, Inc.
- Carvalho, C. (2010). A “Solidariedade Social” na Tributação: Realização da Justiça ou Ineficiência Económica? *Revista de Finanças Públicas E Direito Fiscal*, 3(2), 79–103
- Catarino, J. R., & Monteiro, M. B. (2013). Fiscalidade ambiental - Um estudo sobre a relevância das provisões ambientais nas empresas do PSI 20. *Revista de Finanças Públicas E Direito Fiscal*, 6(3), 153–176.
- Christensen, J., & Murphy, R. (2004). The Social Irresponsibility of Corporate Tax Avoidance: Taking CSR to the bottom line. *Development*, 47(3), 37–44. doi:10.1057/palgrave.development.1100066



da Silva, M. D. C. (2013). *A problemática dos impostos diferidos: grau de harmonização, nível de divulgação e seus determinantes*. Escola Superior de Gestão e Tecnologia de Santarém. Retrieved from [https://repositorio.ipsantarem.pt/bitstream/10400.15/876/6/MarisaSilva\\_MestradoCF\\_2013.pdf](https://repositorio.ipsantarem.pt/bitstream/10400.15/876/6/MarisaSilva_MestradoCF_2013.pdf)

de Carvalho, F. P. M. (2008). *A divulgação voluntária de informação: A influência da adopção da estrutura da Global Reporting Initiative nas empresas da Euronext Lisboa*. Universidade Autónoma de Lisboa.

Desai, M. A., & Dharmapala, D. (2004). *Corporate Tax Avoidance and High Powered Incentives*. *Journal of Financial Economics*. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0304405X05001364>

Desai, M. A., & Dharmapala, D. (2008). Tax and Corporate Governance: An Economic Approach. In W. Schoen (Ed.), *Tax and Corporate Governance* (Vol. 3, pp. 13–30). Springer - Verlag Berlin Heidelberg. doi:10.1007/978-3-540-77276-7\_3

Domingos, R. M. D. (2010). *A evolução da divulgação voluntária de informação nas empresas cotadas da Euronext Lisboa do ano 2006 a 2008*. ISCAL.

Dowling, G. R. (2013). The Curious Case of Corporate Tax Avoidance: Is it Socially Irresponsible? *Journal of Business Ethics*, 1–12. doi:10.1007/10551-013-1862-4

EFRAG. (2011). *Discussion Paper*. European Financial Reporting Advisory Group (EFRAG). Retrieved from [http://www.efrag.org/files/ProjectDocuments/Proactive - Income Taxes/120127\\_Income\\_tax\\_DP\\_final.pdf](http://www.efrag.org/files/ProjectDocuments/Proactive%20Income%20Taxes/120127_Income_tax_DP_final.pdf)

European Commission. (2014). *State aid: Commission investigates transfer pricing arrangements on corporate taxation of Apple (Ireland) Starbucks (Netherlands) and Fiat Finance and Trade (Luxembourg)*. Retrieved April 11, 2016, from [https://europa.eu/rapid/press-release\\_IP-14-663\\_en.htm](https://europa.eu/rapid/press-release_IP-14-663_en.htm)

European Commission. (2015a). *Combating corporate tax avoidance : Commission presents Tax Transparency Package*. Retrieved June 7, 2016, from [https://europa.eu/rapid/press-release\\_IP-15-4610\\_en.htm](https://europa.eu/rapid/press-release_IP-15-4610_en.htm)

European Commission. (2015b). *Commission decides selective tax advantages for Fiat in Luxembourg and Starbucks in the Netherlands are illegal under EU state aid rules*. Retrieved April 11, 2015, from [https://europa.eu/rapid/press-release\\_IP-15-5880\\_en.htm](https://europa.eu/rapid/press-release_IP-15-5880_en.htm)

European Commission. (2016). *State aid: Commission concludes Belgian “Excess Profit” tax scheme illegal; around €700 million to be recovered from 35 multinational companies*. Retrieved April 11, 2016, from [https://europa.eu/rapid/press-release\\_IP-16-42\\_en.htm](https://europa.eu/rapid/press-release_IP-16-42_en.htm)

FASB. (2011). *Accounting Standards Codification 740 Income Taxes*. Financial Accounting Standards Board. Retrieved from <https://law.resource.org/pub/us/code/bean/fasb.html/fasb.740.2011.html>

Feld, L. P., Heckemeyer, J. H., & Overesch, M. (2013). Capital structure choice and company taxation: A meta-study. *Journal of Banking & Finance*, 37(8), 2850–2866. doi:10.1016/j.jbankfin.2013.03.017

Fernandes, P. O., Monte, A. P., & Afonso, S. (2013a). *Corporate Social Responsibility For The Psi 20 Portuguese Companies. Responsibility and Sustainability. Socioeconomic, political and legal issues* (Vol. 1). Research Group on Marketing and Operative Research & Faculty on Economics and Business Sciences, University of León. Retrieved from <https://bibliotecadigital.ipb.pt/handle/10198/11087>

Fernandes, P. O., Monte, A. P., & Afonso, S. C. (2013b). Corporate Social Responsibility for the PSI 20 Portuguese companies. *Responsability and Sustainability*, 1, 7 – 15. Retrieved from [https://bibliotecadigital.ipb.pt/bitstream/10198/11087/1/RS-1\\_2\\_2-Fernandes-et-al.pdf](https://bibliotecadigital.ipb.pt/bitstream/10198/11087/1/RS-1_2_2-Fernandes-et-al.pdf)

Fernandez, R., McGauran, K., & Frederik, J. (2013). *Avoiding Tax in Times of Austerity. Energias de Portugal (EDP) and the Role of the Netherlands in Tax Avoidance in Europe*. Retrieved from [https://www.somo.nl/publications-en/Publication\\_3987](https://www.somo.nl/publications-en/Publication_3987)

Ferreira, H. A. L. (2014). *Impostos diferidos: uma análise à sua contabilização mediante a dimensão das empresas*. ISCAL.

Fisher, J. M. (2014). Fairer Shores: Tax Havens, Tax Avoidance, and Corporate Social Responsibility. *Boston University Law Review. Boston University. School of Law*, 94, 337–365. <http://ezproxy.concytec.gob.pe:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=94865540&lang=es&site=eds-live>

Fonseca, A. (2011). *O impacto do reconhecimento de impostos diferidos nas demonstrações financeiras de empresas não cotadas: estudo de caso de 10 empresas do gabinete de contabilidade - Audifirb, Lda*. ISCAL. Retrieved from [http://repositorio.ipl.pt/bitstream/10400.21/3515/1/Trabalho Final.pdf](http://repositorio.ipl.pt/bitstream/10400.21/3515/1/Trabalho%20Final.pdf)

Garriga, E., & Melé, D. (2004). Corporate Social Responsibility Theories : Mapping the Territory Social Responsibility Corporate Theories : Mapping the Territory. *Journal of Business Ethics*, 53(1/2), 51–71. doi:10.1023/B:BUSI.0000039399.90587.34

Global Reporting Initiative. (2013a). *G4 Sustainability Reporting Guidelines*. Retrieved August 24, 2015, from <https://www.globalreporting.org/resourcelibrary/GRIG4-Part1-Reporting-Principles-and-Standard-Disclosures.pdf>

Global Reporting Initiative. (2013b). *G4 Sustainability Reporting Guidelines. Implementation Manual Governo de Portugal. Plano Estratégico. Combate à Fraude e Evasão Fiscais e Aduaneiras, 2015-2017 (2015)*. Retrieved from [https://info.portaldasfinancas.gov.pt/nr/rdonlyres/e245bdae-d856-4186-a950-f0be649869df/0/plano\\_estrategico\\_combate\\_fraude\\_fiscal\\_aduaneira\\_2015\\_2017.pdf](https://info.portaldasfinancas.gov.pt/nr/rdonlyres/e245bdae-d856-4186-a950-f0be649869df/0/plano_estrategico_combate_fraude_fiscal_aduaneira_2015_2017.pdf)

Gupta, S., Mills, L. F., & Towery, E. M. (2014). The Effect of Mandatory Financial Statement Disclosures of Tax Uncertainty on Tax Reporting and Collections. *The Journal of the American Taxation Association*, 36(2), 203–229. doi:10.2308/atax-50766

Hardeck, I., & Hertl, R. (2013). Consumer Reactions to Corporate Tax Strategies: Effects on Corporate Reputation and Purchasing Behavior. *Journal of Business Ethics*, 123(2), 309–326. doi:10.1007/10551-013-1843-7

Hoi, C. K., Wu, Q., & Zhang, H. (2013). Is corporate social responsibility (CSR) associated with tax avoidance? Evidence from irresponsible CSR activities. *The Accounting Review*, 88(6), 2025–2059. doi:10.2308/accr-50544

Holland, K., Lindop, S., & Zainudin, F. (2016). Tax avoidance: A threat to corporate legitimacy? An examination of companies' financial and CSR reports. *British Tax Review*, (3).

- Hope, O. K., Ma, M. S., & Thomas, W. B. (2013). Tax avoidance and geographic earnings disclosure. *Journal of Accounting and Economics*, 56(2-3), 170–189. doi:10.1016/j.jacceco.2013.06.001
- Huseynov, F., & Klamm, B. K. (2012). Tax avoidance, tax management and corporate social responsibility. *Journal of Corporate Finance*, 18(4), 804–827. doi:10.1016/j.jcorpfin.2012.06.005
- IASB. (2009). *Income Tax: Basis for Conclusions. Exposure Draft ED/2009/2*. International Accounting Standards Board. Retrieved from <https://www.ifrs.org/Current-Projects/IASB-Projects/Income-Taxes/ED-march-09/Documents/EDIncomeTaxesBC.pdf>
- IFRS. (2015). *IAS 12 Income Taxes. Impact of uncertainty when an entity recognises and measures a current tax liability or asset—Proposed draft IFRIC Interpretation (2015)*. London: International Financial Reporting Standards. Retrieved from <http://www.ifrs.org/Meetings/MeetingDocs/Interpretations Committee/2015/January/AP02A - IAS 12 Uncertain tax position - Draft interpretation.pdf>
- Jenkins, J. G., & Sawyers, R. B. (2002). Financial Statement Disclosure of Corporate Tax Shelters. *The CPA Journal*, 72(6), 50–54.
- Jenkins, R. & Newell, P. (2013). CSR, Tax and Development. *Third World Quarterly*, 34(March), 378–396. doi:10.1080/01436597.2013.784596
- Jusoh, W. N. H. W. (2020). Corporate Social Responsibility: Conventional and Islamic Perspectives. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 129–149). IGI Global. doi:10.4018/978-1-7998-0218-1.ch007
- Kenyon, T. (2008). Tax Evasion, Disclosure, and Participation in Financial Markets: Evidence from Brazilian Firms. *World Development*, 36(11), 2512–2525. doi:10.1016/j.worlddev.2007.11.010
- Kim, J., & Im, C. (2017). Study on corporate social responsibility (CSR): Focus on tax avoidance and financial ratio analysis. *Sustainability*, 9(10), 1710. doi:10.3390/u9101710
- Laguir, I., Staglianò, R., & Elbaz, J. (2015). Does corporate social responsibility affect corporate tax aggressiveness? *Journal of Cleaner Production*, 107, 662–675. Advance online publication. doi:10.1016/j.jclepro.2015.05.059
- Lanis, R., & Richardson, G. (2012). Corporate social responsibility and tax aggressiveness: An empirical analysis. *Journal of Accounting and Public Policy*, 31(1), 86–108. doi:10.1016/j.jaccpubpol.2011.10.006
- Lenter, D., Slemrod, J., & Shackelford, D. (2003). Public Disclosure of Corporate Tax Return Information: Accounting, Economics, and Legal Perspectives. *National Tax Journal*, 56(4), 803–830. doi:10.17310/ntj.2003.4.06
- Lisowsky, P., Robinson, L., & Schmidt, A. (2013). Do Publicly Disclosed Tax Reserves Tell Us About Privately Disclosed Tax Shelter Activity? *Journal of Accounting Research*, 51(3), 583–629. doi:10.1111/joar.12003
- Lopes, I. C. R. (2015). *Divulgação de informação voluntária: análise empírica às empresas do PSI-20. ISCAL*.

- Lopes, I. T. (2014). The information compliance indexes: the illustrative case of income taxes. *Contaduría Y Administración: Revista Internacional*, 59(4), 11–37. Retrieved from [https://repositorio.iscte-iul.pt/bitstream/10071/8190/1/publisher\\_version\\_CA2014.pdf](https://repositorio.iscte-iul.pt/bitstream/10071/8190/1/publisher_version_CA2014.pdf)
- MacKenzie, B., Coe Tsee, D., Njikizana, T., Chamboko, R., & Colyvas, B. (2011). *Income Taxes. In 2011 Interpretation and Application of International Financial Reporting Standards*. John Wiley & Sons, Inc.
- McKinley, J., & Owsley, J. (2013). Transfer Pricing and Its Effect on Financial Reporting. *Journal of Accountancy*. Retrieved from <http://www.redi-bw.de/db/ebsco.php/search.ebscohost.com/login.aspx?direct=true&db=buh&AN=92022767&site=ehost-live>
- Mills, L. F., Robinson, L., & Sansing, R. C. (2010). FIN 48 and tax compliance. *The Accounting Review*, 85(5), 1721–1742. doi:10.2308/accr.2010.85.5.1721
- Ministério das Finanças. (2015). *Portaria n.º 220/2015 de 24 de julho (2015)*. PORTUGAL: Diário da República, 1.ª série — N.º 143 — 24 de julho de 2015. Retrieved from [http://www.cnc.min-financas.pt/pdf/SNC/2016/Portaria\\_220\\_2015\\_24Jul\\_DF.pdf](http://www.cnc.min-financas.pt/pdf/SNC/2016/Portaria_220_2015_24Jul_DF.pdf)
- Morais, A. I., & Lourenço, I. C. (2013). Informação a divulgar. In IFRS: Demonstrações financeiras. Um guia para executivos (pp. 76–149). Coimbra: Edições Almedina, S.A.
- Nabais, J. C. (1998). *O dever fundamental de pagar impostos*. Almedina.
- OECD. (1976). *Declaration by the Governments of OECD Member Countries and Decisions of the OECD Council on Guidelines for Multinational Enterprises*. Paris: Organisation for Economic Co-operation and Development (OECD) Publications. Retrieved from <http://www.oecd.org/daf/inv/mne/50024800.pdf>
- OECD. (2011). *OECD Guidelines for Multinational Enterprises*. Paris: Organisation for Economic Co-operation and Development (OECD) Publications. doi:10.1787/9789264115415-en
- OECD. (2013, July 20). *Closing the tax gap*. Remarks by Angel Gurría, Secretary-General of the OECD, G20/OECD Action Plan on Base Erosion and Profit Shifting (BEPS) Moscow. Retrieved from <http://www.oecd.org/about/secretary-general/closing-the-tax-gap.htm>
- Pedro, C. (2013, September 9). Estudo ilustra com o caso da EDP como as empresas portuguesas pagam menos impostos ao deslocarem lucros para a Holanda. *Journal Dos Negócios*. Retrieved from [https://www.jornaldenegocios.pt/empresas/detalhe/caso\\_da\\_edp\\_mostra\\_que\\_empresas\\_lusas\\_sedeadas\\_na\\_holanda\\_pagam\\_menos\\_impostos\\_em\\_portugal.html](https://www.jornaldenegocios.pt/empresas/detalhe/caso_da_edp_mostra_que_empresas_lusas_sedeadas_na_holanda_pagam_menos_impostos_em_portugal.html)
- Pereira, E. J. dos R. (2013). *O reconhecimento e a divulgação dos impostos diferidos em Portugal: Análise às entidades cotadas no PSI geral durante os anos de 2009 a 2011*. ISCAL. Retrieved from <http://repositorio.ipl.pt/bitstream/10400.21/3494/1/Disserta%C3%A7%C3%A3o-Vers%C3%A3oFinal%28Protegido%29.pdf>
- Pinto, L. C. de A. (2014). *Ética e responsabilidade social das empresas cotadas da Euronext Lisboa*. ISCAL.
- Pires, R. C. (2011). Ética e imposto: Reflexão de uma preocupação com a valorização da Sociologia e da Psicologia Fiscais. In *Ética fiscal* (pp. 33–58). Liabo: Universidade Lusíada Editora

Poço, M. de L. C., Lopes, C. M. da M., & Silva, A. M. F. G. da. (2015). Percepção da evasão e fraude fiscal em Portugal: um estudo sociológico - Parte I. *Revista de Finanças Públicas E Direito Fiscal*, 7(3), 131–153.

Preuss, L. (2012). Responsibility in Paradise? The Adoption of CSR Tools by Companies Domiciled in Tax Havens. *Journal of Business Ethics*, 110(1), 1–14. doi:10.1007/10551-012-1456-6

PriceWaterhouseCoopers. (2008). Taxation. In B. Johnson & P. Holgate (Eds.), *IFRS Manual of Accounting - 2009. Global Guide to International Financial Reporting Standards* (pp. 13001–14001). CCH.

PriceWaterhouseCoopers. (2014). *Financial statement presentation: 2014*. Retrieved August 31, 2015, from [http://www.pwc.com/en\\_US/us/cfodirect/assets/pdf/accounting-guides/pwc-financial-statement-presentation-second-edition-2015.pdf](http://www.pwc.com/en_US/us/cfodirect/assets/pdf/accounting-guides/pwc-financial-statement-presentation-second-edition-2015.pdf)

Rafay, A. (Ed.). (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5

Rafay, A., & Ajmal, M. M. (2014). Earnings Management through Deferred Taxes Recognized under IAS 12: Evidence from Pakistan. *Lahore Journal of Business*, 3(1), 1–19. doi:10.35536/ljb.2014.v3.i1.a1

Rafay, A., Yasser, F., & Khalid, Z. (2019). Revaluation of Non-Current Assets under IAS-16: Possibility of any Managerial inducement - Evidence from a South Asian Economy. *DLSU Business and Economics Review*, 29(1), 93–105.

Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.

Reuters. (2012). *UK, Germany push for multinationals to pay “fair share” of taxes*. Retrieved from <https://www.reuters.com/article/2012/11/05/us-g20-tax-idUSBRE8A413D20121105>

Rodrigues, J. (2012). *Sistema de normalização contabilística. SNC explicado*. Porto Editora.

Roque, I. A. M. (2012). *Contabilidade Ambiental: estudo sobre a sua aplicabilidade numa amostra de empresas do PSI-20*. Escola Superior de Ciências Empresariais de Setúbal. Retrieved from [http://comun.rcaap.pt/bitstream/123456789/3996/1/Tese Contabilidade Ambiental - Iolanda Roque.pdf](http://comun.rcaap.pt/bitstream/123456789/3996/1/Tese%20Contabilidade%20Ambiental%20-%20Iolanda%20Roque.pdf)

Sanches, J. L. S. (2006). *Os limites de planeamento fiscal*. Coimbra Editora.

Sanches, J. L. S., Câmara, F. de S. da, & Gama, J. T. da. (Eds.). (2009). *Reestruturação de empresas e limites do planeamento fiscal*. Coimbra: Coimbra Editora.

Scheiwiller, T., & Symons, S. (2014). Corporate responsibility and paying tax. *The OECD Observer. Organisation for Economic Co-Operation and Development*, 1. [http://www.oecdobserver.org/news/archivestory.php/aid/3132/Corporate\\_responsibility\\_and\\_paying\\_tax.html](http://www.oecdobserver.org/news/archivestory.php/aid/3132/Corporate_responsibility_and_paying_tax.html)

Secretário do Estado dos Assuntos Fiscais. Despacho n.º 260/2015 -XIX, Aviso n.º 8256/2015, Diário de República, 2.ª série — N.º 146 — 29 de julho de 2015. PORTUGAL. Retrieved from [http://www.cnc.min-financas.pt/pdf/SNC/2016/Aviso\\_8256\\_2015\\_29Jul\\_NCRF\\_RG.pdf](http://www.cnc.min-financas.pt/pdf/SNC/2016/Aviso_8256_2015_29Jul_NCRF_RG.pdf)

Silva, A. R. M. (2014). *A divulgação da responsabilidade social empresarial nas empresas do PSI geral da Euronext Lisboa: Relatórios de sustentabilidade vs. divulgação online*. ISCAL.

- Silva, M. de L. e. (2015). *A divulgação do risco nas demonstrações financeiras: uma análise ao anexo das sociedades não financeiras portuguesas*. ISCAL. Retrieved from <http://repositorio.ipl.pt/handle/10400.21/4619>
- Tomohara, A., Lee, H. J., & Lee, S. (2012). Did FIN 48 increase companies' tax payments? Trade-off between disclosure and tax burdens. *Applied Economics*, 44, 4239–4248. doi:10.1080/00036846.2011.587789
- Venâncio, R. (2012a, January 4). Mais empresas podem seguir Jerónimo Martins. *Diário Económico*. Retrieved from <http://economico.sapo.pt/noticias/nprint/135089>
- Venâncio, R. (2012b, January 4). Marca Pingo Doce pode sofrer danos de reputação. *Económico*. Retrieved from <http://economico.sapo.pt/noticias/nprint/135087>
- Wells, H. (2002). The Cycles of Corporate Social Responsibility: An Historical Retrospective for the Twenty-First Century. *Kansas Law Review*, 51, 77–170.
- Ylönen, M., & Laine, M. (2014). For logistical reasons only? A case study of tax planning and corporate social responsibility reporting. *Critical Perspectives on Accounting*. Advance online publication. doi:10.1016/j.cpa.2014.12.001
- Zhang, R. (2010). Enterprise social responsibility and tax planning. *2010 International Conference on E-Product E-Service and E-Entertainment, ICEEE2010*. 10.1109/ICEEE.2010.5661450

## **ADDITIONAL READINGS**

- Allison, P. (2013). Why I Don't Trust the Hosmer-Lemeshow Test for Logistic Regression. Retrieved from <https://statisticalhorizons.com/hosmer-lemeshow>
- Annuar, H. A., Salihu, I. A., & Obid, S. N. S. (2014). Corporate Ownership, Governance and Tax Avoidance: An Interactive Effects. *Procedia: Social and Behavioral Sciences*, 164(August), 150–160. doi:10.1016/j.sbspro.2014.11.063
- Avi-Yonah, R. S. (2014). Corporate Taxation and Corporate Social Responsibility. *New York University Journal of Law & Business*, 11(1), 29. Retrieved from <http://repository.law.umich.edu/cgi/viewcontent.cgi?article=2406&context=articles>
- Bonsón, E., & Bednárová, M. (2015). CSR reporting practices of Eurozone companies. *Revista de Contabilidad*, 18(2), 182–193. doi:10.1016/j.rcsar.2014.06.002
- Bouten, L., Everaert, P., Van Liedekerke, L., De Moor, L., & Christiaens, J. (2011). Corporate social responsibility reporting: A comprehensive picture? *Accounting Forum*, 35(3), 187–204. doi:10.1016/j.accfor.2011.06.007
- Buettner, T., Overesch, M., Schreiber, U., & Wamser, G. (2012). The impact of thin-capitalization rules on the capital structure of multinational firms. *Journal of Public Economics*, 96(11-12), 930–938. doi:10.1016/j.jpubeco.2012.06.008

dos Santos, S. I. C. (2013). *A divulgação de informação financeira no relato intercalar: uma análise às entidades das n.o PSI ge r a l*. ISCAL. Retrieved from [https://repositorio.ipl.pt/bitstream/10400.21/4619/1/A divulgação do risco nas demonstrações financeiras - uma análise ao anexo da sociedades não financeiras portuguesas.pdf](https://repositorio.ipl.pt/bitstream/10400.21/4619/1/A%20divulga%C3%A7%C3%A3o%20do%20risco%20nas%20demonstra%C3%A7%C3%B5es%20financeiras%20-%20uma%20an%C3%A1lise%20ao%20anexo%20da%20sociedades%20n%C3%A3o%20financeiras%20portuguesas.pdf)

European Commission. (2014). State aid: Commission investigates transfer pricing arrangements on corporate taxation of Apple (Ireland) Starbucks (Netherlands) and Fiat Finance and Trade (Luxembourg). Retrieved April 11, 2016, from [https://europa.eu/rapid/press-release\\_IP-14-663\\_en.htm](https://europa.eu/rapid/press-release_IP-14-663_en.htm)

European Commission. (2015). Combatting corporate tax avoidance : Commission presents Tax Transparency Package. Retrieved June 7, 2016, from [https://europa.eu/rapid/press-release\\_IP-15-4610\\_en.htm](https://europa.eu/rapid/press-release_IP-15-4610_en.htm)

European Commission. (2015). Commission decides selective tax advantages for Fiat in Luxembourg and Starbucks in the Netherlands are illegal under EU state aid rules. Retrieved April 11, 2015, from [https://europa.eu/rapid/press-release\\_IP-15-5880\\_en.htm](https://europa.eu/rapid/press-release_IP-15-5880_en.htm)

European Commission. (2016). State aid: Commission concludes Belgian “Excess Profit” tax scheme illegal; around €700 million to be recovered from 35 multinational companies. Retrieved April 11, 2016, from [https://europa.eu/rapid/press-release\\_IP-16-42\\_en.htm](https://europa.eu/rapid/press-release_IP-16-42_en.htm)

GRI. (2013a). *G4 Sustainability Reporting Guidelines*. Global Reporting Initiative. Retrieved from <https://www.globalreporting.org/resourcelibrary/GRIG4-Part1-Reporting-Principles-and-Standard-Disclosures.pdf>

GRI. (2013b). *G4 Sustainability Reporting Guidelines: Implementation Manual*. Global Reporting Initiative.

Henriques, M. (2011). *A divulgação de impostos diferidos após a adopção das NIC: o caso espanhol*. ISCTE - UIL. Retrieved from <http://hdl.handle.net/10071/2586>

Levine, D. M., Berenson, M. L., & Stephan, D. (2000). *Estatística: Teória e Aplicações, usando Microsoft Excel em Português*. LTC - Livros Técnicos e Científicos Editora S.A.

Lin, S., Tong, N., & Tucker, A. L. (2014). Corporate tax aggression and debt. *Journal of Banking & Finance*, 40(January 2010), 227–241. doi:10.1016/j.jbankfin.2013.11.035

Lopes, M. dos A. (2014). *Os impostos diferidos no balanço: estudo de caso*. Associação de Politécnicos do Norte (APNOR) Instituto Politécnico de Bragança. Retrieved from [https://bibliotecadigital.ipb.pt/bitstream/10198/10338/1/Magui dos Anjos Lopes.pdf](https://bibliotecadigital.ipb.pt/bitstream/10198/10338/1/Magui%20dos%20Anjos%20Lopes.pdf)

Michelon, G., Pilonato, S., & Ricceri, F. (2014). CSR reporting practices and the quality of disclosure: An empirical analysis. *Critical Perspectives on Accounting*. Advance online publication. doi:10.1016/j.cpa.2014.10.003

Organisation for Economic Co-operation and Development. (2011). *OECD Guidelines for Multinational Enterprises*, 2011 Edition. doi:10.1787/9789264115415-en

Organisation for Economic Co-operation and Development. (2013). Closing the tax gap. Remarks by Angel Gurría, Secretary-General of the OECD, G20/OECD Action Plan on Base Erosion and Profit Shifting (BEPS) Moscow, 20 July 2013, 12h15. Retrieved from <http://www.oecd.org/about/secretary-general/closing-the-tax-gap.htm>

Overesch, M., & Wamser, G. (2010). Corporate tax planning and thin-capitalization rules: Evidence from a quasi-experiment. *Applied Economics*, 42(5), 563–573. doi:10.1080/00036840701704477

Overesch, M., & Wamser, G. (2014). Bilateral internal debt financing and tax planning of multinational firms. *Review of Quantitative Finance and Accounting*, 42(2), 191–209. doi:10.1007/11156-012-0339-3

Pereira, J. P. (n.d.). *Decisão do dono da Jerónimo Martins criticada online com apelo de boicote ao Pingo Doce*. PÚBLICO.

Statista Inc. (2015). Portugal: Growth rate of the real gross domestic product (GDP) from 2010 to 2020 (compared to the previous year). Retrieved December 30, 2015, from <https://www.statista.com/statistics/372306/gross-domestic-product-gdp-growth-rate-in-portugal/>

Taylor, G., & Richardson, G. (2013). The determinants of thinly capitalized tax avoidance structures: Evidence from Australian firms. *Journal of International Accounting, Auditing & Taxation*, 22(1), 12–25. doi:10.1016/j.intaccudtax.2013.02.005

Taylor, G., Tower, G., & Van Der Zahn, M. (2011). The influence of international taxation structures on corporate financial disclosure patterns. *Accounting Forum*, 35(1), 32–46. doi:10.1016/j.accfor.2010.06.001

United Nations Global Compact. (2014). Guide to Corporate Responsibility. Retrieved August 21, 2015, from [https://www.unglobalcompact.org/docs/publications/UN\\_Global\\_Compact\\_Guide\\_to\\_Corporate\\_Sustainability.pdf](https://www.unglobalcompact.org/docs/publications/UN_Global_Compact_Guide_to_Corporate_Sustainability.pdf)

United Nations Global Compact. (2014). Guide to Corporate Responsibility. Retrieved August 21, 2015, from [https://www.unglobalcompact.org/docs/publications/UN\\_Global\\_Compact\\_Guide\\_to\\_Corporate\\_Sustainability.pdf](https://www.unglobalcompact.org/docs/publications/UN_Global_Compact_Guide_to_Corporate_Sustainability.pdf)

United Nations Global Compact. (2015). Business for the Rule of Law Framework. Retrieved August 21, 2015, from [https://www.unglobalcompact.org/docs/issues\\_doc/rule\\_of\\_law/B4ROL\\_Framework.pdf](https://www.unglobalcompact.org/docs/issues_doc/rule_of_law/B4ROL_Framework.pdf)

United Nations Global Compact. (2015). Business for the Rule of Law Framework. Retrieved August 21, 2015, from [https://www.unglobalcompact.org/docs/issues\\_doc/rule\\_of\\_law/B4ROL\\_Framework.pdf](https://www.unglobalcompact.org/docs/issues_doc/rule_of_law/B4ROL_Framework.pdf)

## **ENDNOTE**

- <sup>1</sup> The term International Financial reporting Standards (IFRS) is used to cover International Accounting Standards (IASs) issued previously by International Accounting Standards Committee.



# Chapter 22

## Firms' Characteristics and Tax Evasion

**Md. Harun Ur Rashid**

 <https://orcid.org/0000-0001-7660-9531>

*International Islamic University Chittagong, Bangladesh*

**Anika Morshed**

*International Islamic University Chittagong, Bangladesh*

### ABSTRACT

*The study investigates whether the firms' characteristics, including ownership structure, audit, and familiarity affect tax evasion. The study has used the ordinary least square (OLS) to analyze cross-sectional data of 85 countries between 2007 and 2015 collected from the world enterprise survey. The study finds that the domestic, foreign, and government ownership in the firm increases tax evasion, whereas proprietorship and female ownership decreases the tax evasion. Further, the results show that familiar firms with international recognition are less inclined to evade tax. Similarly, the negative relationship between audit and tax evasion implies that the government should make it compulsory to check the financial statements of the firms by the external auditors, which, in turn, reduces the firms' tax evasion. Moreover, the firms that face more financial constraints evade more tax than the firms with access to the bank loan and solvent ones. The tax authorities should also consider reducing the corporate tax rate as the higher tax rates stimulate the firms to evade more tax.*

### INTRODUCTION

Research on tax evasion has been come out to an obligatory part for every country in this competitive era as most of the real earnings of a country go to the trash for the lack of investigation on taxpayers or tax management. Much more analysis is needed on the topic of firms' tax evasion, which can be theoretical or empirical. Nevertheless, most of the research can be seen from the theoretical perspective due to the lack of data as firms would not like to take the risk of sharing their data. Another reason is, it is complex to capture tax evasion analytically (Alm, Liu, & Zhang, 2019). However, prior research evidenced

DOI: 10.4018/978-1-7998-5567-5.ch022

the significant effect of firm characteristics on tax evasion at both the micro-level (Blackburn, Bose, & Capasso, 2012; Mitra, 2017) and macro-level (Alm, Martinez-Vazquez, & McClellan, 2016; Beck, Lin, & Ma, 2014). Most of the literature has been discussed on individual tax evasion as well as income tax avoidance and a growing literature is working on firm tax evasion in the present situation because of being essential in today's financial condition in the world.

Tax evasion occurs if taxpayers intentionally do not comply with their tax obligations either through the failure of filling return, misreporting income or overstating expenses, or making a lower payment compared to actual tax despite having the ability to pay tax (Rashid, 2020; Islam et al., 2020). Tax evasion is considered as an illegal act which breaks law and influences not to pay tax (Besley, Jensen, & Persson, 2019). It is a willful task which is done in an illegal way to reduce tax liability (Doerrenberg & Duncan, 2019). Tax evasion inaugurated with the informal economy is also called black, underground or shadow economy (Alm et al., 2016; Slemrod, 2007).

Tax evasion has been considered as a subject of discussion for academic research in both developed and developing countries (Umar et al., 2019; Yamen et al., 2018). However, most of it relates to individuals. Most of the previous studies on tax evasion are based on the study of Allingham & Sandmo (1972), which focused on theoretical analysis from the individual perspective, and did not consider the firm with some exceptional studies (Alm et al., 2016; Carrillo, Pomeranz, & Singhal, 2017). Though most of the empirical research has mostly investigated the individual income tax evasion, empirical researches on firm tax evasion have been started recently (Abdixhiku, Pugh, & Hashi, 2018; Alm et al., 2019; Alm et al., 2016).

Research on firm tax evasion has become more critical as firms play a crucial role in an economy and the country's GDP as well. According to Torgler & Schneider (2007), tax evasion is covering more than 50% of countries, especially low-income countries' GDP. If firms continue to evade tax, then most of the countries' tax revenue will go in vain. The study is an attempt to measure which factors influence firms to evade tax and how much firms evade tax across the countries. Social general and economic developments are mostly depended on tax collection capacity. Through firms' tax evasion, a large amount of tax gap is created in government earnings which are one of the crucial reasons behind a country's underdevelopment condition. It is considered a severe loss of government revenue, resulting in pressure to the government in providing public services smoothly (Islam et al., 2020). Therefore, it has been a challenging issue for governments as well as tax authorities to increase the tax revenue from the taxpayers. The marginal net benefit from the firms' income decreases because of poor financial development an economy. The lower stage of financial development makes the higher incidence of evading tax and greater the underground economy size. These types of initiatives are the reasons for resource wastes or inefficient uses (Blackburn et al., 2012). Also, imperfect credit-information sharing system and lower level of bank branch penetration, increase tax evasion more (Beck et al., 2014; Blackburn et al., 2012).

Dearth studies on tax evasion at the firm level are unfortunate, especially given the matter that in most of the countries, firms pay the bulk share of taxes and also consider the bulk of tax evasion as well (Crocker & Slemrod, 2005; Nur-tegin, 2008). Moreover, as per the suggestion of the study of Abdixhiku et al. (2018), there is a considerable gap and thus a permanent need for international and cross country research on tax evasion, while the research worldwide at firm-level characteristics is still insufficient. Therefore, the study aims to reduce the gap by introducing some empirical findings for firm characteristics, cross-country and global tax evasion features.

The investigation of some other internal characteristics of the firm on tax evasion is still unexplored across the countries. For example, the firms' size, age, ownership structure (Rafay et al., 2016), financial

management process, workforce, top management experience, familiarity, audit have yet to be investigated on tax evasion. The limited research on the relationship between firms' characteristics and tax evasion is also a substantial gap in the existing literature. Therefore, the study aims to examine whether the firm characteristics affect tax evasion.

Do the firm characteristics matter for tax evasion? What factors influence the firms in the decision-making process of tax evasion? Along with the responses of the research questions, the study contributes to the existing literature in the following ways. First, shedding light on the theoretical discussion, this study provides empirical evidence on the crucial linkage between firm characteristics and tax evasion. Second, the study aims to examine, to what extent, the ownership structure, funding behaviour and top management experience lead the firms in tax evasion decision-making in line with the study of Beck *et al.* (2014) and Alm *et al.* (2019). Third, the study includes three heterogeneities such as firm-size-large, medium and small firms; industry- manufacturing and servicing firms; and gender at top-level management- male and female along with firm age, audit, international recognition to provide robust results. Finally, the outcome of this research will guide the government and policymakers to understand the relationship between different firm characteristics and tax evasion, which in turn, helps them to take necessary steps to develop policy frameworks for reducing tax evasion.

The rest of the paper is structured as follows. Section 2 discusses the theories and reviews the literature. Section 3 describes the research methods and design with the empirical specification. Section 4 analyzes the results and presents a discussion of the study. Section 5, finally, sets out the conclusions and implications, along with the limitations of the study and suggestions for future research.

## **LITERATURE REVIEW**

Tax evasion is the reflection of the information gap, as agency problems exist between firms and shareholders. By understanding financial policies, firms can reduce information gap and agency problems which have been reconsidered by economists. Desai (2005) considered tax evasion from the perspective of agency cost theory because managers use tax evasion as a rent extension with them. He also added that tax evasion has a positive relation with information asymmetry. The higher the information gap creates; the more tax evasion takes place in firms. It incites firms' managers to hide information from the shareholders and conceals the real income and cash flows of firms. On the other hand, the shareholders and owners would like to know the actual financial position of their business; it may demotivate the tax evasion (Alm *et al.*, 2016; Zhang, Chen, & He, 2018).

Firms and managerial transactions also tamper as tax evasion is not being considered as a legal term. Managers of firms are generally able to divert income earning in the form of rent and show less income than the general one to the shareholders and the tax authorities. If the percentage of tax sheltering is higher on time than the diversion by managers, then it can be taken as strong complementarities (Rafay & Ajmal, 2014). If the cost of tax sheltering is not high and complementarities are not too strong, the managers reduce the tax with the diversion of rents and engaging in more tax-saving activities as well (Desai, 2005). In this case, at what extent, the managers will be able to evade tax highly depend on the external pressure and controlling power of the firm's owners.

Assessing a lending program to estimate whether the firm faces credit constrained, Banerjee & Duflo (2014) documented that the firms face severely credit constrained when the marginal rate of return of

## **Firms' Characteristics and Tax Evasion**

borrowing funds is too high to bear. Due to the unavailability of external funding sources, they find tax evasion as a way to increase internal funds to manage firms' costs (Alm *et al.*, 2019).

To ensure the institutional transparency and familiarity, the firms should improve audit and reporting standard to reduce corruption and tax evasion (Hudori & Mustikasari, 2020). The good quality accountants are also required as a means of promoting accountability and ethical action, complying with tax rules and inviting their customers to avoid tax evasion (Khlif & Guidara, 2018)

## **Firms' Ownership Structure and Tax Evasion**

Firms' ownership structure has substantial impacts on tax evasion as either they play the role of decision-makers or create pressure on the management to maximize their interests. Firms with domestic owners are more likely to be involved in tax evasion than firms with foreign owners (Alm *et al.*, 2016). The domestic owners are like to be involved in bribes and get enough freedom as they are not answerable to anyone for their activities. On the other hand, foreign owners are seen not to be intended to evade tax as they are accountable both to their government and foreign government for their business activities (Alm *et al.*, 2016; Zhang *et al.*, 2018). Though some researchers found that foreign firms are not seemed to have a significant impact on tax evasion, Annuar, Salihu & Obid (2014) found a positive relationship between foreign ownership and tax evasion. And they evidenced that foreign firms pay lower taxes compared to local firms despite making higher profits. Preuss (2010) also documented a consistent positive relationship between tax avoidance and foreign ownership, arguing that the foreign-owned firms use profit-shifting strategies to reduce their tax liabilities. Government-owned firms are also connected with tax evasion. The main reason behind the involvement with tax evasion of government owners is not to manage the firms directly. The management can easily hide the actual income from government and tax authorities as tax audits cannot be feasible because of their political connections (Salihu, Annuar, & Obid, 2015). However, the study of Payne and Saunoris (2020) found a negative relationship between government-owned firms and tax evasion. If the government are trustworthy and free from corruption, then government-owned firms may be less tendency to be involved with tax evasion.

Similarly, the proprietorship owned and controlled by a single owner is more intended to evade tax (Alm *et al.*, 2016; Bornemann, Jacob, & Sailer, 2019). In the sole proprietorship, the owner is always in need of capital and faces obstacles in managing loans compared to large firms; he/she chooses tax evasion as a more accessible way to gather necessary capital.

The probability of tax sheltering is lower when the firm is under control of female ownership and female CFOs as they are less likely to be involved in tax evasion compared to males (Bornemann *et al.*, 2019; Francis *et al.*, 2014). Francis *et al.* (2014) worked on a sample of changing ownership from male to male and another sample of changing ownership from male to female. There result indicated that the probability of tax evasion increases in male-to-male transition. On the other hand, there is a decreasing probability when the transition is male to female. Therefore, the study assumes that female ownership and female participation in top management has a negative relation with tax evasion.

## **Funding Behaviour and Tax Evasion**

Funding behaviour can be defined as the usage and accessibility of the fund. It also means the source from which the firms are using to meet their needs and get accessibility whenever they face crises of capital. Some firms use a bank loan or line of credit, while others do not need any loan. Some firms use

banks to finance their investments, while others use banks to finance their working capital. Some other firms have been identified as access to finance as major constraints. Previous studies showed that the firm decision to evade tax is based on different funding behaviour. For instance, firms that face more financial constraints likely to be involved in more tax evasion than the firm not needing any loan (Alm *et al.*, 2019). There are two reasons why financial constraints push firms toward tax evasion. At first, financial constraints create prevention in the path of accessing external finance, for which the firms intense to evade tax to gain revenues intentionally. In capital market imperfections, the firms find external funds so difficult or expensive to manage, and thereby they are forced to depend on internal funds. Financial constraint firms face difficulties to get access to external finance from financial institutions. For instance, the banks require collateral - something pledged as security for repayment of a loan, to be forfeited in the event of default before sanctioning loan to firms. They find tax evasion as a way to increase internal funds more to manage firms' costs as they cannot get external funds. Second, underdeveloped financial markets influence firms towards the informal sector rather than formal or legal sectors. Also, it is straightforward to deny obligations and other official rules in the informal sector (Alm *et al.*, 2019). In underdeveloped financial markets, credit is costly and less available than the developed markets (Johnson *et al.*, 2000).

On the other hand, the solvent firms may have less tendency to evade tax and would like to pay more tax than the firms need a loan or the firms which are in the line of credit. Therefore, it is assumed that there is a negative relationship between solvent firms and tax evasion. On the other hand, the firms which are with a bank loan or line of credit have a high tendency to evade tax. The underlying reason behind tax evasion by loan taking firms is loan cost<sup>1</sup> for which the actual amount of loan increases for some additional expenses. Hence, the firms feel to evade tax for recovering loans with additional costs (Hasan *et al.*, 2014). The study of Capasso & Santoro (2016) documented that the firms which have taken bank loan show less tendency to evade tax as their banks are of their risks of financial transactions (Sinha, 2021; Gupta & Biswas, 2021). Nevertheless, Hasan *et al.* (2014) found a positive relationship between the firms obtained a bank loan and tax evasion as a pressure of repayment of the bank loans with interest within due time makes the firms' manager think of tax evasion.

### **Audit and Familiarity of Firms and Tax Evasion**

Chen *et al.* (2019) documented that firms try to shelter their income and decide to evade tax only if it is proved that the tax authorities do not perform the investigation. The firms which are certified by external auditors are less likely to be involved in tax evasion (Huseynov & Klamm, 2012). The external auditors check the financial statement of the firms properly and report the exact income in the income statement with verifications (Hudori & Mustikasari, 2020; Khan *et al.*, 2020). Similarly, the firms which are internationally recognized have more familiarity than any other firm (Ramzan *et al.*, 2020); it encourages them to comply with tax obligations. These kinds of firms may have fewer tendencies to evade tax as they have more fear of losing goodwill if the firms are caught or accused of tax evasion. Therefore, the audit and familiar firms may have negative impact on tax evasion.

## **METHODOLOGY**

### **Sampling and Data Collection**

In order to examine the impact of firm characteristics on tax evasion, the study used a cross-sectional data of 85 countries between 2007 and 2015. The study used a variety of sources for data based on the availability of data. For instance, the International Monetary Fund (IMF) working paper- 2018 has been used to gather the shadow economy as a proxy of tax evasion data that cover the latest data up to 2015. For the measurement of the firm characteristics, the study uses the country-level aggregated data from the World Enterprise Survey (WES) of the World Bank Group, which collected data over 135,000 firms from 139 countries. The WES creates over 100 indicators that benchmark the quality of the business environment across the globe. As part of its strategic goal of building a climate for investment, job creation, and sustainable growth, the World Bank has promoted improving the business environment as a key strategy for development, which has led to a systematic effort in collecting enterprise data across countries. The countries are surveyed at the firm level at every 3-4 years to understand what firms experience in the private sector. For economic measurement, GDP, inflation, and tax rate have been gathered from World Bank Indicators.

### **Dependent Variable**

Tax evasion (TE) is used as a dependent variable which is a proxy of the shadow economy (Yamen *et al.*, 2018). Though some researchers have used hypothetical perceptions of evasion or government estimation, none is better than others (Hardeck *et al.*, 2018). As actual tax evasion cannot be measured and impossible to determine, many researchers have used the shadow economy as a proxy for tax evasion (Schneider & Buehn, 2012). Shadow economy determines all hidden economic activities which are concealed from official authorities.

This research is based on the MIMIC model (Multiple Causes Multiple Indicators), a shadow economy macroeconomic measure. The MIMIC model takes various factors such as tax burden, regulatory burden, economic freedom index, business freedom index, unemployment rate and GDP per capita into account (Schneider, Buehn, & Montenegro, 2010) since tax evasion directly affects the dimensions of the shadow economy over time.

### **Independent Variables**

The study has used different types of firm characteristics as independent variables based on country-level aggregated data as the data are available in the World Enterprise Survey of World Bank group. First, the study includes the ownership structure such as domestic owners (DO), foreign owners (FO), government owners (GO), female owners (FeO) and Proprietorship (P) as independent variables. Since the different owners have an interest in the earning management of the firms; they play a significant role in influencing the decision-making process of firms (Nafti, Kateb, & Masghouni, 2020).

Moreover, whether a firm evades tax significantly depends on its financial access or financial constraint (Alm *et al.*, 2019). Therefore, this study examines a variety of funding behaviour such as firms with a bank loan/line of credit, not needing a loan (solvent firms), using banks to finance investments, using supplier/customer credit to finance working capital and firms identifying access to finance as a

major constraint. If financial constraints increase in an economy, tax evasion will also increase. There are also problems with information sharing in financial transition and for which firms do not feel free to access loans or any other financial help from financial institutions. Thus, a positive relationship exists between tax evasion and financial constraints. On the contrary, since the solvent firms can manage necessary funds from internal sources for which they need not bear any loan cost. As a result, the firms make a higher profit and keep a portion of the profit as reinvestment which makes them more solvent. On the other hand, the firms which are with a bank loan or line of credit have a high tendency to evade tax.

Finally, the study also included audit and familiarity as crucial explanatory variables of firm characteristics. Whether a firm will conceal income for tax evasion highly depends on the audit and investigation (Chen *et al.*, 2019). Higher the possibility of an audit, lower the possibility of tax evasion (Rashid, 2020) imply that verification of financial statement by external auditors may reduce tax evasion (Hudori & Mustikasari, 2020). Similarly, the familiar firms with international recognition may not take the risk of losing their reputation by tax evasion.

## **Control Variables**

For cross-country investigation, it is essential to include a few environmental control variables to regulate the country's social and economic differences (Yamen *et al.* (2018). The study uses two types of control variables- institutional and economic factors. The institutional factors cover firms' size (number of workers) age, and top managers' experience. On the other hand, the environmental factors include GDP, inflation and tax rate; both of these factors have a significant effect on tax evasion (Abdikhiku *et al.*, 2018; Atwood & Lewellen, 2019; Carrillo *et al.*, 2017; Chen *et al.*, 2019; Dyreng, Hanlon, & Maydew, 2018; Gupta, 2008).

Firm size is related to the overall firm's assets, profitability, industry sunk cost and more management layers, more sharp skills, number of departments and functions (Doerrenberg & Duncan, 2019; Gupta, 2008). Among smaller firms, tax evasion is highly prevalent, and they are often not qualified for tax exemption compared to large firms, so they choose a way of tax evasion to cope up with the large firms in the competitive market (Benczúr, Kátay, & Kiss, 2018; Irianto, Sudibyo, & Wafirli, 2017). Therefore, the sizes of the firms negatively impact the tax evasion as prior studies showed that the larger the firms' size, the lower the level of tax evasion (Salihu *et al.*, 2015). Similarly, the age of firms has a more considerable influence on tax evasion. Gatsi, Gadzo, and Kportorgbi (2013) and Sharma and Mitra (2015) found a negative correlation between age of firms and tax evasion as new firms always intend to reap more profits. In addition, as a newcomer, they cannot earn much; so new firms find tax evasion as a way of increasing profit.

However, the firms with female participation in the top management are seen in less intended in tax evasion compared to males (Francis *et al.*, 2014; McGee & Preobragenskaya, 2006). Since the female is more risk-averse than that of male, they opposed tax evasion. Moreover, female directors do their best to balance the responsible behaviours of firms toward society and shareholders. Hoseini, Gerayli, and Valiyan (2019) have shown that female makes better decisions than men to promote financial report transparency. Therefore, there may have a negative relationship between tax evasion and a top female manager.

Since the shadow economy represents the percentage of GDP, the countries which have a broader shadow economy are more intended to tax evasion (Schneider, Raczkowski, & Mróz, 2015; Tsakumis, Curatola, & Porcano, 2007). Similarly, firms quickly tend to evade tax when inflation occurs; the nominal

## ***Firms' Characteristics and Tax Evasion***

disposable income is eroded. A positive relation between tax evasion and inflation can happen if the risk aversion associated with the real disposable income rises (Crane & Nourzad, 1986; Islam et al., 2020) and the net effect on tax revenues by inflation is generally not believed (Besley, Jensen, & Persson, 2019). Moreover, the relationship between tax rate and tax evasion is also positive as with increasing one percent of tax rates, three percentages of tax evasion rate go up (Javorcik & Demir, 2019).

## **OLS Regression Model**

OLS (Ordinary Least Square) method has been used to examine the relationship between firms' characteristics and tax evasion; the regression method is:

Model 1-2: Tax evasion =  $f$  (Ownership structure, funding behaviour, other specific characteristics, economics factors)

$$TE_i = \alpha_0 + \beta_1 DO_i + \beta_2 FO_i + \beta_3 GO_i + \beta_4 FeO_i + \beta_5 P_i + \beta_6 Age_i + \beta_7 Size_i + \beta_8 Audit_i + \beta_9 Familiar_i + \beta_{10} Tax Rate_i + \beta_{11} GDP_i + \beta_{12} INF_i + \beta_{13} BLFI_i + \beta_{14} FCF_i + \beta_{15} Solvent_i + \beta_{16} FBL_i + \beta_{17} TME_i + \varepsilon_i$$

Model 3-10: Further to investigate the robustness of the impact of firms' sizes, top management genders, and industry types on tax evasions, the study offers the following econometric models.

Tax evasion =  $f$  (Ownership structure; funding behaviour; other specific characteristics; economics factors; small, medium and large firm; female and male in top-level management; and manufacturing and servicing firms).

$$TE_i = \alpha_0 + \beta_1 DO_i + \beta_2 FO_i + \beta_3 GO_i + \beta_4 FeO_i + \beta_5 P_i + \beta_6 Age_i + \beta_7 Size_i + \beta_8 Audit_i + \beta_9 Familiar_i + \beta_{10} Tax Rate_i + \beta_{11} GDP_i + \beta_{12} INF_i + \beta_{13} BLFI_i + \beta_{14} FCF_i + \beta_{15} Solvent_i + \beta_{16} FBL_i + \beta_{17} TME_i + Y_1 Small_i + Y_2 Medium_i + Y_3 Large_i + \xi_1 TMF_i + \xi_2 TMM_i + \emptyset_1 Manufacturing_i + \emptyset_2 Servicing_i + \mu_i + \varepsilon_i$$

Where, in model 1, from  $\beta_1$  to  $\beta_5$ ,  $\beta_6$  to  $\beta_9$  and  $\beta_{10}$  to  $\beta_{12}$  are the coefficients of ownership structure, firms' specific characteristics, and economic factors, respectively. The elaborations of all variables mentioned in Table 1 and =error term for country; = the number of countries used for the study. In model 2, along with model 1, along with model 1,  $\beta_{13}$  to  $\beta_{16}$  and  $\beta_{17}$  refers to funding behaviour and top management experiences respectively have been added. Additionally, in model 2, to  $Y_3$  are the coefficients of firm sizes, small, medium, and large while  $\xi_1$  to  $\xi_{12}$  and  $\emptyset_1$  and  $\emptyset_2$  are the coefficients of top management male and female, and industry types, manufacturing and servicing firms, respectively. The error term of  $\mu_i$  and  $\varepsilon_i$  represent between and within entity error.



*Table 1. Variables measurements and data sources*

Variables	Short forms	Data Source and Measurements
<b>Dependent variable</b>		Shadow economy around the world- IMF- <a href="https://www.imf.org/~media/Files/Publications/WP/2018/wp1817.ashx">https://www.imf.org/~media/Files/Publications/WP/2018/wp1817.ashx</a>
Tax Evasion	TE	Tax Evasion has been adopted as the proxy of the shadow economy. It is defined as the "Market-based production of goods and services, whether legal or illegal, that escapes detection in the official estimates as a percentage of GDP."
<b>Independent and control variables</b>		World Bank Enterprise Surveys - <a href="https://www.enterprisesurveys.org/data">https://www.enterprisesurveys.org/data</a>
<b>Ownership structures</b>		
Proprietorship	P	Percent of firms with the legal status of Sole Proprietorship
Domestic owners	DO	The proportion of private domestic ownership in a firm (%)
Foreign owners	FO	Percent of firms with at least 10% of foreign ownership
Government owners	GO	Percent of firms with at least 10% of government/state ownership
Female owners	FeO	Percent of firms with female participation in ownership
<b>Funding behaviours</b>		
Bank loan	FBL	Percent of firms with a bank loan/line of credit
Solvent firms	Solvent	Percent of firms not needing a loan
Loan for financial investment	BLFI	Percent of firms using banks to finance investments
Financially constraint firms	FCF	Percent of firms identifying access to finance as a major constraint
Familiarity	Familiar	Percent of firms with an internationally recognized quality certification
Audit	Audit	Percent of firms with an annual financial statement reviewed by external auditors
<b>Control variables</b>		
Age	Age	Age of the establishment (years)
Firms' Size	Size	Number of workers
Top management experience	TME	Years of the top management experience working in the firm sector
<b>Economic factors</b>		World Bank Groups- <a href="https://data.worldbank.org/indicator">https://data.worldbank.org/indicator</a>
Tax rate	Tax rate	Individual country's corporate tax rate
GDP	GDP	Annual Gross Domestic Product per capita
Inflation rate	INF	Rate of price change in the economy as a whole.
<b>Institutional Characteristics</b>		World Bank Enterprise Surveys- <a href="https://www.enterprisesurveys.org/employment-indicators">https://www.enterprisesurveys.org/employment-indicators</a>
Small firm	Small	Individual countries' average percentage of firms of which employees number below 20 (1-19).
Medium size firm	Medium	Individual countries' average percentage of firms of which employees' numbers are from 20 to 99.
Large size firm	Large	Individual countries' average percentage of firms of which employees' number are 100 or above.
The female manager at the top level	TMF	The average percentage of female in the top management of individual sample country's firms
Male manager at the top level	TMM	The average percentage of male at the top management of individual sample country's firms.
Manufacturing firms	Manufacturing	Percentage of firms in the manufacturing sector of each of the sample countries.
Services firms	Servicing	Percentage of firms in the service sector of each of the sample countries.

*Table 2. Descriptive statistics*

Variable	Obs.	Mean	Std. Dev.	Min	Max
TE	85	30.20	10.15	11.75	63.47
Small	85	23.51	12.51	1.6	73.02
Medium	85	34.24	10.10	7.33	60.52
Large	85	42.26	18.78	0.5	90.18
TMF	85	18.18	21.90	0.83	100
TMM	85	80.73	21.77	0.5	99.13
Manufacturing	85	44.13	17.53	8.12	96.12
Servicing	85	55.87	17.53	3.88	91.88
FBL	85	33.59	16.31	2.7	79.6
Solvent	85	46.23	14.18	6	84.6
BLFI	85	25.55	12.21	0.7	53.1
FCF	85	26.39	17.02	0.9	75
Age	85	16.16	4.42	8.2	28.3
DO	85	86.85	12.67	35.2	100
FO	85	12.66	12.65	0	73.3
GO	85	1.04	1.89	0	9.6
P	85	36.33	24.66	0.4	82
Familiar	85	18.83	10.64	0.7	53.4
Audit	85	49.11	21.44	7.8	96.1
FeO	85	33.98	14.11	4.2	69.2
TME	85	16.59	4.10	9.5	28.8
Size	85	39.35	26.70	10.6	184.9
Tax rate	85	38.64	13.54	12	84.5
GDP	85	6701.86	8231.56	243.1	53561.89
INF	85	5.44	5.95	-1.09	34.7

## RESULTS AND DISCUSSION

### Descriptive Analysis

Table 2 shows the descriptive analysis of 85 countries. In the level of tax evasion, a considerable diversity can be seen. The tax evasion among the sample countries ranges from 11.75% to 63.47% with a mean and standard deviation of 30.2% and 10.15% respectively. Most of the firms are controlled by the domestic ownership as their percentage of shares is 86.85% which is more than any other ownership. The descriptive statistics also show that the majority of the firms are solvent and not needing any loan as their percentage is 46.23. The majority of the firms of the sample countries are large (42.26%), while the number of small firms is in the lowest (23.51%). Most of the firms' top management is controlled by the male (80.73%), whereas the percentage of female managers in the top management is only 18.18%.

The percentage of services firms (55.87%) is higher than that of manufacturing firms (44.13%) in the sample countries. The tax evasion and all other factors highly vary among the countries as their standard deviation are too high.

## Correlations

Table 3 shows the pairwise correlation among variables. The findings show that firms needing bank loan (FBL), firms use bank loan as an investment (BLFI) and solvent firms have a negative relationship with tax evasion, while financially constraint firms (FCF) show positive correlations. The study also shows that domestic ownership (DO) has a negative correlation, while foreign ownership, government ownership and proprietorship have a positive correlation with tax evasion. Moreover, both the audit and familiarity have been found in a negative correlation with tax evasion. The results indicate that firms with more familiarity and more prolonged periods of top management reduce the level of tax evasion.

*Table 3a. Pairwise correlations*

	TE	FBL	Solvent	BLFI	FCF	Age	DO	FO
TE	1							
FBL	-0.399***	1						
Solvent	-0.256**	0.084	1					
BLFI	-0.328***	0.644***	0.065	1				
FCF	0.301***	-0.144	-0.68***	-0.057	1			
Age	-0.151	0.392***	0.153	0.396***	-0.165	1		
DO	-0.229**	0.078	0.077	0.135	-0.107	-0.056	1	
FO	0.208*	0.014	-0.035	-0.067	0.004	0.115	-0.903***	1
GO	0.353***	-0.305***	-0.134	-0.249**	0.083	-0.265**	-0.374***	0.297***
P	0.309***	-0.419***	-0.349***	-0.154	0.366***	0.049	-0.0781	-0.028
FeO	-0.136	0.307***	0.093	0.128	-0.208*	0.095	-0.336***	0.122
Familiar	-0.37***	0.162	0.255**	0.054	-0.458***	0.169	-0.051	0.211*
Audit	-0.148	0.296***	0.125	0.334***	-0.144	0.430***	-0.124	0.403***
TME	-0.293***	0.537***	0.141	0.343***	-0.164	0.659***	0.086	-0.008
Size	-0.151	0.239**	-0.002	0.094	-0.230**	0.412***	-0.136	0.204*
Tax rate	0.052	-0.206*	0.062	-0.044	-0.015	-0.056	-0.122	-0.006
GDP	-0.012	0.127	0.139	0.051	-0.128	0.063	0.063	0.003
INF	-0.009	-0.190*	0.120	-0.079	-0.116	-0.102	0.002	-0.078

\*  $p < 0.10$ , \*\*  $p < 0.05$ , \*\*\*  $p < 0.01$

## Firms' Characteristics and Tax Evasion

Table 3b. Pairwise correlations

	GO	P	Familiar	Audit	FeO	TME	Size	Tax rate	GDP	INF
GO	1									
P	0.174	1								
Familiar	0.040	-0.377***	1							
Audit	-0.147	0.028	0.125	1						
FeO	0.134	-0.269**	0.239**	0.280***	1					
TME	-0.284***	-0.298***	0.344***	0.295***	0.179	1				
Size	-0.106	-0.046	0.191*	0.163	0.056*	0.301*	1			
Tax rate	0.125	0.217**	0.096	0.021	-0.097	-0.019	-0.085	1		
GDP	0.027	-0.242**	0.075	0.066	0.176	0.130	-0.017	-0.053	1	
INF	0.082	0.198*	-0.250**	0.034	-0.026	-0.134	0.011	0.221**	-0.210*	1

\*  $p < 0.10$ , \*\*  $p < 0.05$ , \*\*\*  $p < 0.01$

## Multicollinearity Test

Further, the study conducted the Variance Inflation Factor (VIF) to check whether any multicollinearity problem in the variables existed. Multicollinearity occurs when the high correlations exist between the variables. No variable demonstrates the value of VIF more than the recommended level 10 (Hair, Anderson, Tatham, & Black, 1984). Therefore, the study has no multicollinearity problem in regression analysis.

## Regression Results

Table 5 shows the regression results of the study and OLS has been run to find out the relationship between tax evasion and firm characteristics. Among all characteristics, the study found that all types of firms' ownership have a substantial impact on tax evasion shown in column 1 and column 2 of Table 5. More specifically, the domestic (DO), foreign (FO) and government (GO) ownership show positive impact while female ownership (FeO) and proprietorship show a negative impact on tax evasion.

Domestic owners are freer to run their business, and they are not bound to anybody, for why they are not accountable to answer anyone about their cash flows. So, private domestic owners have more tendencies to evade tax. The negative relationship between foreign owners and tax evasion implies that foreign firms are more involved in tax evasion as they do not think about the country where they do business and only think about their profit. They may shift their profits to their own countries, hiding actual income for tax evasion. This result is consistent with the study of Annuar *et al.* (2014) evidenced a positive relationship between foreign ownership and tax evasion since foreign-owned firms use profit-shifting strategies to reduce their tax liabilities (Preuss, 2010).

Government-owned firms also have a positive effect on tax evasion, as the government does not manage the firms directly. For that in the government-owned firms, the managers hold the same position after years, and they know well how to hide their activities from government and tax authorities. Also, the result of tax audits cannot be feasible because of their political connections in many firms (Salihu *et al.*, 2015).

*Table 4. Regression results*

		(1)	(2)	(3)	(4)	(5)
	VIF	TE	TE	TE	TE	TE
DO	7.17	0.1607** (0.0685)	0.2636*** (0.0852)	0.6809*** (0.0605)	0.2262*** (0.0644)	-0.1533 (0.0950)
FO	6.92	0.4360*** (0.0513)	0.3264*** (0.0845)	0.7338*** (0.0481)	0.2909** (0.1321)	-0.0676 (0.0916)
GO	1.47	0.9564*** (0.1697)	1.3885*** (0.2710)	3.3463*** (0.2302)	1.3721*** (0.3018)	1.2842*** (0.2275)
P	2.03	-0.1404** (0.0600)	-0.0530** (0.0262)	-0.2123*** (0.0189)	-0.0556* (0.0305)	-0.2153*** (0.0184)
FeO	1.61	-0.0448 (0.0382)	-0.0975 (0.0848)	-0.2997*** (0.0217)	-0.1023* (0.0565)	-0.2343*** (0.0280)
Age	2.96	1.3029*** (0.2567)	1.5307*** (0.1711)	0.8114*** (0.1684)	1.4620*** (0.2034)	0.7266*** (0.1976)
Size	1.48	-0.0549*** (0.0145)	-0.0676*** (0.0108)	0.0163 (0.0104)	-0.0576*** (0.0190)	0.0770*** (0.0230)
Tax rate	1.34	0.0979 (0.0604)	0.1223*** (0.0313)	0.0936*** (0.0286)	0.1325*** (0.0388)	0.0295 (0.0311)
GDP	1.19	-0.0000 (0.0001)	-0.0001 (0.0001)	-0.0002*** (0.0001)	-0.0001 (0.0000)	-0.0001 (0.0001)
INF	1.43	-0.0911 (0.1083)	-0.1037 (0.1279)	-0.0355 (0.0569)	-0.1216 (0.1292)	0.0520 (0.1017)
Audit	1.49	-0.0642* (0.0366)	-0.0782*** (0.0278)	0.1098*** (0.0195)	-0.0950*** (0.0244)	0.1300*** (0.0314)
Familiar	1.87	-0.3425*** (0.0750)	-0.3144*** (0.1037)	-0.1284*** (0.0313)	-0.3031*** (0.0581)	-0.1468*** (0.0424)
Solvent	2.23	-0.1144** (0.0566)	-0.0912 (0.0678)	0.1323** (0.0551)	-0.0920 (0.0571)	0.0864 (0.0644)
BLFI	1.96		-0.1147 (0.0886)			
FBL	2.83	-0.6205*** (0.0476)	-0.6072*** (0.0452)	-0.1341*** (0.0338)	-0.6549*** (0.0424)	-0.1638*** (0.0503)
FCF	2.79	-0.0160 (0.0405)	0.0735* (0.0421)	0.2902*** (0.0404)	0.0621 (0.0394)	0.2489*** (0.0441)
TME	2.78	0.8335*** (0.2931)	0.8080*** (0.1605)	-0.7516*** (0.1473)	0.8172*** (0.2281)	-0.5760*** (0.1782)
Small				0.1437*** (0.0379)		
Medium					0.0065 (0.0633)	
Large						-0.1797*** (0.0351)
_cons		17.5555** (8.6323)	3.9802 (11.3003)	-41.1836*** (7.1869)	7.4194 (8.0445)	53.1209*** (12.4289)
N		85	85	85	85	85

Standard errors in parentheses

\*  $p < 0.10$ , \*\*  $p < 0.05$ , \*\*\*  $p < 0.01$

### ***Firms' Characteristics and Tax Evasion***

The study found a negative and significant relationship between proprietorship firms and tax evasion, not supporting the prior results (Alm *et al.*, 2016; Bornemann *et al.*, 2019). The result implies that the higher the solely owned business, the lower the possibility of tax evasion. For having sole ownership, proprietorship firms have more fear about punishment for illegal works like getting caught for tax evasion; they are not much able to tackle these things.

Similarly, as the women are more risk-averse than male, they would not like to be involved with tax evasion; their negative feeling to illegal activities prevents them from tax evasion. Moreover, since the female-owned firms have the lower possibility in hiding income and sheltering tax as well, the negative relationship between female ownership tax evasion supports the prior findings (Bornemann *et al.*, 2019; Francis *et al.*, 2014).

During the investigation of funding behaviour, the study found a negative effect of solvent firms and firms with access to bank loans on tax evasion. The findings show that the firms which have accessibility in bank loan are not likely to be involved with tax evasion as they can manage their investment and working capitals whenever they required. Additionally, the solvent firms can manage their funds from internal sources; they have a negative impact on tax evasion. The findings offer an insight that with increasing the number of solvent firms, the level of tax evasion decreases as their cost of capital is less than others. On the contrary, the study found a positive effect of financially constraint firms (FCF) on tax evasion. The result supports the finding of Alm *et al.* (2019) in which they documented that financial constraints firms are more likely to be involved in tax evasion than the solvent ones. Because of financial constraints, firms cannot get easy access to loans and cannot gather necessary capital; it hampers investment decisions. Therefore, the firms find tax evasion is a way to increase their necessary capital.

Further, the results show that familiar firms with international recognition do not tend to evade tax as a negative relationship has been found between familiarity and tax evasion. Internationally recognized firms pay much attention to hold up their position and reputation in the market. Therefore, they would not like to be involved in such kind of illegal activities which can harm their reputation. Therefore, the study documented that the firms which have higher familiarity and international recognition worldwide have lesser the possibility to evade tax.

Similarly, the firms audited by external auditors do not tend to evade tax as a negative relationship exists between audit and tax evasion. Similar results also found by Huseynov & Klamm (2012) and Hudori and Mustikasari (2020), where they commented that a true and fair view of the financial statement by the external auditors reduces tax evasion to a great extent. Furthermore, the study of Chen *et al.* (2019) documented that firms try to shelter their income and decide to evade tax only if it is proved that the tax authorities do not perform the investigation. Therefore, the government should make it compulsory to check the financial statements of the firms by the external auditors, which, in turn, reduces the firms' tax evasion.

Furthermore, the study has investigated the impact of firm size and age on tax evasion. The study found a negative relationship between firm size and tax evasion. The results provide a realization that larger the firm size, lower the possibility of tax evasion. On the other hand, the age of the firms has a positive effect on tax evasion as more experienced firms have more knowledge about the loopholes in tax evasion. Moreover, they can manage the risk where non-experienced firms do not want to take this risk of evasion and thereby getting caught at the starting of business. So, the more aged firms should be under the inspection of government, and thus tax evasion can be under control. Top-level management experience also shows a positive impact on tax evasion. The results indicate that if the top-level management (TME) holds up the same position for a longer period in the same firm, the firms tend to

evade tax. Though, in some other models, TME shows a negative relationship with tax evasion; these results are due to the impact of institutional characteristics.

Finally, the study examined the effect of economic factors such as tax rate, inflation (INF) and GDP on tax evasion. The study found a substantial impact of tax rate and tax evasion. When the tax rate is too high to bear by the taxpayers, they may feel discouraged from paying taxes properly. Therefore, the government should reduce its corporate tax rate to an optimum level. On the other hand, inflation and GDP show a mixed result; some models show a positive impact, while other models show an insignificant impact on tax evasion. Therefore, the government should keep inflation as balanced as it does affect sound decision-making. Otherwise, the high level of inflation in an economy may increase the firms' level tax evasion. Unlikely, the GDP shows a negative effect on some models, which means higher the GDP, lower the level of tax evasion.

### **Additional Tests**

In Table 5, column 3, 4 and 5 represents the impact of different firm sizes on tax evasion. The small firms are positively significant with tax evasion, while large firms are negatively significant and medium-sized firms have no relationship with tax evasion. The results indicate that the greater the number of small firms' size, the higher the level of tax evasion. On the other hand, the higher the number of large firms' size, the lower the possibility of tax evasion. The results are highly consistent in line with the study of Payne and Saunoris (2020). The study shows that both the small and medium firms are highly motivated by both the domestic and foreign shareholders to evade tax while large firms are influenced by government ownership towards tax evasion.

Additionally, small firms are in demand of gaining more profit; they evade tax to increase cash flows even though they are solvent. Moreover, they do not get quick access to loan procedures like large firms. On the contrary, large firms get easy access to loans and other financial bits of help from banks, and they get more tax exemptions due to significant allowable investments and CSR contributions; as a result, they have fewer tendencies to evade tax.

In columns 6 and 7 of Table 5, the study shows a negative relationship between female management at the top level and tax evasion. In contrast, a positive relationship has been noticed between top-level male managers and tax evasion in column 7. These results indicate that higher the female participation in top-level management of a firm, lower the possibility of tax evasion. On the contrary, higher the male participation at the top-level management implies higher the possibility of tax evasion. These results happen as the top management experience, and government ownership influence the male manager than that of the female. Also, another reason of negative association between firms with female managers at the top level and tax evasion is that they are more risk-averse of getting caught than males; they show no propensity to evade tax as a result.

Finally, columns 8 and 9 show the impact of industry category on tax evasion. The study found no significant impact of servicing and manufacturing industries on tax evasion. Nevertheless, when a further model, model 10 was run dropping FCF, the results show a negative relation between manufacturing firms and tax evasion. This result indicates that manufacturing firms may have fewer tendencies to evade tax despite having financial constraints. Moreover, when the tax rate goes up, the manufacturing firms attempt to evade tax than that of servicing firms, as the finding shows a significant and positive relationship between tax rate and tax evasion (Javorcik & Demir, 2019). On the other hand, the tax rate is not a matter for servicing industries; they can easily manage it form the customers than the manufacturing ones.

# **Firms' Characteristics and Tax Evasion**

*Table 5. OLS Results (additional tests)*

	(6)	(7)	(8)	(9)	(10)
	TE	TE	TE	TE	TE
DO	0.1081* (0.0634)	0.1874*** (0.0629)	0.7370*** (0.0943)	0.4810*** (0.0803)	0.6383* (0.3377)
FO	0.1070* (0.0616)	0.2143*** (0.0481)	0.6511*** (0.0478)	0.5762*** (0.0725)	0.5471* (0.3244)
GO	-0.2135 (0.2063)	1.2402*** (0.1596)	0.2600 (0.5065)	2.9198*** (0.2188)	-0.0554 (0.2864)
P	0.1150*** (0.0298)	-0.0690** (0.0265)	-0.1517*** (0.0190)	0.1224*** (0.0252)	-0.1338*** (0.0454)
FeO	0.0655 (0.0470)	-0.0982* (0.0581)	-0.2097*** (0.0344)	0.0588* (0.0307)	-0.1916*** (0.0277)
Age	-0.5195*** (0.1466)	1.5204*** (0.1927)	0.7725*** (0.2832)	0.4837*** (0.0816)	1.0027*** (0.3242)
Size	0.1014*** (0.0221)	-0.0500*** (0.0084)	0.0167 (0.0141)	0.1251*** (0.0244)	0.0138 (0.0191)
Tax rate	0.0947*** (0.0341)	0.1595*** (0.0353)	0.1331 (0.1059)	0.0840** (0.0398)	0.1998*** (0.0449)
GDP	0.0002*** (0.0000)	-0.0001* (0.0000)	0.0001 (0.0001)	0.0001*** (0.0000)	0.0001*** (0.0001)
INF	-0.1195 (0.0854)	-0.1555 (0.1092)	0.3961*** (0.1175)	0.0734 (0.1042)	0.3043*** (0.1100)
Audit	-0.0070 (0.0234)	-0.0738*** (0.0197)	0.1176*** (0.0260)	-0.2607*** (0.0376)	0.1002*** (0.0321)
Familiar	-0.2325*** (0.0558)	-0.2769*** (0.0683)	-0.0813 (0.0532)	-0.6530*** (0.0558)	-0.0865 (0.0667)
Solvent	-0.3490*** (0.0649)	-0.0504 (0.0584)	-0.2497** (0.1108)	-0.1491*** (0.0273)	-0.3443*** (0.0584)
FBL	-0.1339*** (0.0399)	-0.6160*** (0.0807)	-0.0836* (0.0422)	-0.0655** (0.0294)	-0.1243*** (0.0465)
FCF	-0.1376** (0.0569)	0.0758 (0.0555)	0.0990 (0.0812)	-0.1535** (0.0600)	
TME	0.0923 (0.1164)	0.5246*** (0.1975)	-0.8837*** (0.2753)	0.6532*** (0.1186)	-0.9496*** (0.3156)
TMF	-0.0692*** (0.0202)				
TMM		0.0567 (0.0544)			
Service			0.0925 (0.0567)		
Manufacturing				-0.0465 (0.0324)	-0.1690*** (0.0553)
_cons	42.4673*** (9.1950)	5.1337 (8.9877)	-33.5397*** (11.5460)	-15.4719 (10.5793)	-6.9037 (36.2274)
N	85	85	85	85	85

Standard errors in parentheses

\*  $p < 0.10$ , \*\*  $p < 0.05$ , \*\*\*  $p < 0.01$



## **CONCLUSION**

Since firms indeed play the most dynamic roles in the countries' economies, the economy will be weak if the firms evade tax, which will ultimately affect the overall economy and firms' future conditions as well. This study draws an analysis on the impact of firms' characteristics on firm tax evasion across the world. Many factors of firms' characteristics, including ownership structure, funding behaviour, audit, familiarity, industry types, have been used to determine the impact of tax evasion. The result has shown substantial evidence that several firms' characteristics have a significant impact on firms' tax evasion across countries. Firms with more domestic, foreign, government ownership have more tendencies to evade tax, while with increasing the sole proprietorship and female-owned firms, the level of tax evasion decreases. The firms with financial constraints evade more tax than the solvent ones, as the solvent firms decrease the level of tax evasion. Audit and familiarity are also crucial at the firm level as they decrease tax evasion. Tax rate and inflation should be controlled in such a way as they did not instigate firms to evade tax as higher the tax rate and inflation increase greater the level of tax evasion.

This study has some implications across the countries which may be used for all kind of firms. First, the governments, tax authorities and regulatory bodies can know a variety of factors that play a role in reducing the tax collection capacity at the firm level. They can take necessary strategic plans and implement firms level policies to reduce tax evasion. Second, the firms should maintain a balance among the ownership structures so that tax evasion can be decreased. More specifically, the study suggests reducing the domestic, foreign and government ownership and increasing the female and sole ownership business. Third, governments and regulatory bodies should take necessary steps so that the firms can manage their funds at a cheap rate of interest under easy collateral. Forth, countries' governments should be more aware of the firms that evade tax, and enforcement initiatives must be taken against them so that they can be controlled to a certain level. Finally, a firm is not only a profit motive, but also, they are intended to gain the faith of their customers, so they will keep them far away from tax evasion as it is treated illegal activity. If tax evaders are caught and punished once, they will reduce their reputations and thereby lose customers' faith. Further, the study is expected to create an avenue for the researchers and academician, it, in turn, helps them to investigate more firms' characteristics which are responsible for tax evasion.

The study has several limitations. First, this paper uses the shadow economy as a proxy of tax evasion as it is difficult to measure the actual amount of tax evasion. As firms have some internal policy not to share their information with others; a true finding may be biased. Second, the study conducted a cross-country investigation with cross-sectional country-level data due to data unavailability; it may not represent the proper picture of the relationship between firms' characteristics and tax evasion. Future researchers may consider firm-level panel data with large sample size. Finally, limited research on the firms' characteristics and tax evasion will motivate future researchers to explore more other factors of tax evasion.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

- Abdixhiku, L., Pugh, G., & Hashi, I. (2018). Business tax evasion in transition economies: A cross-country panel investigation. *The European Journal of Comparative Economics*, 15(1), 11–36.
- Allingham, M. G., & Sandmo, A. (1972). Income tax evasion: A theoretical analysis. *Journal of Public Economics*, 1(3-4), 323–338. doi:10.1016/0047-2727(72)90010-2
- Alm, J., Liu, Y., & Zhang, K. (2019). Financial constraints and firm tax evasion. *International Tax and Public Finance*, 26(1), 71–102. doi:10.1007/10797-018-9502-7
- Alm, J., Martinez-Vazquez, J., & McClellan, C. (2016). Corruption and firm tax evasion. *Journal of Economic Behavior & Organization*, 124, 146–163. doi:10.1016/j.jebo.2015.10.006
- Annuar, H. A., Salihu, I. A., & Obid, S. N. S. (2014). Corporate ownership, governance and tax avoidance: An interactive effects. *Procedia: Social and Behavioral Sciences*, 164, 150–160. doi:10.1016/j.sbspro.2014.11.063
- Atwood, T., & Lewellen, C. (2019). The complementarity between tax avoidance and manager diversion: Evidence from tax haven firms. *Contemporary Accounting Research*, 36(1), 259–294. doi:10.1111/1911-3846.12421
- Banerjee, A. V., & Duflo, E. (2014). Do firms want to borrow more? Testing credit constraints using a directed lending program. *The Review of Economic Studies*, 81(2), 572–607. doi:10.1093/restud/rdt046
- Beck, T., Lin, C., & Ma, Y. (2014). Why do firms evade taxes? The role of information sharing and financial sector outreach. *The Journal of Finance*, 69(2), 763–817. doi:10.1111/jofi.12123
- Benczúr, P., Kátay, G., & Kiss, Á. (2018). Assessing the economic and social impact of tax and benefit reforms: A general-equilibrium microsimulation approach applied to Hungary. *Economic Modelling*, 75, 441–457. doi:10.1016/j.econmod.2018.06.016
- Besley, T., Jensen, A., & Persson, T. (2019). Norms, enforcement, and tax evasion (No. w25575). National Bureau of Economic Research.

- Blackburn, K., Bose, N., & Capasso, S. (2012). Tax evasion, the underground economy and financial development. *Journal of Economic Behavior & Organization*, 83(2), 243–253. doi:10.1016/j.jebo.2012.05.019
- Bornemann, T., Jacob, M., & Sailer, M. (2019). *Do Corporate Taxes Affect Executive Compensation?* Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3403486](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3403486)
- Capasso, S., & Santoro, L. (2016). *The determinants of the contract of corruption: Theory and Evidence* (Working Paper No. 429). Naples: Centre For Studies in Economics and Finance.
- Carrillo, P., Pomeranz, D., & Singhal, M. (2017). Dodging the taxman: Firm misreporting and limits to tax enforcement. *American Economic Journal. Applied Economics*, 9(2), 144–164. doi:10.1257/app.20140495
- Chen, Y., Ge, R., Louis, H., & Zolotoy, L. (2019). Stock liquidity and corporate tax avoidance. *Review of Accounting Studies*, 24(1), 309–340. doi:10.1007/11142-018-9479-6
- Crane, S. E., & Nourzad, F. (1986). Inflation and tax evasion: An empirical analysis. *The Review of Economics and Statistics*, 68(2), 217–223. doi:10.2307/1925500
- Crocker, K. J., & Slemrod, J. (2005). Corporate tax evasion with agency costs. *Journal of Public Economics*, 89(9-10), 1593–1610. doi:10.1016/j.jpubeco.2004.08.003
- Desai, M. A. (2005). The degradation of reported corporate profits. *The Journal of Economic Perspectives*, 19(4), 171–192. doi:10.1257/089533005775196705
- Doerrenberg, P., & Duncan, D. (2019). *How does firm tax evasion affect prices?* Universität Mannheim. Retrieved from <https://madoc.bib.uni-mannheim.de/47857/>
- Dyreng, S. D., Hanlon, M., & Maydew, E. L. (2018). When does tax avoidance result in tax uncertainty? *The Accounting Review*, 94(2), 179–203. doi:10.2308/accr-52198
- Francis, B. B., Hasan, I., Wu, Q., & Yan, M. (2014). Are female CFOs less tax aggressive? Evidence from tax aggressiveness. *The Journal of the American Taxation Association*, 36(2), 171–202. doi:10.2308/atax-50819
- Gatsi, J. G., Gadzo, S. G., & Kporgbi, H. K. (2013). The effect of corporate income tax on financial performance of listed manufacturing firms in Ghana. *Research Journal of Finance and Accounting*, 4(15), 118–124.
- Gupta, R. (2008). Tax evasion and financial repression. *Journal of Economics and Business*, 60(6), 517–535. doi:10.1016/j.jeconbus.2007.10.002
- Gupta, R. P., & Biswas, B. (2021). Banking Scams in India: A Case Based Analysis. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Hair, J., Anderson, R. E., Tatham, R. L., & Black, W. (1984). *Multivariate data analysis*. Petroleum Publishing.
- Hardeck, I., Inger, K., Moore, R., & Schneider, J. (2019). *Cross-Cultural Evidence on Tax Disclosures in CSR Reports—A Textual Analysis Approach*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3308467](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3308467)

- Hasan, I., Hoi, C. K. S., Wu, Q., & Zhang, H. (2014). Beauty is in the eye of the beholder: The effect of corporate tax avoidance on the cost of bank loans. *Journal of Financial Economics*, 113(1), 109–130. doi:10.1016/j.jfineco.2014.03.004
- Hoseini, M., Gerayli, M. S., & Valiyan, H. (2019). Demographic characteristics of the board of directors' structure and tax avoidance. *International Journal of Social Economics*, 46(2), 199–212. doi:10.1108/IJSE-11-2017-0507
- Hudori, R., & Mustikasari, E. (2020). The Strength of Audits, Reporting Standards and Corruption, on Tax Evasion: A Cross-Country Study. *International Journal of Economics & Business Administration*, 8(2), 554–567. doi:10.35808/ijebe/481
- Huseynov, F., & Klamm, B. K. (2012). Tax avoidance, tax management and corporate social responsibility. *Journal of Corporate Finance*, 18(4), 804–827. doi:10.1016/j.jcorpfin.2012.06.005
- Irianto, B. S., Sudibyo, Y. A., & Wafirli, A. (2017). The Influence of Profitability, Leverage, Firm Size and Capital Intensity Towards Tax Avoidance. *International Journal of Accounting and Taxation*, 5(2), 33–41. doi:10.15640/ijat.v5n2a3
- Islam, A., Rashid, M. H. U., Hossain, S. Z., & Hashmi, R. (2020). Public policies and tax evasion: Evidence from SAARC countries. *Heliyon (London)*, 6(11). Advance online publication. doi:10.1016/j.heliyon.2020.e05449
- Jayasekara, S. F. S. D. (2021). Risk-based AML/CFT Regulations for Effective Supervision. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Johnson, S., Kaufmann, D., McMillan, J., & Woodruff, C. (2000). Why do firms hide? Bribes and unofficial activity after communism. *Journal of Public Economics*, 76(3), 495–520. doi:10.1016/S0047-2727(99)00094-8
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Khelif, H., & Guidara, A. (2018). Quality of management schools, strength of auditing and reporting standards and tax evasion. *EuroMed Journal of Business*, 13(2), 149–162. doi:10.1108/EMJB-05-2017-0017
- McGee, R. W., & Preobragenskaya, G. G. (2006). The ethics of tax evasion: A survey of Romanian business students and faculty. *Accounting and Financial Systems Reform in Eastern Europe and Asia*, 299–334.
- Mitra, S. (2017). To tax or not to tax? When does it matter for informality? *Economic Modelling*, 64, 117–127. doi:10.1016/j.econmod.2017.02.024
- Nafti, O., Kateb, I., & Masghouni, O. (2020). Tax evasion, firm's value and governance: Evidence from Tunisian Stock Exchange. *Journal of Financial Crime*, 27(3), 781–799. doi:10.1108/JFC-02-2020-0023
- Nur-tegin, K. D. (2008). Determinants of business tax compliance. *The B.E. Journal of Economic Analysis & Policy*, 8(1), 1–26. doi:10.2202/1935-1682.1683

- Payne, J. E., & Saunoris, J. W. (2020). Corruption and Firm Tax Evasion in Transition Economies: Results from Censored Quantile Instrumental Variables Estimation. *Atlantic Economic Journal*, 48(2), 195–206. doi:10.1007/11293-020-09666-2
- Preuss, L. (2010). Tax avoidance and corporate social responsibility: You can't do both, or can you? *Corporate Governance: International Journal of Business in Society*, 10(4), 365–374. doi:10.1108/14720701011069605
- Rafay, A., & Ajmal, M. M. (2014). Earnings Management through Deferred Taxes Recognized under IAS 12: Evidence from Pakistan. *Lahore Journal of Business*, 3(1), 1–19. doi:10.35536/ljb.2014.v3.i1.a1
- Rafay, A., Sadiq, R., & Ajmal, M. M. (2016). The Effect of IAS-24 Disclosures on Governance Mechanisms and Ownership Structures in Pakistan. *Lahore Journal of Business*, 5(1), 15–36. doi:10.35536/ljb.2016.v5.i1.a2
- Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.
- Rashid, M. H. U. (2020). Taxpayer's Attitude Towards Tax Evasion in a Developing Country: Do the Demographic Characteristics Matter? *International Journal of Applied Behavioral Economics*, 9(2), 1–19. doi:10.4018/IJABE.2020040101
- Salihu, I. A., Annuar, H. A., & Obid, S. N. S. (2015). Foreign investors' interests and corporate tax avoidance: Evidence from an emerging economy. *Journal of Contemporary Accounting & Economics*, 11(2), 138–147. doi:10.1016/j.jcae.2015.03.001
- Schneider, F., & Buehn, A. (2012). *Shadow economies in highly developed OECD countries: What are the driving forces?* Retrieved from <https://www.econstor.eu/bitstream/10419/67170/1/727543865.pdf>
- Schneider, F., Buehn, A., & Montenegro, C. E. (2010). *Shadow economies all over the world: New estimates for 162 countries from 1999 to 2007* (Working Paper No. 5356). Washington, DC: World Bank Group.
- Schneider, F., Raczkowski, K., & Mróz, B. (2015). Shadow economy and tax evasion in the EU. *Journal of Money Laundering Control*, 18(1), 34–51. doi:10.1108/JMLC-09-2014-0027
- Sharma, C., & Mitra, A. (2015). Corruption, governance and firm performance: Evidence from Indian enterprises. *Journal of Policy Modeling*, 37(5), 835–851. doi:10.1016/j.jpolmod.2015.05.001
- Sinha, A. (2021). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Slemrod, J. (2007). Cheating ourselves: The economics of tax evasion. *The Journal of Economic Perspectives*, 21(1), 25–48. doi:10.1257/jep.21.1.25
- Torgler, B., & Schneider, F. (2007). *Shadow economy, tax morale, governance and institutional quality: a panel analysis* (Working Paper, No. 1923). Center for Economic Studies and ifo Institute (CESifo), Munich. Retrieved from <https://www.econstor.eu/bitstream/10419/25968/1/538033703.PDF>

Tsakumis, G. T., Curatola, A. P., & Porcano, T. M. (2007). The relation between national cultural dimensions and tax evasion. *Journal of International Accounting, Auditing & Taxation*, 16(2), 131–147. doi:10.1016/j.intaccaudtax.2007.06.004

Umar, M. A., Derashid, C., Ibrahim, I., & Bidin, Z. (2019). Public governance quality and tax compliance behavior in developing countries: The mediating role of socioeconomic conditions. *International Journal of Social Economics*, 46(3), 338–351. doi:10.1108/IJSE-11-2016-0338

Yamen, A., Allam, A., Bani-Mustafa, A., & Uyar, A. (2018). Impact of institutional environment quality on tax evasion: A comparative investigation of old versus new EU members. *Journal of International Accounting, Auditing & Taxation*, 32, 17–29. doi:10.1016/j.intaccaudtax.2018.07.001

Zhang, L., Chen, Y., & He, Z. (2018). The effect of investment tax incentives: Evidence from China's value-added tax reform. *International Tax and Public Finance*, 25(4), 913–945. doi:10.1007/10797-017-9475-y

## **ENDNOTE**

<sup>1</sup> Indicates loan interest and other formality costs.

## APPENDIX

Table 6. Tax evasion score for sample countries

SL	Countries	TE Score	No. of Firms	SL	Countries	TE Score	No. of Firms
1	Albania (2013)	25.68	360	44	Latvia (2013)	16.68	336
2	Angola (2010)	36.54	360	45	Lebanon (2013)	27.96	561
3	Armenia (2013)	34.56	360	46	Lithuania (2013)	18.3	270
4	Azerbaijan (2013)	42.26	390	47	Madagascar (2013)	46.27	532
5	Bahamas, (2010)	37.77	150	48	Malawi (2014)	34.28	523
6	Bangladesh (2013)	28.22	1442	49	Malaysia (2015)	26.07	1000
7	Belarus (2013)	34.07	360	50	Mauritania (2014)	24.38	150
8	Belize (2010)	45.51	150	51	Mauritius (2009)	21.18	398
9	Bhutan (2015)	20.28	253	52	Mexico (2010)	31.15	1480
10	Bosnia and Herzegovina (2013)	33.18	360	53	Moldova (2013)	39.26	360
11	Botswana (2010)	26.44	268	54	Mongolia (2013)	13.04	360
12	Brazil (2009)	36.9	1802	55	Morocco (2013)	29.79	407
13	Bulgaria (2013)	22.37	293	56	Mozambique (2007)	33.53	479
14	Burkina Faso (2009)	35.64	394	57	Namibia (2014)	22.85	580
15	Burundi (2014)	36.25	157	58	Nepal (2013)	33.46	482
16	Cabo Verde (2009)	31.48	156	59	Nigeria (2014)	50.64	2676
17	Central African Republic (2011)	36.94	150	60	Pakistan (2013)	30.62	1247
18	Chile (2010)	14.06	1033	61	Papua New Guinea (2015)	35.16	65
19	China (2012)	12.41	2700	62	Philippines (2015)	28.04	1335
20	Congo, Dem. Rep. (2013)	45.65	529	63	Poland (2013)	18.86	542
21	Congo, Rep. (2009)	40.65	151	64	Romania (2013)	23.97	540
22	Costa Rica (2010)	24.6	538	65	Russian Federation (2012)	31.88	4220
23	Croatia (2013)	25.28	360	66	Rwanda (2011)	29.53	241
24	Czech Republic (2013)	11.79	254	67	Senegal (2014)	35.91	601
25	Dominica (2010)	30.71	150	68	Slovak Republic (2013)	11.75	268
26	Eritrea (2009)	44.45	179	69	Slovenia (2013)	23.02	270
27	Estonia (2013)	17.97	273	70	Solomon Islands (2015)	30.89	151
28	Ethiopia (2015)	25.1	848	71	South Africa (2007)	21.81	937
29	Fiji (2009)	33.48	164	72	Sri Lanka (2011)	39.33	610
30	Gabon (2009)	63.47	179	73	Suriname (2010)	25.18	152
31	Georgia (2013)	56.57	360	74	Sweden (2014)	11.88	600
32	Ghana (2013)	39.25	720	75	Tajikistan (2013)	39.63	359
33	Guinea-Bissau (2006)	40.4	159	76	Tanzania (2013)	44.04	813

*continues on following page*

# ***Firms' Characteristics and Tax Evasion***

*Table 6. Continued*

SL	Countries	TE Score	No. of Firms	SL	Countries	TE Score	No. of Firms
34	Guyana, CR (2010)	28.73	165	77	Trinidad and Tobago (2010)	29.85	370
35	Hungary (2013)	21.63	310	78	Tunisia (2013)	32.94	592
36	India (2014)	18.33	9281	79	Turkey (2015)	27.33	6006
37	Indonesia (2015)	21.76	1320	80	Uganda (2013)	32.46	762
38	Israel (2013)	19.9	483	81	Ukraine (2013)	39.99	1002
39	Jamaica (2010)	36.92	376	82	Venezuela, R.B. (2010)	33.5	320
40	Jordan (2013)	14.64	573	83	Vietnam (2015)	14.78	996
41	Kazakhstan (2013)	30.77	600	84	Yemen, Rep. (2013)	31.07	353
42	Kenya (2013)	29.99	781	85	Zambia (2013)	30.83	720
43	Kyrgyz Republic (2013)	31.35	270				



Section 6

# Technology and Financial Crimes

# Chapter 23

## Regulations for Cybercrimes: The Case of the EU Cybersecurity Act

**Delphine Defosse**

*Northumbria University, UK*

### ABSTRACT

*The internet has made all types of information readily available, and this wealth of knowledge has opened up a whole new world of problems: cybercrimes. Despite the enactments of various legislation at both national and international level, cybercriminals are still mostly unpunished. The continued development of new technologies and mechanisms to protect anonymity on the Internet makes finding any response much harder. The lack of a common definition further impedes the finding of a global solution to eradicate the phenomenon. This creates an enforcement gap that allows cybercriminals to operate with near impunity. Over the years, the EU has taken steps to develop an adequate legal framework to strengthen the existing legislation. This chapter discussed that in EU, the adoption of The Cybersecurity Act 2019 would be enough to resolve some of the lingering issues of cybercrimes.*

### INTRODUCTION

Technology has provided new ways of solving old problems and sharing information in a faster manner. The Internet has made all types of information readily available, and this wealth of knowledge has opened up a whole new world of problems: *cybercrimes*.

Cybercrime is one of the biggest challenges facing humanity, with enormous economic impact. While the economic impact of illegal activity on the internet is difficult to quantify, according to a 2018 report by the Center for Strategic & International Studies, funded by McAfee, the estimated costs worldwide are \$600 billion annually (Lewis, 2018).

Cybercrime does not only represent one of the greatest threats to all enterprises, but it also has a significant impact on society as a whole. From minor romance scams targeting elderly to major data breaches involving personal information from millions, everyone is a potential target of cybercrimes. As Lewis (2018) noted, “Cybercrime is relentless, undiminished, and unlikely to stop. It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low”.

DOI: 10.4018/978-1-7998-5567-5.ch023

This perception of punishment being rare is due to the fact that cybercrimes threaten and violate all the implicit assumptions on which traditional laws are based. Even so, governments are applying ‘traditional’ laws to cybercrimes. The cyberspace is, however, borderless and indifferent to a person poaching data from another (Rho, 2007). Regulating such space with traditional legislations is bound to fail, as new types of crimes require new approaches. In fact, cybercrimes create a systemic risk, as more and more devices are connected to the Internet, expanding the playing field of cybercriminals and rendering such machines more vulnerable.

Although cybercrimes are not a new phenomenon, regulation is still in its infancy. As a report of McConnell International LLC (2000) highlighted, “*undeterred by the prospect of arrest or prosecution, cybercriminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations’ security*”. While governments have enacted anti-cybercrime laws, the inability of national law enforcement agencies, in the past, to make any significant advancement in catching and prosecuting cybercriminals, has been criticised. This inability is mainly due to the lack of any truly cohesive policy and law. As a result, the international community felt the urge to introduce sanctions and measures to protect the user and rights, with more or less success.

Despite the enactments of various legislation at both national and international level, cybercriminals are still mostly unpunished. The continued development of new technologies and mechanisms to protect anonymity on the Internet makes finding any response much harder. The lack of a common definition further impedes the finding of a global solution to eradicate the phenomenon. Indeed, not having a uniform definition impacts not only the enactment of cybercrimes laws at the national level but also international cooperation. This creates an enforcement gap that allows cybercriminals to operate with near impunity.

Over the years, the EU has taken steps to develop an adequate legal framework to address the challenges posed by cybercrime. Two main instruments were adopted: The Council Framework Decision 2005/222 (2005) on attacks against information systems and the Directive 2013/40/EU (2013) on attacks against information systems. To strengthen the existing legal framework and enhance the security of networks and information systems, the Cybersecurity Act was adopted in 2019. The Act gives the European Union Agency for Cybersecurity (ENISA) a permanent mandate and strengthens its role in prevention, advice, and cooperation. While it is not, *per se*, intended to deal with cybercrimes, ENISA increased mandate could resolve some of the lingering issues, but would it be enough?

## **1. CYBERCRIMES: CONCEPTUAL UNDERSTANDING**

### **1.1. Overview**

*We might not officially know what cybercrime is, but everyone is talking about it. Even without a dictionary definition, legislators and law enforcers all over the world seem to believe of cybercrime that they “know it when they see it,” as U.S. Supreme Court Justice Potter Stewart said of obscenity in 1964. Laws that address online crime are being passed in all jurisdictions, and those who make and enforce the laws are, after a slow start, springing into action to address the problem. (Littlejohn Shinder, 2002).*

Cybercrime is an umbrella term used to describe two distinct but yet closely related activities, cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crimes primarily cover acts that

are directed against computers or network resources, while cyber-enabled crimes are traditional crimes committed over the cyberspace, such as theft, fraud, and forgery (Opukri & Imomotimi Ebienfa, 2013).

Due to this dichotomy, no globally accepted definition encompassing all the facet of cybercrimes has ever been reached. Instead, a variety of definitions coexist, which can be divided into two groups: the narrow and the broad definition. While a single definition has not been reached, cybercrime is generally defined as a subcategory of computer crime.

This recurring definitional problem, paired with the quick changes occurring over the cyberspace, makes it difficult to enact effective legislations to combat cybercrimes. Indeed, approaching cybercrimes as merely the online counterpart of traditional crimes is too simplistic of an approach to a complex problem. While most cybercrimes have their traditional crimes counterparts, the fast growth of the cyberspace allows for even more innovative crimes. At the same time, the issues regarding the definition of some phenomena in the 'real world' are identical in the cyberspace. For instance, no common definition of terrorism (Saeed, Mubarik, & Zulfiqar, 2021; Sambo & Sule, 2021) at international level exists, making it harder to define cyberterrorism (Maghaireh, 2005; Opukri & Imomotimi Ebienfa, 2013).

Cybercrimes are a relatively new phenomenon, and governments often have problems grasping all the components involved. The earliest reported incidents occurred in the 1970s and involved employees altering files in computer databases or sabotaging computer systems to seek revenge against their employers. During that period, the world came to know and face the problem that hackers were creating. The media stories were mostly about teenagers breaking into computer systems, either as pranks or for malicious purposes. As a result, cybercrimes were initially regarded as traditional crimes committed through a computer, completely overlooking possible cyber-dependent crimes.

The picture is not as black and white as it seems. Indeed, a computer can play an incidental role in the commission of a traditional offence. For instance, blackmail letters that are written on a computer but are sent through the post or left at someone's home or office. In this case, the computer is neither the target nor the mean. Another example of a crime that sometimes is referred to as partly a cybercrime, a drug trafficker A that is shipping his drug to customer B by containers and tracking said 'delivery' through the post website. In such cases, the computer only serves an informational purpose and has a 'passive' role (Goodman, 1997).

### 1.2. Narrow Definitions

The narrow definition of cybercrime comes from early writings on the topic. Such early definitions have influenced most of the cybercrimes laws that were enacted before or in early 2000. One of the pioneers in computer writings, Parker (1976a) used the term 'computer abuse' "*because the word abuse allows him to avoid having to differentiate between what is a crime and what is not*" (Frelberger, 1981). He defined computer abuses as "*any incident associated with computer technology in which a victim suffered or could have suffered loss, and a perpetrator by intention made or could have made gain*" (Parker, 1976a). However, also as "*any international act in which one or more victims suffered or could have suffered a loss and one or more perpetrators made or could have made profit*" (Parker, 1976b). Relying on a similar idea, Kshetri analyses cybercrime in terms of cost-benefit to the offender. In his opinion, cybercrimes are crimes that use a computer network or Internet communication to commit an offence (Kshetri, 2006).

Others define cybercrime in terms of different categories based on the type of committed crime. For example, Forester and Morrison (1994) described computer crime as "*a criminal act that has been committed using a computer as the principal tool*". Power (2000) argues that most computer crimes involve

either fraud or abuse and sometimes both. He identifies computer fraud as “*computer-related crimes involving deliberate misrepresentation or alteration of data in order to get something of value*”. While computer abuse is defined as “*willful or negligent unauthorized activity that affects the availability, confidentiality or integrity of computer resources*”. He explained that computer abuse can include “*fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation.*”

Narrow definitions of cybercrime were reproducing an adapted version of traditional criminal laws to computer crimes. However, with the evolution of the phenomenon, Parker (1976b) realised that the narrow definition was not sufficient and adopted a new definition, which focused on the knowledge of computer technologies to commit computer-related crimes. (Jackson, Hruska, & Parker, 1992).

Smith, Grabosky, and Urban (2004) created a distinction between cybercrimes as a single word and cybercrimes as a descriptive term. In their opinion, the former encompasses “*new criminal offences perpetrated in new ways and the latter is conventional crimes perpetrated using new technologies*”. The distinction made by Smith, Grabosky, and Urban (2004) does not entirely reflect the reality, as a single offence could fall under both categories. Taking a simple example: one can forge an IP address to gain access to the Internet to carry a crime. In this case, there are two offences; the first crime would be a cybercrime, forgery of an IP address, and the second would be a cybercrime as a fraud on the Internet is a conventional crime perpetrated through new technologies, complicating the case even further.

Some international or regional instruments concern cybercrime only in the narrower conception of the computer system or data as the offence object.<sup>1</sup> For instance, some of the existing laws, such as the Convention on Cybercrime (also known as the Budapest Convention) have been drafted in late 1990 and early 2000 with mainly hackers in mind.<sup>2</sup> The Department of Justice of the United States (DOJ) defines computer crimes as “*any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution*” (Carter & Perry, 2004). This definition is narrow in the sense that it only includes traditional crimes perpetrated over the cyberspace or through the help of a computer, but it does not include new offences. Similarly, Title 18 of the U.S. Code, in Chapter 47, Section 1030, defines several fraudulent and related activities that can be prosecuted under federal law in connection with computers. At the same time, the wording is broad and vague, such as the word, prosecution.

In Australia, the definition given by the Australian Bankers’ Association (ABA) is less comprehensive. Indeed, cybercrime is defined as “*any crime effected or progressed using a public or private telecommunications service*”<sup>3</sup>. In the UK, the Association of Chief Police Officers (ACPO) has defined computer crimes as “*the use of networked computers, telephony or Internet technology, to commit or facilitate the commission of crime*” (UK Metropolitan Police Authority, 2007). This definition is consistent with the network-specific nature of the term, cybercrime.

The narrow definitions present two significant flaws; either profit is placed as the central motivation or based on existing offences carried out over the Internet. The problem with the first approach is that while most cyberattacks are influenced by profit, some are not. For instance, there are four commonly known reasons hackers hack; revenge, profit, glory, and to aid in showing security flaws (Branigan, 2004; Rafay, 2019). Similarly, malware writers<sup>4</sup> can be distinguished based on their motivations and their objectives. (Furnell, 2001a). These definitions, thus, left some important aspects aside. The second set of definitions is also too narrow as it does not encompass new types of offences and is quickly outdated.

Grabosky (2001) refers to this matter as “*old wine in new bottles*” since, in his opinion, cybercrime is “*basically the same as the terrestrial crime with which we are familiar*”. However, such analogy has been criticised by Wall (2016), who described it as “*new wine, no bottles*”. Indeed, the distinction be-

tween conventional crimes perpetrated through technological means and new offences must be made to provide an appropriate benchmark effectively.

### 1.3. Broader Definitions

The significant deficiency of the narrow definition is that the binary nature of cybercrime is not taken into consideration. Indeed, the computer can either be the target or tool of the crime, as Wilson (2008) has described. To remediate this problem, another group of scholars has established broader definitions of the concept of cybercrime. During the Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders in Vienna, cybercrime was divided into two categories; “*a. Cybercrime in a narrow sense (computer crime): Any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. b. Cybercrime in a broader sense (computer-related crime): Any crime that can be committed by means of a computer system or network, in a computer system or network, or against a computer system or network. In principle, it encompasses any crime capable of being committed in an electronic environment*” (United Nation, 2000). The CoE Convention on Cybercrime defines cybercrimes as offences against confidentiality, integrity, and availability of computer data and systems: computer-related offences: content-related offences: and offences related to infringements of copyright and related rights.

Branigan (2004) defines cybercrimes as occurring when “*the criminal uses technology in the commission of a crime, or a criminal attacks technology and makes it the target of the crime*”. The binary nature of cybercrime is better reflected in this definition; the computer can either be the target or tool of the crime. Hess (2002) defines cybercrime as “*harmful acts committed from or against a computer or network*.” For instance, Section 502 of the Californian Penal Code reflects this binary nature by listing seven computer crime acts and regarded as a public offence.<sup>5</sup>

Wall (2007) notes that the term cybercrime “*has a greater meaning if we construct it in terms of transformation of criminal or harmful behaviour by networked technology, rather than simply the behaviour itself*.” He also interprets the term broadly to refer to “*criminal or harmful activities that involve the acquisition or manipulation of information for gain*.” Brenner (2004) divided computer crime into three categories; the use of a computer as a target, such as hacking and dissemination of viruses, the use of a computer as a tool to commit criminal activities, such as cyber fraud, and finally, the use of a computer as incidental to the crime<sup>6</sup>.

The most widespread definition (Britz, 2013) defines cybercrime as: “*any crime that involves computers and networks, including crimes that do not rely heavily on computers*”. This definition allows any criminal activity involving a computer to be defined as a cybercrime. While it encompasses the broadness of the spectrum of cybercrimes, it is also vague.

Some international or regional instruments address a broader range of offences, including acts where the offence’s object is a person or value, rather than a computer system or data, but where a computer system or information system is still an integral part of the modus operandi of the offence, such as the ECOWAS<sup>7</sup> Draft Directive. (Pocar, 2004).

Halder and Jaishankar (2011) define cybercrimes as “*Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim, directly or indirectly, using modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)*”.

Tavani (2000) expressed a new view on the problem by introducing three different perspectives: legal, moral, and informative. He stated that *“from a legal perspective, computer crime might be viewed as a useful category for prosecuting certain kinds of crimes. [...] From a moral perspective, the need for a separate moral category is that many of the ethical issues associated with computer crime also border on distinct but related issues involving intellectual property, personal privacy, and free speech in cyberspace. [...] From a descriptive perspective [...], it could help us gain a certain level of clarity and precision in analysing crimes involving the use of computer technology”*.

#### **1.4. The Global Vision of Cybercrime**

The increasing ubiquity of global connectivity presents a serious risk that rates of cybercrime will increase. Both the narrow and broad definitions, to some degree, fail to present a fluid conception of cybercrime. The common issue is that, on top of being complex, an act may be illegal in one nation but not in another, allowing a form of forum shopping. For instance, hacking is not universally recognised as a criminal offence. Interestingly, the Council of Europe Convention on Cybercrime of 2001 does not define cybercrime itself but its various components, such as computer system, traffic data, and service provider. The growing concern over cyberattacks demands a globally agreed definition, which would enable national law enforcement agencies to be more efficient.

The broadness of the spectrum of crimes is also not reflected within the existing definitions. Cybercrime is so broad that its application can vary from sending offensive emails perceived by the recipient as harassment to hacking into a company's database to steal or destroy information. There are also some grey areas of crimes that some qualify as cybercrimes, while others do not. Take the theft of computer hardware devices or the storing of illegal information as examples. For the author, the first does not qualify as cybercrime because it requires a physical act. The use of a computer to store illicit information is less clear cut; in this type of case, the network is not a means of committing a crime but rather facilitates the management of crime. As such, any peripheral role of a computer in a (traditional) crime would create issues as to whether or not it should be excluded from the scope of cybercrime. Consequently, depending on the action, laws applicable to 'traditional' crimes can be effective while others necessitate new responses. For instance, old crimes such as theft, fraud, white-collar crimes<sup>8</sup> and harassment find new forms in the cyberspace but can still be prosecuted according to 'traditional' criminal law. Other crimes, such as hacking, cannot be placed into existing categories.

Any global definition must be based on the broad definition approach. However, as all the attempts to define cybercrime demonstrates, cybercrime is such a broad and all-encompassing term that it is nearly impossible to define without omitting a type of crime, either existing or foreseeable. The broad definition seems more adequate because it encompasses both categories of offences; computers as targets of the crime and computers as means to a traditional offence.

## **2. THE ECONOMIC IMPACT OF CYBERCRIMES**

While legal challenges are preventing the finding of an effective global response, cybercrimes are becoming more frequent and sophisticated. Most perpetrators know that they can act in near impunity while obtaining high returns, which renders cybercrimes very attractive. This also explains why the costs of cybercrimes are on the rise, with a predicted worldwide cost in excess of \$6 trillion annually by 2021

(Dixon, 2019). The cost of cybercrimes is expected to grow exponentially in the years to come, alongside the expansion of the digital economy and emerging innovative technologies, which pose new risks.

As noted above, cybercrime is an umbrella term that covers various criminal activities. The cost of all these activities on society is impossible to establish. For instance, Intellectual property (IP) theft is among one of the most difficult to estimate. It affects not only the IP owner but also the trade and jobs (EUIPO, 2019). As such, “cybercrime damages innovation”, some activities, such as financial frauds and scams, are easier to quantify, while much more difficult to stop. Financial frauds are conducted either through fraudulent emails, such as phishing, or through viruses. Financial frauds include both the stealing of financial information and the demand for ransom—for instance, the WannaCry or Petya ransomware attack that encrypted data and demanded payment (Intel Security, 2014).

Recently, scams have received increased attention from the media. In Australia, the cost of scams, in 2018, was close to half a billion dollars while in the US, this number reached a staggering \$3.5 billion in 2019 (Scamwatch, 2019). In the UK, criminals “*stole £1.2 billion through fraud and scams in 2018.*” (UK Finance, 2018). In the US, “*the most financially costly complaints involved business email compromise, romance or confidence fraud, and spoofing, or mimicking the account of a person or vendor known to the victim to gather personal or financial information*” (Gorham, 2019). In Australia, investment scams are the most commonly reported scams (\$86 million), followed by romance scams (\$60.5 million). In the UK, unauthorized payment frauds represent the biggest problem (£671.4 million), followed by invoice and mandate scams (£123.7 million) and investment scams (£50.1 million). In Europe, the most common scams in 2019 were buying scams, identity theft, and monetary fraud.

Scams can be extremely lucrative, especially because criminals are getting so sophisticated that it becomes harder and harder for victims to spot the red flags and tell real from fake. For instance, in 2018, romance scams in the US amounted to a total of \$143 million, more than any other consumer fraud (Fletcher, 2019). In Australia, the cost of romance scams, for the same year, was \$60.5 million (Scamwatch, 2019). In the UK, romance scams amounted to £12.6 million in 2018 (UK Finance, 2018). While romance scam is a major problem in Australia and the US, costing victims millions of dollars a year, it seems a lesser problem in the UK and Europe. Romance scams can even combine multiple offences, such as credit card frauds or identity theft.

Data breach is one of the fastest-growing crimes posing a major threat to both businesses and individuals. For example, the Epsilon attack, which exposed the names and addresses of millions of users, cost the company billions of dollars, or the Yahoo’s breach, which remains, probably, the most important one, whereby the hackers stole data, but not financial information, from 3 billion accounts. (Larson, 2017). Similarly, the Marriott Hotels breach in 2018, whereby the hacker obtained access to the personal details of 500 million customers (BBC, 2018). These breaches, when resulting in identify theft, have a huge economic impact. While the number of victims in the US went down between 2017 and 2018, the financial costs of such frauds have risen to \$3.4 billion (Marchini & Pascual, 2019).

More than financial losses, identity theft can lead to possible arrest and lower credit score ratings (Gredler, 2016). In Europe, ID theft is also on the rise due to the large number of different identity cards and residence documents used across the EU. To combat this growing problem, the EU Civil Liberties (LIBE) Committee approved, in 2018, plans for a new single identity card to improve ID card security and reduce document fraud, which is estimated to cost €2 billion annually (KYC360, 2018). Even more complex are identity thefts related to minors. In the US, minors “are often targeted for bank account, credit card, and government benefits fraud” because the cybercriminal only needs the child’s social security number (Otutua-Amoah, 2017). These cases can have enormous impacts on the victims’ lives.



On top of resulting in high costs, cybercrimes also represent a barrier to trade. For instance, business email compromise (BEC) has been a concern for years. In 2019, this practice cost more than \$1.7 billion to US companies. (Gorham, 2019). However, the highest cost of cybercrimes comes from damage to companies' reputation, brand image, and national economy (Intel Security, 2014). Cybercrimes could also result in loss of opportunity, including services and employees. Aside from the financial loss and related consequences, the cost of cybercrimes also involves the costs of countermeasures and insurances, which amounts to billions.

Unfortunately, many cybercrimes go unreported for two main reasons: fear of embarrassment and fear of negative repercussions (Wall, 2007). Companies might be reluctant to report cybercrimes by fear of the embarrassment it might cause them, and the harm done to the company's reputation. The second reason is the fear of the negative repercussion, such as acknowledging that the computer security is inadequate. For instance, if customers discover that the security system of the bank in which they have a saving account has been broken in, they most certainly will transfer their funds to a bank perceived as more secure. Consequently, the real cost of cybercrimes is difficult to estimate.

### **3. LEGAL CHALLENGES IN FIGHTING CYBERCRIME**

As already discussed, the term cybercrime is used to describe a wide variety of criminal acts that are often committed remotely using Information and Communication Technologies (ICTs). The lack of a globally agreed definition represents an underlying legal challenge in the fight against cybercrimes. Indeed, most of the issues that will be discussed in this section could be, at least partially, resolved if a global definition existed. Indeed, even in the Convention on Cybercrimes, the term was not defined, which results in different interpretations at national level.

Moreover, the lack of a universally recognised definition can result in some leaders enacting anti-cybercrime laws targeted at opponents, dissidents, and other civil society groups. (Ben-Hassine, Sayadi, & Samaro, 2018). Even more complex are situations related to activities that do not have a universally recognised definition, such as terrorism (Memdani, Kademi & Rafay, 2021). Due to the lack of consensus on a global definition of terrorism, cyberterrorism is a grey area that could be used against opponents of governments. For instance, various cases of hacking in the US have been tackled as cyberterrorism, such as the South Pole Station case, where hackers threatened to sell the station's data and expose the failures of the system. (USDOJ, 2004). The facts seem to suggest that it was more a hacking than a cyberterrorism attack. The closest to an act of cyberterrorism is certainly when Ardit Ferizi "*accessed a protected computer without authorization and obtaining information in order to provide material support to ISIL*" (USDOJ, 2016). This is even more concerning because any intrusive measures on the cyberspace can have far-reaching consequences; if someone's mailbox is continuously controlled, the person will lose his privacy without knowing it (Hussain *et al.* 2019).

The biggest challenge is when an activity is criminalised in one country but not in another, which renders cooperation and prosecuting impossible due to the dual criminality requirement found in most extradition instruments.<sup>9</sup> Consequently, cybercriminals might not be extradited and prosecuted. This situation is partially created by the impossibility of reaching a consensus on the definition of cybercrimes. Without such definition and a minimum of harmonisation, dual criminalisation will always constitute an insurmountable obstacle. The importance of having measures that can effectively deal with cybercrime is exemplified by the 'Love Bug' virus case<sup>10</sup>, whereby the offender was never charged because the Philip-

piners had no law against hacking, which led to the charges in the US being dismissed. (Brenner & Koops, 2004). Therefore, national laws against cybercrimes must be harmonized for them to be more effective.

However, harmonization can be problematic due to the different existing views on a specific activity. Contrary to traditional crimes, cybercrimes are global crimes as highlighted in a report of the European Commission, which stated that “*computer-related crimes are committed across cyberspace and do not stop at the conventional state-borders. They can [...] be perpetrated from anywhere and against any computer user in the world*” (Commission of the European Communities, 2001; Allan, 2005). The lack of geographical borders renders traditional law and mutual agreements inadequate and slow (Meyer, 2000). Indeed, cybercrimes are global crimes, but yet they are subject to local law enforcement.

Cybercrimes do not always fit within specific categories. By trying to rely on the ‘real’ world counterpart of the cybercrimes, it makes it harder to investigate and prosecute such crimes. For most people, cybercriminals are limited to hackers, the idea mostly conveyed by movies. By introducing categories of crimes, based on either the nature of the crime, the motivation, the victim, or other, laws will be more suitable and will better coop with the issues created by cybercrime. The legitimate ground for creating separate categories was given by Tavani while introducing three different perspectives: legal, moral, and descriptive. (Tavani, 2000). He noted that “*From a legal perspective, computer crime might be viewed as a useful category for prosecuting certain kinds of crimes [...] From a moral perspective, the need for a separate moral category is that many of the ethical issues associated with computer crime also border on distinct but related issues involving intellectual property, personal privacy, and free speech in cyberspace [...] From a descriptive perspective [...], it could help us gain a certain level of clarity and precision in analysing crimes involving the use of computer technology.*” Therefore, having a classification of crimes is useful, from a legal perspective, to investigate and prosecute such crime. It also helps to draft laws that are adequate for the type of crimes that are targeted. As noted above, some cybercrimes can be prosecuted under existing statutes dealing with real-world crimes, while others cannot be prosecuted that way.

In addition to no existing fitting categories, cybercrimes evolve quickly; as long as there is money to be made, new types of attacks will be developed and sold on the Dark Web. As Schiappa (2019) noted, “*Now, with ransomware as a service (RaaS) and other hacker toolkits like malware-as-a-service and phishing-as-a-service, the world of cybercrime has evolved from a hacker hobby into a capitalist market*”. This constant evolution makes it harder for governments and law enforcers to erase the problem. Any definition of cybercrime might be outdated even before it is enacted.

The prosecution of cybercrimes is further complicated by a central legal issue, jurisdiction. The electronic environment challenges the traditional methods for asserting jurisdiction and requires a rethinking of the claim that cyberspace should be governed by territorially defined rules. (David & David, 1996). As Oraegunam (2016) noted, “*it is hard to territorially locate conduct in cyberspace because of the dispersed and amoeboid nature of the network that makes up the Internet*”. The traditional approach does not work, even more so, that cybercrimes often have a transnational aspect to them. One of the best examples of the lack of jurisdiction is romance scams, which involve at least two countries and require international cooperation to arrest the scammers. Indeed, love scammers are often part of an international ring of cyberthieves, such as the recent arrest of Nigerians nationals in the US or the Australian jailed for her role in romance scams (ABC News, 2019; CDPP, 2019). In most romance scams, however, foreign authorities can only request the help of the local government to arrest scammers as they have no authorities to do so themselves, making it a very lucrative business for scammers with relatively low chances of being prosecuted. For instance, in the case of the death of Jette Jacobs, a 67-year-old Aus-

tralian national, the arrest of the suspect was only made after a request by WA Police major fraud squad and the Australian Federal Police to the Nigerian authorities (Nicholson, 2014). Similarly, international cooperation resulted in the arrest of three members of the Fin7 in Poland, Germany, and Spain who were facing charges in the US for deploying the Carbanak malware and stealing more than 15 million customer card records. (USDOJ, 2018). All these examples demonstrate that it takes years, significant resourcing, and international cooperation to arrest only a few members of a single cybercrime organisation.

The fact that data can be permanently moving or stored in multiple jurisdictions poses a challenge to prosecutors as it might be hard to establish where to file the request. For instance,

uploaded offending material on various websites. In the US, based on an old libel case, it can be presumed that the offence is committed in the state where the uploader is located.\* At the EU level, the CJEU rulings in *Fiona Shevill* (1995) and *eDate* (2011)<sup>†</sup>, makes it clear that the claimant can choose between suing before the court of the place of publication or where the harm has been suffered, or the place where the claimant's centre of interests is based. This can become an even more complicated question when the request is addressed to a private service provider as national laws in place might impede it to cooperate.

Even when the victim and perpetrator are located in the same jurisdiction, relevant evidence may not. These situations would still necessitate international cooperation. The current frameworks are, however, not suitable for large-scale cyberattacks requiring important international collaboration. Instead, the success of an operation will depend on the diplomatic relationship between the countries involved, which is time-consuming and could result in the loss of evidence. For instance, the suspected leader of a cybercrime ring specialised in cyber bank robbery was arrested in 2018 after a five-year investigation (Europol, 2018). This investigation and successful arrest were only possible through international cooperation between the Spanish National Police, Europol, the US FBI, the Romanian, Moldovan, Belarussian and Taiwanese authorities and private cybersecurity companies. (Europol, 2018). While it is a victory, *per se*, the length of the investigation allowed the cybercrime ring to steal over 1 billion euros. This demonstrates the inadequacy of the current system to intervene promptly to avoid the cost to mount.

The jurisdictional limitation also creates an attribution problem; the lengthy cooperation procedures can result in evidence being lost. The volatile nature of electronic evidence and the facility with which it can be deleted or altered require a targeted and timely collection. (Eoyang, Peters, Mehta, & Gaskew, 2018). Evidence can also be lost due to differences in data retention obligations or chain of custody's breach, making it harder to prosecute a suspect or the designation of the country having jurisdiction can become impossible due to encryption tools.

Encryption and anonymization tools, which are essential in ensuring the protection of fundamental human rights and security, also generate new challenges for law enforcement. Both tools render the investigation of cybercrimes more complicated. For instance, authorised interception of communication is made less effective by encryption. Digital forensic analysis is also negatively affected, allowing criminals to hide evidence of their illicit activities, such as terrorists, organised groups, or sex offenders. In addition to making the investigation more complex, it also makes conviction more complicated, mainly if cryptocurrencies are used to finance the criminal activities. The existing laws do not allow for the prosecution to avoid the problem. Instead, the lack of receivable evidence can result in charges being dropped.

As cybercrimes are often motivated by profit, cybercriminals are increasingly using digital payment methods to launder money due to their unregulated and pseudo-anonymous nature. Moreover, cryptocurrencies can be used either as a tool or target in the facilitation of cybercrimes. For instance,

the ‘WannaCry’ ransomware which pressed victims to pay \$300 in Bitcoin (Baker, s.d.), highlights how cryptocurrencies can be a tool in the facilitation of cybercrimes. Similarly, when cryptocurrencies are used to pay for illegal goods or services on the Dark Web, they become a tool. At the same time, cryptocurrency payment processors are not immune against traditional forms of cybercrimes, such as hacking and phishing, resulting in cryptocurrencies being a target (Reddy & Minnaar, 2018). As Marria (2019) noted, *“in recent years, cryptocurrency has become the favored detergent for criminals to launder money”*. It has been estimated that \$200 billion in ill-gotten gains a year are laundered through a combination of cryptocurrencies and peer-to-peer marketplaces (Bell, 2019). In 2018, it was reported that *“£4 billion had been laundered through cryptocurrencies in Europe alone”* (Marria, 2019). Cryptocurrencies are extremely attractive for cybercriminals as they are highly portable, easy to use, relatively anonymous, and have a low level of regulation. Indeed, crypto assets often fall outside the scope of the EU financial regulations (EBA, 2019). As a result, there has been a call to introduce anti-money laundering regulations applicable to cryptocurrencies (Rafay, 2021).

Without the ability to track the source of the cryptocurrency, governments and law enforcement agencies cannot possibly prevent the cybercrimes linked to cryptocurrency (Iqbal *et al.*, 2019). As Marria (2019) noted, *“the global adoption of sites means money launderers can easily hide their illicit profits amongst legitimate ones, as well as move these payments across borders discreetly”*. Moreover, the linkage of cryptocurrency to a specific crime is rendered more complicated through mixing. As van Wegberg, Oerleman, and van Deventer (2018) explain, *“on the Dark Web, services are being offered to anonymize bitcoins even further, by mixing them, or in this case – launder them”*.

Cryptocurrencies do not only cause problems due to their nature but also because of the lack of a recognised uniform definition, making it harder for law enforcements to stop cybercrimes. For instance, some countries such as France still do not have a clear definition of cryptocurrencies. In fact, it was only in March 2020 that the Commercial Court of Nanterre recognized BTC as a currency (Singer, 2020). At the same time, the regulation of cryptocurrencies, due to their potential link to terrorism, has quickly moved up the agenda, resulting in the enactment of the 5th EU Anti-Money Laundering Directive, which came into force in January 2020. It requires *“the registration of cryptocurrency exchanges with financial regulators and the transfer of client wallet addresses to them. In general, the EU has been gradually tightening its regulation of the cryptocurrency market”* (Perez, 2020). The delay in regulating cryptocurrencies was mainly caused by serious privacy issues.

As the Europol and Eurojust report states, *“Law enforcement experts share the opinion that organised crime networks actively exploit existing jurisdictional boundaries in their criminal business models to avoid detection and prosecution”* (Eurojust, 2019). The borderless nature of cybercrimes requires another approach than the traditional jurisdictional one based on geographical borders. Indeed, fighting cybercrime local has proven to have limited effects because the crimes are rarely committed in the same jurisdiction as where the damages are felt. Even if the substantive laws are similar, the adjectival laws and enforcement procedures may differ.

To facilitate cooperation and access to digital evidence, many countries have entered into bilateral or multilateral treaties that set parameters for the conduct of investigations. The two most common forms are extradition instruments and mutual legal assistance (MLA). Extradition instruments stipulate the procedure to extradite an individual from one country to the requesting state. However, many of these instruments require dual criminality, namely that the conduct is criminalised in both countries. As noted earlier, this is probably the biggest challenge cybercrime prosecution is currently facing. MLA aims at facilitating cooperation on cybercrime investigation, by, for instance, collecting and sharing evidence

(Mulligan, 2018). MLAs can either be binding or non-binding international or regional instruments. The Council of Europe Convention on cybercrime (2001) is worth mentioning as it is the only legally binding international treaty explicitly dealing with cybercrimes in place.<sup>11</sup>

#### **4. THE CONVENTION ON CYBERCRIME 2001: REMEDIES (AND FAILURES)**

The Convention on cybercrime has tried to solve some of the issues by providing a guideline for drafting national legislation and harmonizing criminal law provisions on cybercrimes. It offers some flexible mechanisms to avoid conflict with national legislation and proceedings while still ensuring human rights protection. The Convention also establishes standard rules for investigative powers, which are suited to the information technology environment. As such, the Convention provides global standards and a framework for effective, fast international cooperation. The Convention was opposed by civil liberties groups that feared that the new investigative authorities might endanger privacy. (Vatis, 2010). Other criticisms related to the lack of procedural safeguards to limit the extended powers of law enforcement authorities, the lack of criminalization of any violation of data protection rules, and the ‘limited’ grounds for refusal of cooperation. For instance, Goldsmith noted that “*The duty to cooperate contains large loopholes for requests that prejudice such essential interests as national sovereignty and security*” (Goldsmith, 2011). A final ground for concern is that the Convention allows, under certain conditions, law enforcement authorities direct access to personal data stored abroad without ensuring compliance with the local data privacy standards (Tosoni, 2018). Today, “*The Convention represents the most substantive, and broadly subscribed, multilateral agreement on cybercrime*” (Vatis, 2010).

Still, the shortcomings of the Convention are obvious. While a large number of the European Member States and the US have ratified the Convention, other major players, such as China, India, and Russia, have not (Hakmeh, 2017). The term cybercrime is not defined; instead, some of its major components are. Additionally, the definitions are vague and subject to different interpretations in different states (Goldsmith, 2011). Moreover, the Convention requires contracting parties to define criminal offences and sanctions under their domestic laws for the four categories of computer-related crimes recognized by the Treaty. Consequently, there might still be behaviours that are criminalized in one state but not the other. For these aspects, the Treaty relies on the traditional approach, which is not adequate to fight cybercrimes.

States are also required to establish domestic procedures for detecting, investigating, and prosecuting computer crimes, collecting electronic evidence, and establishing a rapid and effective international cooperation system. Although the Treaty defines the procedures related to requests for mutual assistance, with a contact point available 24/7, there are no provisions to prevent data losses. Instead, the available data will depend on domestic procedural law. The lack of enforcement mechanism allows some government to not comply with their obligations. (Goldsmith, 2011).

The problem of jurisdiction has not really been tackled in the Convention. Instead, Article 22(1) establishes that states must adopt adequate legislation to “*establish jurisdiction over any of the substantive offences set forth in the Convention that are committed in the state’s territory.*” However, the Convention does not define what “*committed in the state’s territory*” means. In the Explanatory Note, the drafters noted that “*a Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not.*” The problem in this example is that it does not give any guid-

ance regarding a situation where the attacker is within the territory, but the computer system is not. The Convention also failed to address “*cyber-attacks that are not just criminal acts but may also constitute espionage or the use of force under the laws of war.*” (Vatis, 2010).

While some praise the Convention, which has been used as a basis of various regional instruments<sup>12</sup>, others have highlighted the “stunning cyber enforcement gap” that still exists. (Eoyang *et al.*, 2018). According to a 2018 report, less than 1% of cyber incidents result in enforcement action in the US, meaning that “*cybercriminals can operate with near impunity compared to their real-world counterparts*” (Eoyang, Peters, Mehta, & Gaskew, 2018). The sharp rise in the cost of cybercrimes seems to demonstrate the inefficacy of the system. However, as the European Commission’s Operational Guidance on cyber capacity building highlighted, the implementation of a new legislative framework remains one of the biggest areas of concern (European Commission, 2018).

## 5. EU CYBERSECURITY ACT: RESPONSE TO THE CHALLENGES

The EU has a limited ability to legislate in the field of criminal law, which has always remained part of national sovereignty. However, as it became apparent that cybercrimes were affecting the single market, the EU became more involved in finding a common solution. Consequently, over the years, the EU has taken significant steps to develop an adequate legal framework to address the challenges posed by cybercrime. The EU adopted two main instruments: The Council Framework Decision, 2005 on attacks against information systems and the Directive on attacks against information systems, 2013. Initially, cybercrimes were included as ‘eurocrimes’ back in 2009. (Buono, 2016).

Although Article 1 of the Directive on attacks against information systems stipulates that it establishes “*minimum rules concerning the definition of criminal offences and sanctions in the areas of attacks against information systems,*” the Directive does not define cybercrimes. The Directive retained prior crimes from the Framework Decision while adding criminalisation of specific tools for committing offences. While the Directive is in line with the Cybercrime Convention, it did not bring many changes. The Directive raises the level of criminal penalties to a maximum term of imprisonment of at least two years. The Directive comprises five categories of offences; illegal access to information systems (Article 3), illegal system interference (Article 4), illegal data interference (Article 5), illegal interception (Article 6) and tools used for committing these offences (Article 7). The Directive left important questions to Member States’ discretion. Article 12 is the only provision that regulates procedural matters.<sup>13</sup> However, it is broadly phrased and could result in a conflict of jurisdiction. While the Directive is quite complicated and includes a wide range of possible illegal conduct and sanctions to be imposed, it offers very little explanation or unclear definitions on key terms. Moreover, some offences are missing, such as cyberterrorism or identity theft. Finally, the Directive does not regulate criminal proceedings.

To strengthen the existing legal framework and enhance the security of networks and information systems, the Cybersecurity Act was adopted in 2019. The Act can be divided into two parts: first, the role and mandate of ENISA; second, a European system of certification of the cybersecurity of devices connected to the Internet and other digital products are introduced. Indeed, the Act strengthens the role and mandate of ENISA. Sadly, the operational management of cyber incidents remains an exclusive competence of the Member States, ENISA will only continue to provide its assistance. The significant change brought by the new Framework is the granting of a new competency to ENISA; cybersecurity certification. ENISA will be able to issue European cybersecurity certificates and statements of con-

formity for information and communication technology (ICT) products, services, and processes to be recognized in all Member States. As of now, the certification is on a voluntary basis, but Member States or the Union could make it mandatory at a later stage. Penalties for infringements is left to Member States.

The new Act will, however, have limited impact on the five common challenges identified by Europol and Eurojust; data loss, loss of location, challenges associated with National Legal Frameworks, obstacles to international cooperation, and challenges of public-private partnerships (Europol; Eurojust, 2019). The report deplores the overturning of the Data Retention Directive (DRD) by the European Court of Justice (CJEU) because it leaves law enforcement and prosecutors “uncertain about the possibilities to obtain data from private parties” (Europol; Eurojust, 2019). *“The CJEU’s ruling of 21 December 2016 in the Tele2 Sverige and Watson cases and the resulting requirements for targeted data retention and access criteria for competent authorities have further exacerbated this problem.”* (Europol; Eurojust, 2019). The lack of uniform data retention is a key challenge in cross-border cybercrimes. Another challenge is related to the fact that Internet Service Providers (ISPs) *“cannot differentiate between end-users connected to the same ESP with the same shared IPv4 address at a given point in time.”* (Europol; Eurojust, 2019). Encryption and anonymization tools result in loss of location by investigators and law enforcement.

The third challenge identified is associated with National Legal Frameworks. According to the report, *“despite the existence of international legislative instruments, differences between domestic legal frameworks in the MS and international instruments often prove to be a serious impediment to international criminal investigation and prosecution of cybercrime, partly due to an incomplete transposition of international instruments into domestic legislation. The main differences regard the criminalization of conduct and provisions to investigate cybercrime and gather e-evidence”* (Europol; Eurojust, 2019). This challenge might be partially solved with the enactment of the Cybersecurity Act through the new mandate of ENISA: *“ENISA is also mandated to increase operational cooperation at EU level, helping Member States who would request it to handle cyber incidents, and supporting EU coordination in case of large-scale attacks and crises”* (Europa, 2019). This new mandate, combined with a European Investigation Order (EIO), could result in faster cooperation among MS and avoid the deletion of electronic evidence. The new Act could also help overcome one of the significant gaps in the EIO Directive; the lack of provisions regarding the collection of common types of electronic evidence.

The fourth challenge relates to international cooperation. While there is a framework for the preservation of evidence, there is none for the quick sharing of evidence. Since the collection of electronic evidence is often a time-sensitive issue, the current framework, based on mutual legal assistance (MLA) agreements, is regarded as ineffective and too slow. Similarly, the current system is not effective in dealing with large scale cyberattacks, especially if the attack touches various industries at once.

The final identified challenge relates to the cooperation with the private sector. Private party reporting of data breach is among the most effective measures to fight cybercrimes. For instance, scammers are mainly investigated and prosecuted after private party reporting. As the report noted, *“little consensus exists on the legal framework that is required to facilitate effective and trust-based cooperation with the private sector, while at the same time regulating legal and transparency issues surrounding that cooperation. Moreover, data protection regulation and fear of liability may result in limitations to cooperation with private industry.”* (Europol; Eurojust, 2019).

## CONCLUSION

Cybercrimes is an expanding phenomenon that costs the global economy trillions each year. The growth of Internet access provides cybercriminals with an increasing number of vectors to carry out their crimes. Still, the legal responses are unsatisfactory. Despite the global best efforts, cybercrime is a growing industry that can affect anyone, from infant to elderly and numerous jurisdictions.

At the same time, the legal challenges to fight cybercrimes are still numerous; no commonly agreed definition, jurisdiction problems, possible loss of data, lack of timely cooperation, and loss of location. The lack of a uniform definition is one of the major issues, although less so in Europe, as an activity can be regarded as a crime in one jurisdiction but not the other. In addition, to complicate possible cooperation, it also leads to a form of forum shopping by criminals.

The current framework makes it difficult for law enforcement to fight cybercrimes effectively. Contrary to traditional crimes, cybercrimes are global crimes as highlighted in a report of the European Commission which stated that “*computer-related crimes are committed across cyberspace and do not stop at the conventional state-borders. They can [...] be perpetrated from anywhere and against any computer user in the world.*” (Commission of the European Communities, 2001; Allan, 2005). The lawless nature of the cyberspace and the lack of geographical borders renders traditional law and mutual agreements inadequate and slow (Meyer, 2000). Indeed, cybercrimes are global crimes, but yet they are subject to local law enforcement.

While the Convention on cybercrime has tried to solve some of the issues, others have persisted. As Buono noted, “*One of the main consequences of the global nature of information networks and worldwide connectivity is the ever-growing vulnerability to cybercrimes.*” (Buono, 2016). The borderless nature of the cyberspace represents the second major challenge. Often, the suspect perpetrates his/her act from a jurisdiction, while the effects of that act are felt in another jurisdiction. Moreover, data can be easily lost due to divergences in procedures. These gaps make cybercrimes a low risk but high yield venture.

By their very nature, cybercrimes require extensive cross-border cooperation. However, the international legal framework is still fragmented and mainly based on a 2001 Convention, which, in some respects, is outdated. The current global framework lacks a single governance architecture. Moreover, fighting cybercrimes requires a new approach instead of the application of ‘traditional’ laws. The application of laws related to ‘traditional’ crimes might also affect the efficiency of the actions taken. For instance, identifying the place where a cybercrime was committed can prove challenging and even nonsensical in some jurisdictions (Wall, 2019). Traditional criminal law is, therefore, ill-suited to cybercrimes. Unfortunately, until now, legislation enacted to combat cybercrimes have been based on conventional criminal laws. The EU Cybersecurity Act is no exception to the rule; the Act is still heavily based on traditional criminal law.

While the Act was not *per se* aimed at fighting cybercrimes, some of the lingering challenges identified by Europol and Eurojust might be resolved, at least at the EU level. However, it can be wondered why the Act did not try to fill some of the gaps left by the Directive to create a more robust framework. In fact, it seems that the Act will only be one more piece of legislation added to the existing legislative building. It can be wondered how effective certification of products can be if that very product can be targeted and modified by cybercriminals.



## DISCLAIMER

The contents and views of this chapter are expressed by the author in her personal capacity. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The author extends sincere gratitude to

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## REFERENCES

- Allan, G. (2005). Responding to cybercrime: A delicate blend of the orthodox and the alternative. *New Zealand Law Review*, 149-178.
- Baird, B., Baird, L. L. Jr, & Ranauro, R. P. (1987). The Moral Cracker? *Computers & Security*, 6(6), 471–478. doi:10.1016/0167-4048(87)90028-9
- Baker, O. (n.d.). *What is Bitcoin and why does Ransomware love it?* Retrieved from <https://www.eurostaffgroup.com/media-hub/what-is-bitcoin-and-why-does-ransomware-love-it-85435/>
- BBC. (2018, November 30). *Marriott hack hits 500 million Starwood guests*. Retrieved from <https://www.bbc.com/news/technology-46401890>
- Bell, A. (2019, January 22). *How Cybercriminals Clean Their Dirty Money*. Retrieved from <https://www.darkreading.com/attacks-breaches/how-cybercriminals-clean-their-dirty-money-/a/d-id/1333670>
- Ben-Hassine, W., Sayadi, E., & Samaro, D. (2018, September 12). *When “Cybercrime” Laws Gag Free Expression: Stopping the Dangerous Trend Across MENA*. Retrieved from <https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/>
- Branigan, S. (2004). *High-Tech Crimes Revealed: Cyberwar Stories from the Digital Front*. Addison-Wesley.
- Brenner, S. (2004). US Cybercrime Law: Defining Offences. *Information Systems Frontiers*, 6(2), 115–132. doi:10.1023/B:ISFI.0000025780.94350.79

## **Regulations for Cybercrimes**

Brenner, S., & Koops, B.-J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*, 4, 2–46.

Britz, M. (2013). *Computer Forensics and Cyber Crime: An Introduction*. Pearson Education Inc.

Buono, L. (2016). Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. *ERA Forum*, 17(3), 343–353.

Campbell, T. (2016). *Practical Information Security Management: A Complete Guide to Planning and Implementation*. Apress. doi:10.1007/978-1-4842-1685-9

Carter, A., & Perry, A. (2004). Computer Crime. *The American Criminal Law Review*, 41, 313–365.

CDPP. (2019). *Australian jailed for her role in international romance scam*. Retrieved from <https://www.cdpp.gov.au/case-reports/australian-jailed-her-role-international-romance-scam>

Commission of the European Communities. (2001). *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*. Commission of the European Communities. Retrieved from [https://itlaw.wikia.org/wiki/Creating\\_a\\_Safer\\_Information\\_Society\\_by\\_Improving\\_the\\_Security\\_of\\_Information\\_Infrastructures\\_and\\_Combating\\_Computer-related\\_Crime](https://itlaw.wikia.org/wiki/Creating_a_Safer_Information_Society_by_Improving_the_Security_of_Information_Infrastructures_and_Combating_Computer-related_Crime)

David, R., & David, P. (1996). Law and Borders -The Rise of Law in Cyberspace. *Stanford Law Review*, 48(5), 1367. doi:10.2307/1229390

Dixon, W. (2019, February 19). *Fighting cybercrime – what happens to the law when the law cannot be enforced?* Retrieved from <https://www.weforum.org/agenda/2019/02/fighting-cybercrime-what-happens-to-the-law-when-the-law-cannot-be-enforced/>

Easttom, W. C. (2018). *Network Defense and Countermeasures: Principles and Practices*. Pearson.

EBA. (2019). *Report with advice for the European Commission on crypto-assets*. EBA. Retrieved from <https://eba.europa.eu>

Eoyang, M., Peters, A., Mehta, I., & Gaskew, B. (2018, October 29). *To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors*. Retrieved from <https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors>

EUIPO. (2019). *Online Copyright Infringement in the European Union: Music, Films and TV (2017-2018), trends and drivers*. EUIPO.

Eurojust. (2019). *Common challenges in combating cybercrime*. Europol and Eurojust Public Information.

Europa. (2019, June 26). *The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification*. Retrieved from <https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity>

European Commission. (2018). *Operational Guidance for the EU's international cooperation on cyber capacity building*. European Commission.

Europol. (2018, March 26). *Mastermind Behind Eur 1 Billion Cyber Bank Robbery Arrested in Spain*. Retrieved from <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>

Finance, U. K. (2018). *Fraud the Facts 2019: The definitive overview of payment industry fraud*. UK Finance. Retrieved from <https://www.ukfinance.org.uk/>

Fletcher, E. (2019, February 12). *Romance scams rank number one on total reported losses*. Retrieved from <https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses>

Forester, T., & Morrison, P. (1994). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press.

Frelberger, P. (1981). Micro Crime Macro Problem. *InfoWorld*, 38–39.

Furnell, S. (2001b). *Cybercrime: Vandalizing the Information Society*. Addison Wesley.

Furnell, S. M. (2001a). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, 1(2), 35–44.

Goldsmith, J. (2011, March 9). Cybersecurity Treaties A Skeptical View. *Future challenges in national security and law*, 6. Retrieved from <https://perma.cc/F5LD-27C4>

Goodman, M. (1997). Why the Police Don't Care About Computer Crime. *Harvard Journal of Law & Technology*, 10, 466–494.

Gorham, M. (2019). *2019 Internet Crime Report*. FIB.

Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, 10(2), 243–249. doi:10.1177/a017405

Gredler, C. (2016, September 9). *The Real Cost of Identity Theft*. Retrieved from <https://www.csid.com/2016/09/real-cost-identity-theft/>

Hakmeh, J. (2017, June 6). *Building a Stronger International Legal Framework on Cybercrime*. Retrieved from <https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime>

Halder, D., & Jaishankar, K. (2011). *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. IGI Global.

Hess, P. (2002). *Cyberterrorism and Information War*. Anmol Publications.

Hussain, M., Nadeem, M. W., Iqbal, S., Mehrban, S., Fatima, S. N., Hakeem, O., & Mustafa, G. (2019). Security and Privacy in FinTech: A Policy Enforcement Framework. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 81–97). IGI Global. doi:10.4018/978-1-5225-7805-5.ch005

Intel Security. (2014). *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cyber-crime II*. Intel Security. Retrieved from [https://www.csis.org/files/attachments/140609\\_McAfee\\_PDF.pdf](https://www.csis.org/files/attachments/140609_McAfee_PDF.pdf)

## **Regulations for Cybercrimes**

- Iqbal, S., Hussain, M., Munir, M. U., Hussain, Z., Mehrban, S., Ashraf, A., & Ayubi, S. (2019). Crypto-Currency: Future of FinTech. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 1–13). IGI Global. doi:10.4018/978-1-5225-7805-5.ch001
- Jackson, K. M., Hruska, J., & Parker, D. (1992). *Computer Security References Book*. CRC Press.
- Kshetri, N. (2006). The Simple Economics of Cybercrime. *IEEE Security and Privacy*, 4(1), 33–39. doi:10.1109/MSP.2006.27
- KYC360. (2018, December 6). *EU group approves new-look ID cards to combat €2 billion identity theft*. Retrieved from <https://www.riskscreen.com/kyc360/news/new-look-eu-id-cards-to-help-combat-e2-billion-identity-theft-approved/>
- Larson, S. (2017, October 4). *Every single Yahoo account was hacked - 3 billion in all*. Retrieved from <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html>
- Le Nguyen, Ch. (2020). National criminal jurisdiction over transnational financial crimes. *Journal of Financial Crime*, 27(4), 1361–1377. doi:10.1108/JFC-09-2019-0117
- Lewis, J. (2018, February). *Economic Impact of Cybercrime—No Slowing Down*. Retrieved from [https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm\\_source=Press&utm\\_campaign=bb9303ae70-EMAIL\\_CAMPAIGN\\_2018\\_02\\_21&utm\\_medium=email](https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email)
- Littlejohn Shinder, D. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress Shinderbooks.
- Maghaireh, A. (2005). Combating Cyberterrorism: The Response from Australia and New Zealand. In *International Terrorism: New Zealand Perspectives papers from a seminar held in Wellington* (pp. 81–92). Institute of Policy Studies.
- Marchini, K., & Pascual, A. (2019, March 6). *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*. Retrieved from <https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt>
- Marria, V. (2019, February 4). *How Cryptocurrencies Are Empowering Cybercriminals*. Retrieved from <https://www.forbes.com/sites/vishalmarria/2019/02/04/how-cryptocurrencies-are-empowering-cybercriminals/#7be42bc237c5>
- McConnell International LLC. (2000, December). *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*. Retrieved from <http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf>
- Memdani, L., Kademi, T. T., & Rafay, A. (2021). Effect of Terrorism Financing on selected Global Indices: The Case of 2015 Paris Attacks. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Meyer, G. (2000). Hacker, Phreakers, and Pirates: The Semantics of the Computer Underground. In G. M. Godwin (Ed.), *Criminal Psychology and Forensic Technology: A Collaborative Approach to Effective Profiling*. CRC Press.

- Mulligan, S. (2018). *Cross-Border Data Sharing Under the CLOUD Act*. Congressional Research Service.
- News, A. B. C. (2019, August 24). *Dozens of Nigerian nationals arrested in California over alleged \$68m love scam*. Retrieved from <https://www.abc.net.au/news/2019-08-24/fbi-take-down-alleged-nigerian-love-scammers-in-46-million-case/11445500>
- Nicholson, L. (2014, February 4). 'We all told her not to go': Lonely WA grandmother Jette Jacobs' search for love ended in death. Retrieved from <https://www.watoday.com.au/national/western-australia/we-all-told-her-not-to-go-lonely-wa-grandmother-jette-jacobs-search-for-love-ended-in-death-20140204-31ywq.html>
- Opukri, C., & Imomotimi Ebienfa, K. (2013). International Terrorism and Global Response: An Appraisal. *American Journal of Humanities and Social Sciences*, 1(3), 109–115. doi:10.11634/232907811301373
- Oraegbunam, I. K. (2015). Jurisdictional challenges in fighting cybercrimes: Any panacea from international law? *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 6, 57–65.
- Otutua-Amoah, N. (2017). Statistically Speaking: The Numbers Behind Cybercrimes. *Child. Legal Rts. J.*, 37, 174–179.
- Parker, D. (1976a). Computer abuse perpetrators and vulnerabilities of computer systems. In *National Computer Conference* (pp. 65-73). AFIPS. Retrieved from <https://dl.acm.org/doi/10.1145/1499799.1499810>
- Parker, D. (1976b). *Crime by Computer*. Charles Scribner's Sons.
- Perez, E. (2020, July 12). *How the US and Europe Are Regulating Crypto in 2020*. Retrieved from <https://cointelegraph.com/news/how-the-us-and-europe-are-regulating-crypto-in-2020>
- Pocar, F. (2004). New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research*, 10(1), 27–37. doi:10.1023/B:CRIM.0000037565.32355.10
- Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*. Que Corporation.
- Rafay, A. (Ed.). (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Reddy, E., & Minnaar, A. (2018). Cryptocurrency: A Tool and Target for Cybercrime. *Acta Criminologica: Southern African Journal of Criminology*, 31(3), 71–92.
- Rho, J. (2007). Blackbeard of the Twentieth Century: Holding Cybercriminals Liable under the Alien Torts Statute. *Chicago Journal of International Law*, 7, 695–718.
- Saeed, S., Mubarik, F., & Zulfiqar, S. (2021). Money Laundering: A Thought-Provoking Crime. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Sambo, U., & Sule, B. (2021). Financing as a Livewire for Terrorism: The Case of North-Eastern Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

## **Regulations for Cybercrimes**

Scamwatch. (2019, April 29). *Scams cost Australians half a billion dollars*. Retrieved from <https://www.scamwatch.gov.au/news-alerts/scams-cost-australians-half-a-billion-dollars>

Schiappa, D. (2019, September 12). *The Big Business Of Cybercrime: The Dark Web*. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2019/09/12/the-big-business-of-cybercrime-the-dark-web/>

Singer, A. (2020, March 15). *French Court Moves the BTC Chess Piece — How Will Regulators Respond?* Retrieved from <https://cointelegraph.com/news/french-court-moves-the-btc-chess-piece-how-will-regulators-respond>

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber Criminals on trial*. Cambridge University Press. doi:10.1017/CBO9780511481604

Sukhai, N. (2004). Hacking and Cybercrime. In *1st Annual Conference on Information Security Curriculum Development* (pp. 128-132). ACM Press. 10.1145/1059524.1059553

Tavani, H. T. (2000). Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace. *ACM SIGCAS Computers and Society*, 30(3), 3–9. doi:10.1145/572241.572242

Tosoni, L. (2018). Rethinking Privacy in the Council of Europe’s Convention on Cybercrime. *Computer Law & Security Review*, 34(6), 1197–1214. doi:10.1016/j.clsr.2018.08.004

UK Metropolitan Police Authority. (2007, January 25). *Progress of MPS E-crime Strategy*. Retrieved from <http://policeauthority.org/metropolitan/committees/mpa/2007/070125/10/index.html>

USDOJ. (2004). *Report from the Field: The USA Patriot Act at Work*. U.S. Department of Justice.

USDOJ. (2016, September 23). *ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison*. U.S. Department of Justice. Récupéré sur Retrieved from <https://www.justice.gov/usao-edva/pr/isil-linked-hacker-sentenced-20-years-prison>

USDOJ. (2018, August 1). *Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies*. U.S. Department of Justice. Retrieved from <https://perma.cc/KMS2-9UQT>

van Wegberg, R., Oerleman, J.-J., & van Deventer, O. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419–435. doi:10.1108/JFC-11-2016-0067

Vatis, M. (2010). The Council of Europe Convention on Cybercrime. In *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (pp. 207-223). Washington, DC: The National Academies Press.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Wiley.

Wall, D. (2016). Cybercrimes New wine, no bottles? In P. Davies, P. Francis, & V. Jupp (Eds.), *Invisible crimes: their victims and their regulation*. Springer.

Wall, J. (2019). Where to Prosecute Cybercrimes. *Duke Law & Technology Review*, 17, 146–161.

Wilson, C. (2008, January 29). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*” CRS Report for Congress, 2008, Order Code RL32114. Retrieved from <https://fas.org/sgp/crs/terror/RL32114.pdf>

## **ADDITIONAL READINGS**

Baxter, R. (1973). A Sceptical Look at the Concept of Terrorism. *Akron L. Rev.*, 380-387.

Council Framework Decision 2005/222/JHA on attacks against information systems, OJ L 69 of 16 March 2005, pp. 67–71.

Council of Europe, *Convention on Cybercrime*, Budapest, 23/11/2001, STE n°185

Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, OJ L 218 of 14 August 2013, pp. 8–14.

(2011). *eDate Advertising GmbH and Others v X and Société MGN Limited*, (2011) Cases no C-509/09 and C-161/10. *ECLI:EU, C*, 685.

Franck, T., & Lockwood, B. (1974). Preliminary Thoughts Towards an International Convention on Terrorism. *The American Journal of International Law*, 69-90.

Government, H. M. (2018). *The United Kingdom’s Strategy for Countering Terrorism*. HM Government.

Higgins, R. (2002). The General International Law of Terrorism. Dans R. Higgins, & M. Flory, *International Law and Terrorism* (pp. 27-43). Routledge.

Levy, S. (1994). *Hackers: Heroes of the Computer Revolution*. Delta.

Masferrer, A., & Walker, C. (2013). *Counter-Terrorism, Human Rights and the Rule of Law: Crossing legal Boundaries in Defence of the State*. Edward Elgar.

National Audit Office. (2019). *Progress of the 2016–2021 National Cyber Security Programme*. National Audit Office. <https://perma.cc/8KX6-MGHK>

Paust, J. (1975). A Survey of Possible Legal Responses to International Terrorism: Prevention, Punishment, and Cooperative Action. *Ga. J. Int’l & Comp., L*, 431–469.

Schwartz, W. (1994). *Information Warfare: Chaos on the Electronic Superhighway*. Thunder’s Mouth Press.

Shevill and Others v Presse Alliance (1995) Case no. C-68/93, *ECLI:EU:C:1995:61*

Sieber, U. (1986). *The International Handbook on Computer Crime*. Wiley Publisher.

Steinmetz, K. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime*. NYU Press.

Tavani, H. T. (2004). *Ethics and Technology: ethical issues in an age of information and communication technology*. Wiley.

## Regulations for Cybercrimes

United Nation Congress on the Prevention of Crime and the Treatment of Offenders, *Crimes Related to Computer Networks*, Conference held in Vienna from 10 to 17 April 2000, A/CONF.187/10

UNODC. (2009). *Frequently Asked Questions on International Law Aspects of Countering Terrorism*. United Nations.

Weimann, G. (2004). Cyberterrorism: The Sum of All Fears? *Studies in Conflict and Terrorism*, 129–149.

Yar, M. (2005). Computer Hacking: Just Another Case of Juvenile Delinquency? *Howard Journal of Criminal Justice*.

Yound, S., & Aitel, D. (2004). *The Hacker's Handbook: The Strategy behind Breaking into and Defending Networks*. CRC Press.

Zamir, I. (1989). Human Rights and National Security. *Israel Law Review*, ●●●, 375–406.

## ENDNOTES

\* Letter, Secretary of State to United States Ambassador to Mexico. Department of State, Washington, November 1, 1887.

† C-68/93, Shevill and Others v Presse Alliance, 7 March 1995; cases C-509/09 and C-161/10, eDate Advertising GmbH and Others v X and Société MGN Limited, 25 October 2011.

<sup>1</sup> EU Decision on Attacks against Information Systems and Commonwealth of Independent States Agreement

<sup>2</sup> Parker defines hacking as “the process of attempting to gain unauthorised access into a computer and communication system.” (Jackson, Hruska, & Parker, 1992).

<sup>3</sup> Cybercrime Inquiry (2004) Australian Bankers' Association Inc.

<sup>4</sup> Malware refers to any program or file that is harmful to a computer user. It is a program that causes a variety of damage to a computer when infected, such as altering data or deleting them. Malware includes computer viruses, Trojan horses, and other miscellaneous programs. Trojan horses are probably the most widely spread virus. Often, a user receives an innocent-looking e-mail but embedded within the attachment, or in some cases, even the HTML message itself, is a coded page that connects the PC to a Web site. From there, a small Trojan horse is downloaded into the computer, and the hacker is alerted that the computer has been penetrated. The increase in Internet usage also increases the Trojans' threat. (Campbell, 2016). The difference between virus and Trojan could be made by an analogy to burglary. A virus is like a burglar who breaks into a house, steals the contents, and then leaves, while a Trojan is a burglar who repeatedly breaks into a home. (Easttom, 2018).

<sup>5</sup> 1) knowingly accessing and without permission, altering, damaging, deleting, destroying or otherwise using computer data to execute a scheme to defraud, deceive or extort; or wrongfully control or obtain money, property, or data; 2) accessing without permission in order to copy or make use of any data from a computer system or network, or to take or copy any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network; 3) using computer services without permission; 4) without permission to add, alter, damage, delete or destroy any software or computer programs internal or external to a computer, computer system



or computer network; 5) disrupting computer services or cause a denial of computer services to an authorized user, computer system or network; 6) provide or assist in providing unlawful access to a computer; 7) introducing contaminants into a computer, system or network.

<sup>6</sup> Others who concur with this view see: (Sukhai, 2004; Furnell, 2001a).

<sup>7</sup> Economic Community of West African States (ECOWAS)

<sup>8</sup> White-collar crimes are generally defined as nonviolent crimes committed in the course of business activities, usually motivated by monetary profit.

<sup>9</sup> At the same time, dual criminalisation is not only a problem for cybercrimes; they also create obstacles in the prosecution of transnational financial crimes. (Le Nguyen, 2020)

<sup>10</sup> The creator of the Love Bug made it look like an innocuous attachment to an e-mail. However, when opened, the bug installed itself on the computer's hard drive, replaced itself with a copy of itself, and then sent infected e-mails to the addresses logged in the Outlook Express folder. Since Microsoft Windows is one of the most commonly used software, the bug became particularly powerful. Losses sustained in terms of lost work hours have been estimated to be around \$10 billion.

<sup>11</sup> The UN Convention against Transnational Organized Crime can be of some help to facilitate co-operation but has never been intended to combat cybercrimes.

<sup>12</sup> The Malabo Convention (The African Union Convention on Cyber Security and Personal Data Protection, adopted on June 27, 2014, [EX.CL/846\(XXV\)](#)) and The Arab Convention on Combating Information Technology Offences 2010.

<sup>13</sup> 1. Member States shall establish their jurisdiction with regard to the offences referred to in Articles 3 to 8, where the offence has been committed: (a) in whole or in part within their territory; or (b) by one of their nationals, at least in cases where the act is an offence where it was committed. 2. When establishing jurisdiction in accordance with point (a) of paragraph 1, a Member State shall ensure that it has jurisdiction where: (a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or (b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory. 3. A Member State shall inform the Commission where it decides to establish jurisdiction over an offence referred to in Articles 3 to 8 committed outside its territory, including where: (a) the offender has his or her habitual residence in its territory; or (b) the offence is committed for the benefit of a legal person established in its territory.

# Chapter 24

## Dark Web: The Digital World of Fraud and Rouge Activities

**Jason Diodati**

*Mount Royal University, Canada*

**John Winterdyk**

*Mount Royal University, Canada*

### ABSTRACT

*There is a pressing need for understanding blockchain, cybercrime, and dark web-based fraud. As the world continues to turn digital, uses of cryptocurrencies are becoming mainstream. With this technological adoption becoming a reality, crime is adapting to the times. “Click here for free Bitcoin,” “set up an account and earn 100BTC instantly” are merely anecdotal examples of the ways the act of fraud is innovating. Deeper into this proliferation of technology lies the dark web, where your social security and identity may be offered for a small sum as we speak. Blockchain technology fueled dark web marketplaces’ enormous growth, which facilitated identity fraud and many other cybercrimes taking place as we speak. This chapter and its authors aim to provide a thorough yet simplified explanation of these technologies while expressing current trends and theories surrounding dark web fraud trading of fraud guides and the use of social engineering. This chapter aims to explain all aspects of this area of cybercrime for all to understand.*

### INTRODUCTION

On June 15, 2020, a user or group of users gained unauthorized access to Twitter (CBC, 2020a; CBC, 2020b). Using the powers of access, the person, who took control, decided to manipulate celebrity accounts to harness their large followings and platform. These celebrity accounts could have purported any message of their choosing with the power of reaching millions upon millions of people worldwide. How did these hackers use their new-found global platform? *“I am feeling generous because of Covid-19. I will double any BTC payment sent to my BTC address for the next hour. Good luck and stay safe out*

DOI: 10.4018/978-1-7998-5567-5.ch024

*there!”* (CBC, 2020a; CBC, 2020b). How did this happen, some may ask? In a nutshell, individuals gained access to Twitter using new tactics. They accessed verified accounts, a tool Twitter uses to authenticate celebrities, political figures, and organizations that communicate publicly. Individuals with verified accounts range from Elon Musk to Barack Obama (they were both compromised). Due to said verification, they have amassed millions of followers. This begs the question: why this message? Of all the information to disseminate to a wide-ranging audience, why post messages can seem to be a blatant scam? There is no way anyone fell for this!

When preparing this chapter, over USD 120k is believed to have been transferred to the cryptocurrency address posted (CBC, 2020a; CBC, 2020b).

Welcome to the digital world of fraud where cryptocurrencies, social engineering, and anonymization drive rogue digital activities. Decentralized currencies finance these activities with tools to mask identities that are widely accepted as currency in the Deep Web and in a world where cryptocurrencies surge in popularity, gone are the days of Bitcoin on society’s fringe; you can now officially buy a car with BTC (Kiley, 2018). The proliferation of Blockchain technology and TOR’s use creates near-perfect storms not only for citizens globally but also for the governments that oversee them. Traditional fraud has now been virtually replaced with cyber fraud, where the trends show a USD 600B yearly cost of cybercrime is accounted for, in large part, by cyber fraud. How are these figures and financial bounties achieved? What is Blockchain? Cryptocurrency? Social Engineering? These are all terms this chapter aims to explain and connect. We must develop an understanding of these terms and provide a brief history of dark markets and blockchain technology. We will see the interconnected nature of blockchain/cryptocurrency technology, dark markets, and cybercrime (i.e., looking mostly at cyber fraud) through the content. In time, the connection will demonstrate that the proliferation of blockchain whitepapers and technology led to the development of dark markets that facilitate cybercrime (Rafay, 2019).

Widespread adoption of cryptocurrency is on its way (CBC, 2020a; CBC, 2020b). If there is any chance to combat incoming and present issues like SIM hijacking, Two Factor Authentication fraud (TFA), and COVID fraud, it must be seized using proper legislation. A multidisciplinary approach: a strategy will be delineated based on the opinion of the chapter authors.

## METHODOLOGY

The existing literature surrounding blockchain, the DW, and cryptocurrency generally employ complex language and descriptors. To properly delineate and predict future cyber threats to the increasingly digital world, there must be an understanding of the underlying technology that facilitates these criminogenic behaviours. The methodology follows this logic by explaining the intricacies of these technologies in layman’s terms. With the explanations achieved, examining key contributors in blockchain use and digital fraud where a nexus between all mentioned innovations are discovered through emerging trends within the DW, specifically revolving digital fraud, and blockchain fraud.

## A FORAY INTO THE BLOCKCHAIN, DARKWEB, AND CRYPTOCURRENCY

The interconnected weaving of blockchain technology, cryptocurrencies, and the Darkweb (DW) create a toolbox of resources for those looking to commit fraud in a much more streamlined, covert manner.

There needs to be a robust understanding of the technology in order to understand how these technologies intersect.

## BLOCKCHAIN

Imagine you are in a group project for an assignment, and the goal is to connect with other groups in the class to achieve your task. This group project starts with you alone, and you need others in your group to accomplish the task at hand due to its complexity. The more groups you enlist, the easier the project becomes. You approach others in the class, asking if you can pair your group with their group. Eventually, you enlist five or six other groups to join your group, and the assignment becomes more accessible and more comfortable, using the resources of multiple different groups. This, in essence, is the model of blockchain technology. Blockchain technology uses various computer systems to harness the power required to solve complex tasks. Every time a computer system is added to the blockchain, the harnessing power of these systems increases. With power increases come increases in efficiency, where complex equations are solved faster and faster.

Now, if you have ever been in a group project, you will know that while somebody always, inevitably, does less work than the rest of the group, there always seems to be a self-proclaimed “leader,” who for better or for worse, believes that her or his way of doing things is best. They claim responsibility for the physical assignment; they want to be the ones to put it all together and to hand it in themselves literally. What if this person becomes sick? What if they become corrupt (unlikely, but follow us), go rogue and decide that nobody deserves a passing grade? Or worse, they choose to give ideas and answers to other groups for a fee? This rarely happens in group projects, but it is an all too familiar reality in the real world. This is the beauty of blockchains: they are decentralized while providing each member of a transaction, or nodes, the ability to approve all actions within any digital Exchange of goods or currency through a ledger. Richard Bradley, a who runs the Digital Supply Chain team for Deloitte, an extensive multinational Services network, provided the following simplified explanation:

*You (a “node”) have a file of transactions on your computer (a “ledger”). Two government accountants (let us call them “miners”) have the same file on theirs (so it is “distributed”). As you make a transaction, your computer sends an e-mail to each accountant to inform them. Each accountant rushes to be the first to check whether you can afford it (and be paid their salary “ Bitcoins”). The first to review and validate hits “REPLY ALL,” attaching their logic for verifying the transaction (“proof of work”). If the other accountant agrees, everyone updates their file...*

*This concept is enabled by “Blockchain” technology” (Bradley, 2020).*

Of course, this is an incredibly reductive explanation of the technology but provides a grounded example in explicit wording. Not only could crucial societal infrastructure such as sensitive government agency information and health care data be strongly protected and encrypted, but even banking and digital currency (Khan et al., 2020). Researchers in Brazil have recently concluded that blockchain technology within the healthcare sector “could reinvent the way patient’s electronic health records are shared and stored by providing safer mechanisms for health information exchange of medical data in the healthcare industry, by securing it over a decentralized peer-to-peer network” (Mayer et al., 2020). Their findings

included that “*as healthcare data are already distributed across multiple stakeholders, the blockchain has distributed ledger technology (DLT) infrastructure could outperform existing centralized systems in accessing, extending, and securing the data*” (Mayer *et al.*, 2020). The findings continue by describing the efficiency of blockchain infrastructure, saying, “*...Decentralized systems could also streamline costs, reduce transaction times, and be more efficient than centralized systems due to lower overhead and fewer intermediaries*” (Mayer *et al.*, 2020). This came when the first death related to cyber-crime occurred in a hospital due to a security breach (Wetsman, 2020).

## **BEYOND DECENTRALIZATION, HOW DOES A BLOCKCHAIN NETWORK CREATE MORE SECURITY?**

Think of a blockchain network as a series of cardboard puzzle pieces where one altered piece of that puzzle would require Changing all the other details for them to fit again. This would not only require much work but would require much expertise as well. Using technical terms, a blockchain has a distributed ledger, which includes the details of a transaction, and helps the nodes approve transactions between entities (Chang *et al.*, 2020). Once a transaction is approved, another block is added to the chain. Once a block is added to the chain properly, it creates a hash code, including the hashing from the previously accepted block, linking them (Reuters, 2020). A hash code can be defined as a mathematical operation in which a series of numbers and letters are generated as a unique identifier (Reuters, 2020). If a hash code is altered in any way, it will result in the chain breaking. Any bad actor or fraudster would have to determine each previous hash’s mathematical code in the chain to manipulate the blockchain network (Reuters, 2020) successfully. For this exact reason, blockchain technology is incredibly sought after by the private sector and government and healthcare systems (IBM, 2020). Figure 1 below demonstrates the steps in which are taken to process a transaction through blockchain technology.

## **TYPES OF BLOCKCHAIN**

While the most common type of blockchain networks are public blockchains, there are also private blockchains, permissioned blockchain networks, and consortium blockchains (IBM, 2020). The differences are as follows:

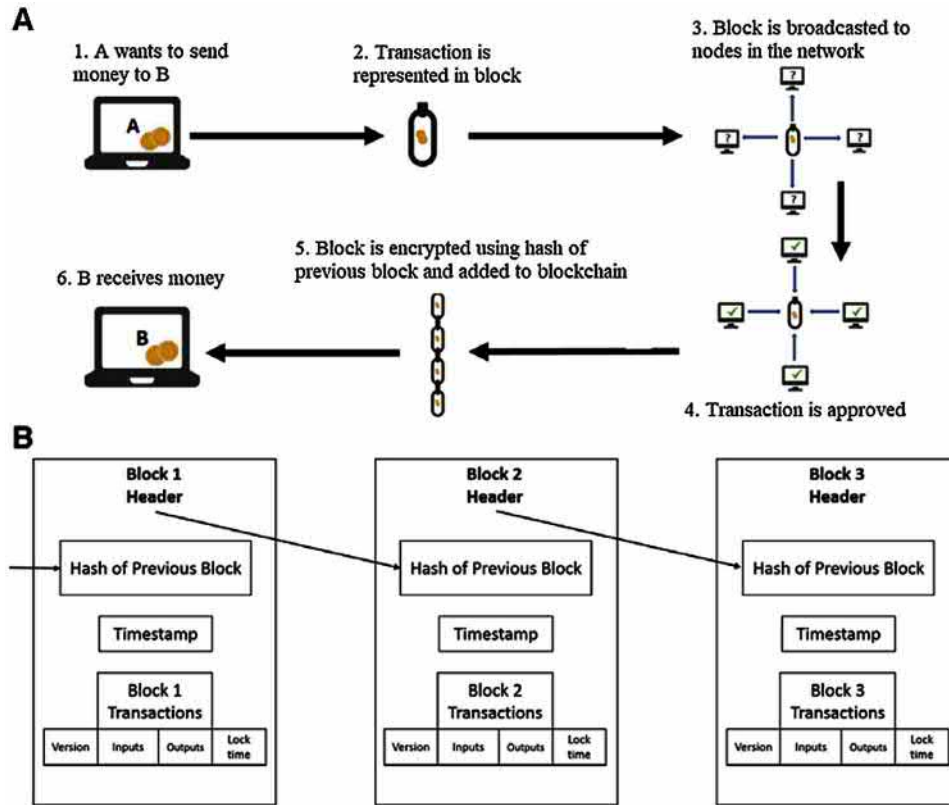
### **Public Blockchain**

Used in cryptocurrencies such as Bitcoin and Ethereum, where the blockchain is accessible by all, and the ledger of transactions is publicly available to anyone (IBM, 2020).

### **Private Blockchain**

A blockchain network is generally used in corporations where a company or entity controls the network. This can usually create a higher security level and be protected using a firewall (IBM, 2020).

Figure 1. Process transaction execution on blockchain  
Source: IBM, 2020.



## Permissioned Blockchain Networks

A permissioned blockchain network applies to private and public blockchains, where an invitation is required to join the network (IBM, 2020).

## Consortium Blockchain Networks

This blockchain is also applicable to organizations but is more practical to uses where multiple organizations make up the blockchain. All administrating businesses can choose who can conduct transactions within the network (IBM, 2020).

## CRYPTOCURRENCY

Imagine a world with smartphones but no high-capacity batteries. Smartphones would not function the way they do now; they would require tethering to a power source. Like batteries, blockchain technology is, in essence, why cryptocurrency is a reality today. Without the security and power that blockchain provides, the digital currency would not have the robustness needed to fend off the inevitable barrage

of attempted theft and destabilization from the digital world. In a globally interconnected computing system, security is at the forefront of concern, especially around digital currency.

The Financial Action Task Force (FATF), a group dedicated to eradicating money laundering and help efforts against financial crime in the United States (Rafay, 2021), defines cryptocurrency as “...a digital representation of value that can be digitally traded and functions as (1) a medium of Exchange; and or (2) a unit of account; and or (3) a store of value but does not have legal tender status...issued nor guaranteed by any jurisdiction” (FATF, 2020). In essence, cryptocurrency has many applications, which generally is the root cause of confusion around the subject (Kiley, 2018).

At the time of this writing, over 1,800 cryptocurrencies exist, and that number grows more extensive as time ticks on (Kenthineni & Cao, 2020). The continually evolving and emerging marketplace also contributes to the overall confusion regarding cryptocurrency. The disorder has been further when cryptocurrencies are named after popular internet memes such as Dogecoin (Coindesk, 2020). Mainstream adoption of cryptocurrencies is taking place as we speak. Many countries, for example, allow for specific cryptocurrencies to be used at the same point of purchase as fiat currency. For this reason and the many applications, both civilian and military, the baseline understanding of cryptocurrency is key to adapting to the technological future.

## DARKWEB (DW)

The Internet is a vast digital landscape with varying levels of visibility and accessibility. Some have referred to the segregation as the Clearnet and Darkweb. The Darkweb is also referred to as the Darknet (Sarker *et al.*, 2019). Researchers define the Clearnet as “...the Web pages and files that are unencrypted and accessible through search engines (e.g., Google, Bing, Yahoo)” (Graham & Pitman, 2020). The definition continues by clarifying that “...the Clearnet is the space that one refers to when references are made to the World Wide Web or cyberspace. The Clearnet, then, is the normative Internet space against which the Darknet is contrasted” (Graham & Pitman, 2020).

As these researchers have identified, the Darknet’s definition is in strong contrast with the Clearnet, in that the Darknet requires uncommon and untraditional means to be accessed and is generally seen as a more fostering ecosystem for criminogenic behaviour versus the Clearnet (Chertoff & Simon, 2015).

It is important to note that standard terms used for the Darkweb include Darknet and Dark Markets. Darknet refers to the network itself, where Darkweb relates to the websites available within the Darknet. Dark Markets refer mostly to the criminogenic markets that thrive within the Darknet/Darkweb.

To access the Darkweb, the most traditionally used method is via The Onion Router, or TOR (Graham & Pitman, 2020). TOR is a downloadable application that allows access to the Darkweb subset of the Internet and other sources such as the Freenet (Owen & Savage, 2015). While researchers have concluded that DW and TOR use are not explicitly linked to hacker culture, it nonetheless provides positively deviant and illegal content such as human and drug trafficking. It is referenced heavily in research focusing on such subjects (Owen & Savage, 2015). Tor uses relays, which allows the user an extra layer of personal protection and obfuscation of their identity (Owen & Savage, 2015). Relays essentially scramble a user’s IP address. This unique identifier can be tracked through internet-based activity and is defined as being “...assigned by the internet Service provider to every device that connects to the Internet. The IP address allows Internet traffic to be delivered to the correct user, but in some cases, it can also be used to trace the origin of Internet activity” (Brown, 2016).

Most research surrounding the DW focuses on the ecosystem itself and how these dark markets sustain themselves. Those who have researched dark marketplaces have found that drug markets are constructed similarly to websites like eBay, where product reviews are essential to the marketplace's viability (Ferguson, 2017). For this chapter, drug marketplaces will be discussed as they parallel to fraud marketplaces within the DW. While these marketplaces are digital, there are some intrinsic connections to traditional fraud that must be examined.

## FRAUD: TRADITIONAL VS. DIGITAL AND TAXONOMIES OF FRAUD

Society has long been infatuated with fraud stories, as fraud has been a phenomenon explored since human civilization's beginnings (Bolton & Hand, 2002). Take, for example, *Catch Me If You Can*, an award-winning film that follows the true story of 17-year-old Frank Abignale Jr., who stole from banks using fraudulent cheques for the better part of three years during the early 1970s. Abignale Jr. was able to produce his cheques by manipulating the routing number, forcing said cheques to reroute to different parts of the country he chooses to defraud before they end up bouncing. With the lament of technology, fraud has evolved from physical cheques to more digital means, and the tactics involved are just as fascinating as traditional fraud (Karpoff, 2020).

## TRADITIONAL FRAUD VS. DARK FRAUD

There are many definitions of traditional fraud; however, Fraud.net defines general fraud as the following:

*Fraud is defined as the wrongful or criminal act to deceive someone for their own financial or personal gain. Legal definitions of fraud vary across countries, at the federal and state levels in the U.S., and even among nations, but most have, at their core, the use of deception to make a gain by unlawful or unfair means. Many types of fraud exist, including occupational, operational, investor, accounting, credit card and Insurance fraud, but all forms share that the perpetrator knowingly receives a benefit to which they are not rightfully entitled. The purpose of fraud may be financial gain but also covers the acquisition of other Services, such as obtaining a driver's license, a passport or other travel documents, or qualifying for a mortgage by using falsified documents or making false statements. (Fraud.net, 2020).*

This definition encompasses most legal fraud cases, where victimization focused on physical means to achieve its goal. Stealing a credit card or fabricating cheques, physical, tangible items can be stolen or mimicked for fraudulent use.

Cyber fraud, or digital fraud, is differentiated by researchers as traditional fraud but using a digital means to achieve deception and receive the proceeds of fraud such as identity or financial gains (Khan & Kanich, 2017). However, differences between the two will be observed.

Fiscal statistics of traditional fraud vary from country to country, but as demonstrated in Figure 2 and Figure 3 below, in the United States, fraud complaints have steadily increased from 2015-2019, and identity theft complaints have increased overall as well (Insurance Information Institute, 2020).



Figure 2. Identity Theft and Fraud Reporting in the United States 2015-2019

Source: Insurance Information Institute, 2020.

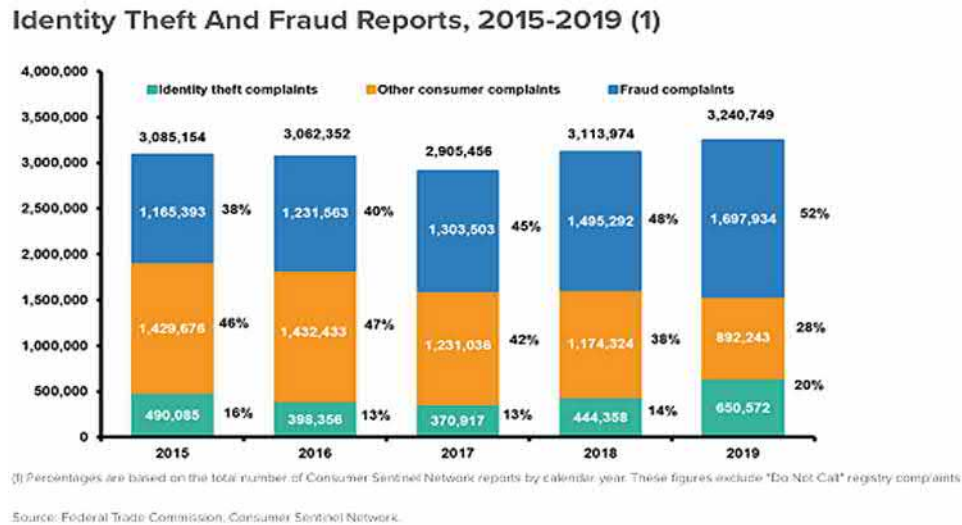


Figure 3. Fraud Losses and Incidents 2013-2019

Source: Insurance Information Institute, 2020.



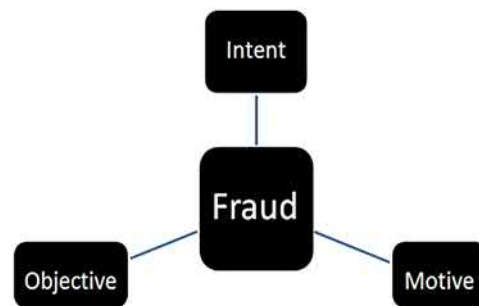
There are subcategories of fraud that have been identified by researchers. Before diving into the typology of fraud, it is essential to note the similarities between all fraud activities. Researcher Cybil Onwubiko (2020) describes that the triangle of fraud, intent, motive, and objective, is intrinsic to all typologies of fraudulent behaviour. Below, in Figure 4, Onwubiko provides a visual representation of the triangle of fraud.

Onwubiko (2020) continues by describing that "...[e]very fraud has intent. Fraud is intentional and strategic, often involving concealment and deception. The intent is the deliberate act to commit fraud or to defraud a person or an entity (e.g., an institution or company) of its possession" (Onwubiko, 2020). The study further explains that this description fits all fraud no matter the country or jurisdiction. Onwubiko's (2020) findings align with earlier research, such as Laleh and Azgomi (2009) added the differentiation between "online and offline fraud" (Onwubiko, 2020). Onwubiko continues by describing that every fraud includes the motive where each perpetrator of fraud receives some benefit from the act, whether physically tangible such as financial gain or access to an identity (Onwubiko, 2020). This

could also include social growth, such as a boost in career. The research continues by describing that “Every fraud has an objective. The objective of fraud is primarily deception, trickery, concealment, and evasion. Deception is the act of deceiving: such as to be false, to fail to fulfil, to cheat, to ensnare, to cause to accept as real that which is inaccurate or invalid (Thomas *et al.*, 2004).

*Figure 4. Triangle of Fraud*

*Source: Onwubiko, 2020.*



The fraud triangle is critical to understanding the transition between traditional fraud and digital fraud; it demonstrates considerable overlaps between both modalities (Onwubiko, 2020). The differentiations also help understand the typologies of fraud, where recent research has dictated over 230 types of fraud across different modalities and motivations (Onwubiko, 2020). For the purposed of dark web fraud, only useful taxonomies will be examined.

## TYPOLOGIES OF FRAUD

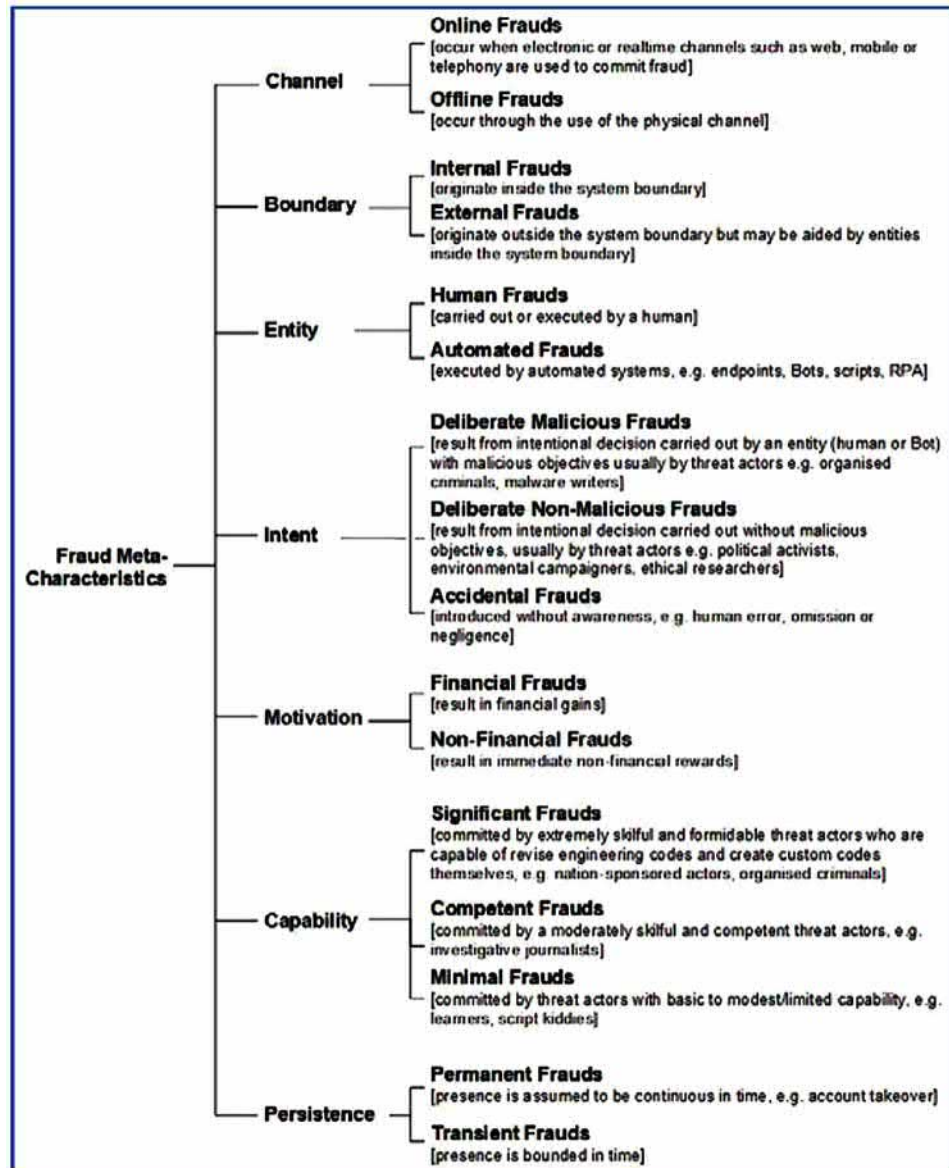
To correctly classify fraudulent behaviour, it is imperative to explore the different taxonomies within a criminal activity (Thomas *et al.*, 2004). Not only does this allow for quicker identification of fraudulent behaviour, but it creates more promising results should the perpetrator be unidentifiable through digital or physical obfuscation (Kemp et al, 2020). To determine taxonomies, the first step is to identify the meta characteristics of fraud, as demonstrated in Figure 5 below (Onwubiko, 2020).

As we can see from In Figure 5 above, channel, boundary, entity, intent, motivation, capability, and persistence are all considered meta-characteristics. Each combination of meta-characteristics creates a different scenario of fraud. For example, an online internal fraud, where automated deliberate means were used to conduct a significant financial fraud, resulting in permanent loss of an account, would be a much more accurate classification of fraud than purely digital, financially-motivated fraud. These taxonomies help experts determine the severity, or rather, the implications of the fraudulent activity to identify the perpetrator and their intention, as demonstrated in Figure 6 below (Onwubiko, 2020).

The matrix in Figure 6 covers the overlapping nature of meta characteristics with fraud classes, of which there are four: account takeover frauds, payment frauds, application frauds, and non-financial frauds. They are described by Onwubiko (2020) as such:

Figure 5. Meta Characteristics of Fraud

Source: Onwubiko, 2020



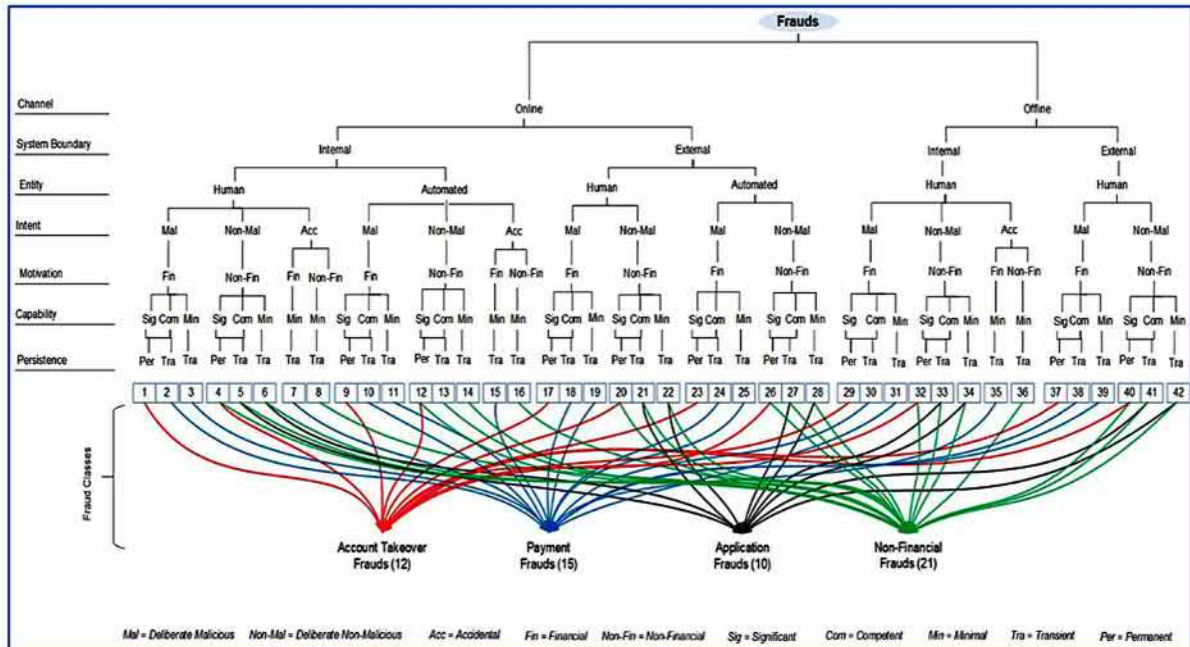
## Account Takeover

Account takeover frauds are fraud types that lead to a victim's account being taken over by the fraudsters. It comprises both financial and non-financial frauds and includes deliberate malicious fraud and deliberate non-malicious fraud. Account takeover fraud (ATF) usually results in permanent fraud, so it is called an account takeover. It can be financial (e.g., card fraud or non-financial, such as social media account takeover, electoral fraud taking over legitimate electorate accounts, or cloning and operating such accounts). ATF encompasses many other forms. The forms include, among others, fungible

## Dark Web

Figure 6. Fraud Matrix

Source: Onwubiko, 2020.



credentials where fraudsters use fake identities to open a bank account or social welfare account and then use the “‘legitimate’ account to obtain government notarised identity, such as drivers’ licence or citizen’s ID card. (Onwubiko, 2020).

## Payment Fraud

Payment fraud is a category of fraud types that result to financial payments, they range from insider related financially motivated frauds, such as occupational frauds, insider trading, to external financially related frauds, such as money laundering, advance fee frauds etc. They also could involve internal to external financially motivated frauds, those requiring collusion, subversion, and covert operations, such as claims fraud, and consumer investment frauds. (Onwubiko, 2020).

## Application Fraud

Application fraud is a category of fraud types that are committed through applications made either offline or online whether for eventual financial gain, such as loan or mortgage application or non-financial gains such citizens’ welfare application (e.g., national ID card for a citizen or school entrance application made by a parent using someone’s postcode so that her daughter can gain entrance to a grammar school in a different neighbour, etc.). It is pertinent to note that application frauds are typical examples of multi-step frauds. These are frauds that start with an application, but “ultimately, the frauds are realized in different ways (Onwubiko, 2020).

## Non-Financial Fraud

*Non-Financial fraud category comprises fraud types not relating to financial gain, instead of motivated by personal rewards, belief and gratis, (e.g., a promotion at the workplace, environmental, social, religion and or racial commitment/campaign). Typical examples of non-financial related frauds include false information (i.e., misinformation) ranging from companies overstating their annual reporting to influence the share market. It could also involve making their company attractive when it is not; to understate the opposite, which could be done to avoid paying much in tax returns. Investigative journalistic fraud is another typical example; they will go to any length to expose government or an authority's wrongdoing, unethical practices or racial or ethnic biases (Onwubiko, 2020).*

*Social and environmental activists fight for what they believe in, and they too will go to any length to campaign based on their belief system, even to the extent of risking their lives (e.g., whistle-blowers). One of the new frauds identified in this category is synchronized fraud – this is when social media accounts (e.g., Twitter accounts, bot, and individual accounts) are set up and used to boost an individual's or companies' tweets by synchronizing multiple Twitter accounts. Some bots accounts, and others individually setup 'bogus' accounts in the pretence to demonstrate the popularity of that Twitter account (Onwubiko, 2020).*

We can identify immediately, based on Onwubiko's (2020) definitions, which type of fraud the Twitter hack first described in this chapter belongs to a hybrid between financial and non-financial fraud. The hybrid act combines financial gain elements, the deceptive earning of Bitcoin, non-financial fraud tactics to engage the victims through synchronized fraud, and a new fraud described recently (Onwubiko, 2020). Whatever entity was behind the attack synchronized many verified accounts to display the same message. This type of automation creates an easier deployment of the intended objective and allows the entity to overwhelm the administrators within Twitter by simultaneously engaging each message. Consequently, as CBC identifies, Twitter could quickly intercept hijacked accounts by merely searching for the replicated post through the server once they realized the tactic deployed (CBC, 2020a; CBC, 2020b).

The meta-characteristics and classifications of fraud help to understand the motivations and intentionality behind fraudulent acts. Without the insight provided, it becomes challenging to classify unprecedented technological innovations, which renders the bad actors behind new attacks much more likely to succeed without detection (Conrad & Wahsheh, 2020). Researchers and those looking to stop fraudulent behaviour with technology alone underestimate the idea that technology alone is the cause of digital fraud's rapid evolution. Instead, the growth of digital fraud is mainly due to technological advancements, but human beings in and of themselves are also responsible for this astounding rise in criminality (Kay & King, 2019).

## DARK WEB FRAUD TRADE AND BLOCKCHAINS FOR FRAUD

The subset of the Internet we have discussed, the DW is home to many different markets and Services (Ferguson, 2017). DW fraud trade is one of the most burgeoning, trending markets at the time of this writing, with new markets emerging as quickly as exploits are uncovered. To properly understand how fraud trade is possible within the DW, other factors within these markets must be analyzed, most specifically

social engineering (Potter, 2018). Social engineering plays a critical role in digital fraud, specifically fraud perpetuated within the DW, considering that while technology and its security improve, it is only as strong as the weakest link. In this case, the weakest link in the chain is us, human beings.

## SOCIAL ENGINEERING

Leaders in the field define social engineering as “*skillfully maneuvering human beings to take action in some aspect of their lives*” (Hadnagy, 2018). Researchers have explained that it is a multidisciplinary practice that involves artistic elements, where a deep sociological understanding of human beings comes into play (Potter, 2019). In a more real-world application, social engineering can come in the form of manipulating one’s surroundings to accomplish an objective (Kaur et al., 2018). If a person spends too much time on Facebook, they can set up a timer on their phone to make sure they do not overuse the Service. This, in essence, is a form of social engineering—a modification of one’s surroundings to accomplish a task.

To achieve the objective social engineering sets out to accomplish, one must take steps to do so; it is referred to as the social engineering attack cycle (Hadnagy, 2018). Figure 7 offers a visual representation of the process.

*Figure 7. Social Engineering Attack Cycle (Hadnagy, 2018).*



The first step involves “information gathering”. All those quizzes on social media designed to help friends “know you”? Those are rich sources of information that social engineers can use to their advantage. The notion that these quizzes that become “viral” or include a call to action to share to one’s social media are made with the primary intention to extract information has yet to be determined or proven in research. Still, it will indeed be examined in the future. The information gathered can be anything from your favourite TV show to your mother’s hometown. This information gathered, specifically within the DW fraud trade, can also be sourced from once-trusted-now-breached places where it was believed the story would be kept anonymized and safe. An example of this would-be Twitter selling users’ phone



numbers that were given to the social media giant purely for two-factor authentication purposes (Cox, 2019). We will return to this issue later in the chapter.

Information alone will generally not be beneficial, as those looking for a large bounty or overly sensitive data will need to delve deeper. Once information is gathered on the intended target, establishing a relationship and rapport is crucial to the information garnered (Potter, 2018). Once a target is selected, whether physically or digitally, they must be made to feel comfortable in their relationship with the fraudster/social engineer. Without this level of comfort determined, mainly when the engineer and target are previously known to each other, the risk of detection is high (Potter, 2018). Establishing rapport needs to be the second step in the attack cycle as gathering information is essential to successful rapport establishment; it provides the attacker with common ground to build off with their target.

The third step in the attack cycle is exploitation, where the target is now involved in the engineering directly (Potter, 2018). The fraudster will use the information gathered and use social nuance and constructs to convince the target to play along with the exploitation. An excellent example of this would-be quid-pro-quo exploits, where the fraudster convinces the victim that they have helped them in some way and that the attacker now needs help in return. More on quid-pro-quo later.

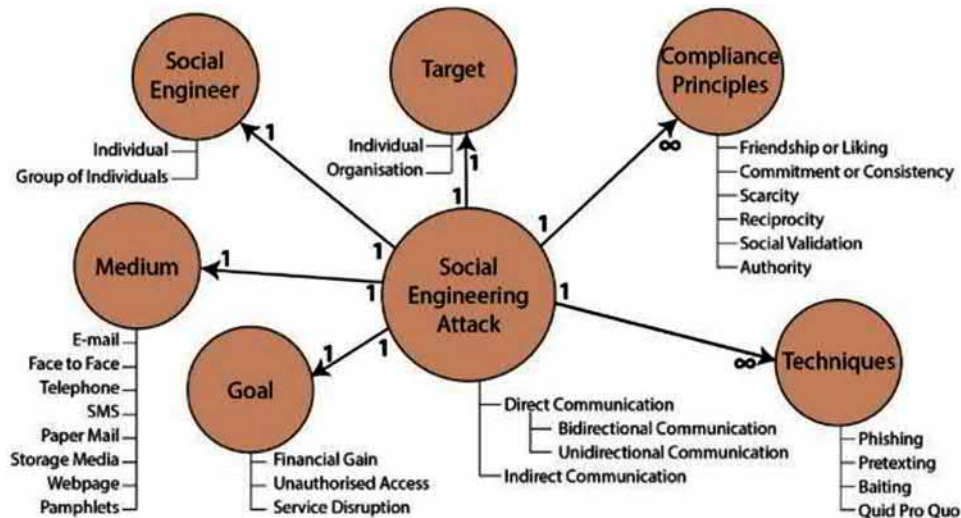
Finally, the execution of the attack is the last step in the cycle. The victim has been primed, the stage set, and with the right amount of persuasion, the victim obliges in the fraudster (Potter, 2018).

It is important to note that this cycle can be repeated until the fraudster is caught (Hadnagy, 2018). For this reason, understanding the process of attack is critical. While it seems obvious, many cookie crumbs that the digital age has allowed society members to spill, creating a trail that gives bad actors a leg up in the fight. We offer an example to demonstrate the importance of social media caution and public post restraint. Suppose you were to publicly post a picture of your parents standing in front of their house on social media. In that case, a savvy fraudster could see that as a potential passcode, using the house number across many different services. Pair that with the attack cycle, where the fraudster creates rapport and dupes you into the execution portion of the process, you have made three potential victims. This example is not meant to induce fear but rather to demonstrate the implications of what one posts publicly on social media. Later in the chapter, Dark Web trade fraud victimology will be discussed, as many of the victimological traits are in sync. A few examples of social engineering were provided in this explanation, but social engineering's ontological model will paint a much better picture in Figure 8 below (Potter, 2018).

As demonstrated by the illustration in Figure 8, fraudsters and social engineers have many options by way of a medium, compliance principles, and techniques. Most notably, the methods are of particular interest, as there are many more than those listed above. In some cases, these techniques are difficult to achieve, but as we will see later, the recent trends within the DW are changing the game. For now, let us explore some of the more common techniques of social engineering attacks. As explained by Potter (2018), possessing Master of Science, Financial Crime, and Compliance management from Utica College, a private university located in upstate New York, whose writing focuses on two-factor authentication and social engineering.

Figure 8. Social Engineering Attack Graph

Source: Potter, 2018



## TECHNIQUES OF SOCIAL ENGINEERING

### Baiting

It is a form of Social Engineering that relies on human curiosity and often includes a promise of something enticing (Bacon, 2018). Baiting can consist of but is not limited to a free download of music with malware attached, a free entry into a lottery/drawing that requests [personal identifying information], or an offering of free money. The latter requires the victim to use their banking credentials on another site to “verify” their accounts and set up the deposit. Whiteman (2017), in his research on Social Engineering, explained that this form of SE tactic is the modern-day equivalent of the Greek’s Trojan Horse given to the city of Troy (Potter, 2018).

“Quid Pro Quo: a Latin phrase translated to mean “this for that.” Usually, with this tactic, a Service is offered. Most of the time, the fraudster impersonates IT support to fix an issue if the antivirus (AV) is disabled (Whiteman, 2017). The “fix” is a software update that is malware (i.e., Eurograbber, Marcher Banker, or Android), which is intended to intercept SMS one-time passwords” (Potter, 2018).

### Phishing/Vishing/SMiShing

It is a fraudulent e-mail/telephone call/SMS text that appears to be legitimately used to trick the recipient into clicking a link, downloading an attachment, or replying with valuable information (Bacon, 2018). Hacquebord & Pernet (2017), senior threat researchers at Trend Micro, gave an example of a phishing e-mail that directed victims to click on a link to download an app designed to circumvent the Google Authenticator app, was by a group known as Pawn Storm. The e-mail claimed to be from Google, indicating that they detected several suspicious sign-in attempts and should download an application known as Google Defender. This group has been around since 2004 and is well known for its credential phishing campaigns. However, due to the increased use of SMS [one-time password] and authenticator apps, they



have become more sophisticated in their phishing campaigns (Ali et al., 2019). This SE scheme abused Open Authentication (OAuth), which authorizes third-party apps access to social media, gaming, and or online e-mail accounts (Potter, 2018).

## Pretexting

When an impersonator lies to a victim about who they are or the company they represent to gain access to personal, financial, or other privileged data to confirm their identity on financial and mobile accounts (Bacon, 2018). Pretexting relies on urgency and fear, just like phishing schemes, but it also depends on trust. Fraudsters will carefully fabricate an identity and background story that leaves little room to be questioned (Whiteman, 2017). Once the trust is built, it is easier to gain the needed information to complete an [account takeover]" (Potter, 2018).

## Scareware

*A trick is used to scare the victim into thinking their computer is infected or downloading illegal material (Bacon, 2018). The fraudster then offers a solution to fix the phony problem, which could be the installation of malware, remote access, and or the request of an OTP (Potter, 2018).*

### Man in the Middle (MITM)

*Gogan, a specialist within digital security solutions, revealed that this SE technique could be used to obtain credentials, [personal identifying information], and OTP codes. Not only can MITM intercept the information as it is being sent, but it could alter it before it reaches its destination. Gogan (2018) also indicated in his writings that many forms of MITM exploit vulnerabilities, such as Man in the Cloud (MITC), Man in the Mobile Application (MITMA), Man in the Internet of Things (MITIoT), or Man in the Browser (MITB). Pierluigi Paganini, Chief Technology Officer at Cybsec Enterprise, explains that with MITB, a malicious add-on or plugin is downloaded and infects the browser and can intercept OTP codes inputted. It can also modify a transaction's content, conduct transfers covertly, and hide previously completed transactions. Pharming is a parallel comparison in that a fraudster hijacks a bank's website and redirects visitors to a fake site that is remarkably like the original where they can obtain information and manipulate it before sending it on to the original destination (Potter, 2018).*

## IDENTITY THEFT TACTICS

Potter (2018) does an excellent job explaining these exploits, which are only a subset of the total amount of techniques. Identity theft fraud within the DW is wide-ranging; for this reason, it is also important to note the differences between standard identity fraud practices, such as account takeover (ATO), existing account fraud (EAF) and new account fraud (NAF).

Account takeovers within mobile phones are a growing problem, particularly in the United States, where most ATOs occur using a victim's mobile phone in a SIM Hijacking format (SHJ) (Potter, 2018). Sim hijacking is the act of fraudulently changing a victim's SIM card account information to receive communication illicitly via a new SIM card belonging to the fraudster (Potter, 2018). This ties in with

## Dark Web

two-factor authentication (TFA), a security measure that most password-based Services provide to authenticate a user by sending a one-time password (OTP) to the user's phone number (Potter, 2018). Because of the dependence on telephone numbers as TFA credentials, once a fraudster has access, only prompt realization and fast action of password Changing will deter the bad actor from successfully taking over all associated accounts (Potter, 2018).

Existing account fraud (EAF) involves the victim's "*checking, savings, loans, credit cards, debit cards, and any other financial instruments that the victim had before the fraud occurrence*" (Potter, 2018). Potter notes that this tactic is prevalent in Nigeria, where a small group of Nigerian fraudsters could control an investment bank in Brazil, taking over \$231M in three years, all by infiltrating a top executive using the attack cycle. It has been reported that in 2017, EAF created \$5.1B in losses (Javelin, 2020).

New account fraud (NAF) causes a world of headaches purely because victims of this type of identity fraud are generally marked from it on their credit scoring, causing lending issues in future (Potter, 2018). This fraud focuses on identifying information that allows fraudsters to open many different accounts over different Services and exploit each account (Potter, 2018). Having access to a victim's SIN or SSN enables a fraudster to open bank accounts, new telecommunication accounts, government subsidy accounts and so on (Potter, 2018).

NAF is incredibly essential to understand in Canada due to the rise of cybercrime as well as the COVID-19 outbreak (McMillan, 2019). The Canadian government offered a Canadian Emergency Response Benefit (CERB) for those affected financially by COVID-19 shutdowns, as demonstrated in Figure 9 and Figure 10 (CAFC, 2020).

Figures 9. Impact of COVID-19 Fraud in Canada  
Source: CAFC, 2020.



Figure 10. Impact of Total Fraud in Canada 2020  
Source: CAFC, 2020.



All the fraudulent acts discussed occur, generally, on the Clearnet. The access of CERB funds, bank accounts, account takeovers all happen on websites accessible by traditional browsers. Earlier, it was noted that these identify thefts and fraudulent acts can be incredibly difficult to coordinate and execute and generally required a robust technological understanding of the task at hand (Loukas et al., 2020). Thanks to the DW, the entry barrier is nowhere near vital because we enter a dark, sinister world of fraud guides.

## DARK WEB FRAUD GUIDES

Imagine a world where recipes did not exist. Creating intricate dishes would be incredibly challenging to achieve, considering there would be no basis from which to begin. Cooking would be for those who had a deep understanding of the relationships between flavours and textures from deep experience, verbal, and physical teachings from a chef from whom they could learn. This exact scenario used to be the case for complex, high stakes, digital fraud. The intricacies of the DW paired with the tools, programming knowledge, and social engineering required to infiltrate large financial or data assets, successfully create, as mentioned, a barrier to entry (Dark Reading Staff, 2020). As of late, that barrier shrinks smaller and smaller (Terbium Labs, 2020).

Fraud guides are a set of instructions put together by experienced fraudsters who use past experiences and amassed knowledge to market a step-by-step replication of their work (Terbium Labs, 2020). Figure 11 is a direct example of an offering of a fraud guide within a DW marketplace.

*Figure 11. Example of Darknet Tutorial Posting*  
Source: Terbium Labs, 2020.



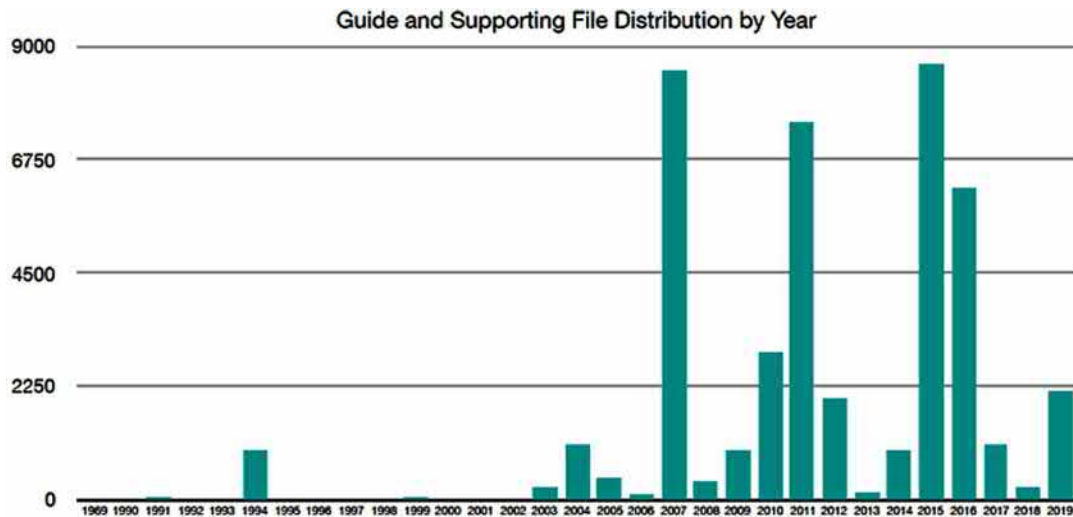
However, this is not the first of its kind by any stretch of the word. At Terbium Labs (2020) reports, deviant guides date back to, most recently, the recirculation of *The Anarchist's Cookbook* by William Powell in the early 1990s.

The circulation of dark fraud guides is no new phenomenon, and, as demonstrated in Figure 12 above, peaked in 2015 and just under 9000 available manuals. However, what is particularly interesting is the price of the offerings, as demonstrated in Fig 1. The offering's cost is no more than a few dollars for 15 guides (Akosan, 2020). The ease of access and proliferation of technology create an influx of more

## Dark Web

Figure 12. Frequency of Dark Web Fraud Guide Distribution by Year

Source: Terbium Labs.



robust synthesis of the material, as broader adoption of technology is beginning earlier and earlier in life (Apple, 2020).

Asif (2020) from Hackread.com reports that fraud guides are the most sold item on the dark web. The article identifies three of the “big box” equivalents on the DW: The Canadian HeadQuarters, Empire Market, and White House Market (Asif, 2020). Of the content sold on the DW, the article continues by describing that 49% of market transactions were dark fraud guides, 15.9% accounted for personal data such as passwords and social security numbers, with a price on average of \$8.45USD.

## COMMON FRAUD GUIDE SUBJECTS

Earlier, we discussed some of the standard techniques of digital fraud within the context of social engineering. Terbium Labs (2020) has provided the most common procedures in fraud guides, as demonstrated below in Figure 13.

While the fraud markets operate in the DW, the information used generally comes from the Clearnet (Vasquez, 2017). Similarly, while fraud guides are sold and distributed through DW channels, their execution occurs typically within the Clearnet. This lends to the original assertion of social media caution and public post restraint. The private information you post publicly can be used to gather information and formulate attacks (Potter, 2018).

## Information Sought From the Clearnet

Terbium Labs’ (2020) recent report, as shown in Figure 14, on the current trends of fraud guides provides data suggesting the type of information fraudsters look for within the Clearnet to disseminate within the DW.

Figure 13. Types of Guides

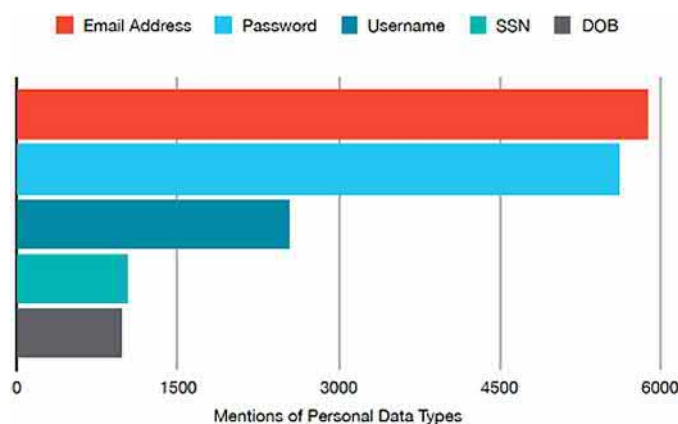
Source: Terbium Labs, 2020.

**TYPES OF GUIDES**

ACCOUNT TAKEOVER	GAINING ACCESS TO USER ACCOUNTS
ACCOUNT CREATION	OPENING AN ACCOUNT (OFTEN A FINANCIAL ACCOUNT) USING FRAUDULENT INFORMATION
CASHING OUT	EXPLOITING FINANCIAL INFORMATION FOR PROFIT, INCLUDING PAYMENT CARDS, BANK ACCOUNTS, AND PAYMENT PROCESSING SERVICES
CARDING	USING STOLEN PAYMENT CARDS ON E-COMMERCE PLATFORMS OR FOR IN-STORE PURCHASES
COUNTERFEITS	MANUFACTURING FRAUDULENT MATERIALS, INCLUDING CREDIT CARDS, IDENTITY DOCUMENTS, AND ACCOUNT STATEMENTS
PHISHING	SCAMMING USERS INTO TAKING ACTIONS OR PROVIDING SENSITIVE INFORMATION ON WHAT THEY BELIEVE ARE LEGITIMATE SERVICES
BYPASSING CONTROLS	USING TECHNICAL METHODS TO CIRCUMVENT EXISTING SECURITY CONTROLS OR AUTHENTICATION SERVICES
DOXING	CONDUCTING TARGETED ATTACKS AND/OR INVESTIGATIONS TO LEAK EXTENSIVE PERSONAL DETAILS ABOUT ONE OR MORE INDIVIDUALS
IDENTITY THEFT AND SYNTHETIC IDENTITIES	EXPLOITING IDENTITY INFORMATION OR DEVELOPING NEW IDENTITIES USING A COMBINATION OF REAL AND FAKE INFORMATION
RESOURCES	COMPILING LISTS OF WEBSITES OR BUSINESSES THAT CAN ASSIST IN ILLICIT ACTIVITY, INCLUDING BOTH LEGITIMATE AND ILLEGITIMATE SERVICES
TECHNICAL KNOWLEDGE	PROVIDING GUIDANCE ON TECHNICAL PROCEDURES FOR ILLICIT ACTIVITY, OFTEN USED TO ENHANCE OPERATIONAL SECURITY (OPSEC)
INSIDER KNOWLEDGE AND TROUBLESHOOTING	ADDRESSING COMMON PROBLEMS OR QUESTIONS IN FRAUDULENT ACTIVITY, BASED ON BOTH ILLICIT AND LEGAL MATERIAL

Figure 14. Types of Marketable Personal Information and their Frequency of Mention within Darknet Markets

Source: Terbium Labs, 2020.



E-mail/password combinations are by far the most popular information discussed and subsequently provided to buyers within the DW fraud markets. However, based on the research conducted by Terbium Labs, there seems to be more focus on username/e-mail address combinations (Terbium Labs, 2020). While TL does not detail why this combo is preferred, the argument could be formulated that usernames and e-mails in combination can generate leads to other existing accounts across different Services. For example, suppose your username is DarkFraudLover and you, like many, use similar or the same username over several Services (like a brand or organization). In that case, it allows fraudsters to infiltrate and control more accounts, leaving the risk of the account being taken back by the victim low.

## **Victimization**

The traditional thoughts and beliefs around dark fraud victims are not as concurrent as they used to be (Potter, 2020). Due to the prevalence of social engineering, anyone can be a victim; however, a high concentration of victims tends to be those aged 45 and above (Potter, 2020). Even those without e-mails or usernames for digital Services can still have their personal information is stolen or leaked (Abdulai, 2020). As mentioned previously, the trails of the information left on social media paired with companies who seem to sell information that the user deemed private leave users at high risk regardless of age (Newman, 2019). As discussed, the report left out in the open in the Clearnet becomes used and manipulated on the DW, exceptionally when digital aliases are replicated across many platforms.

## **BITCOIN: A GLIMPSE INTO DIGITAL CURRENCY WITH BEN PERRIN**

Like many before us, the lead authors' first foray into the Bitcoin space was spurred on by a combination of greed and morbid curiosity. Throughout 2013, the lead author watched as the digital asset climbed through two parabolic rallies from double digits to over USD 1000.

Before this mania's peak, the media documented the takedown of the now infamous Ross William Ulbricht (b. 1984 -) and his darknet market "*The Silk Road*." He massed some USD 25.8 million in profits. This website had facilitated transactions of illicit goods for Bitcoin since 2011 but was seized by the FBI on October 1, 2013. Ross Ulbricht is now serving a life sentence without the possibility of parole. A variety of darknet alternatives continue to increase around the globe.

Contrary to expectations at the time, Bitcoin's price did not crash upon the news but instead went on to rally over the following two months. It was this ironic turn of events that prompted us to dig deeper. Was this merely anonymous online drug money with little value proposition outside of criminal activity? Or was there something more to it?

## **BITCOIN FUNDAMENTALS**

Bitcoin's whitepaper was released in October of 2008, presenting itself as peer-to-peer digital cash. Following its launch on January 3, 2009, and the gradual propagation of the network across the globe, it began to take on specific properties, positioning itself as a digital gold type.

While many of these qualities exist on a sliding scale, Bitcoin currently exhibits strong immutability, censorship resistance, borderless-ness, transparency, auditability, and scarcity. There is a hard cap of 21,000,000 Bitcoin that will ever be created, transactions are near irreversible once confirmed by the network, and the underlying rule set governing the protocol is protected by the most robust computing network.

One thing that Bitcoin most certainly does not have is anonymity.

## **BITCOIN IS HORRIBLE FOR CRIMINALS IN THE LONG RUN**

Bitcoin's number one value proposition today is its embedded monetary policy. In a world of unprecedented actions by the world's central banks, global sound money with a limited supply stands in stark contrast.

Scarce digital money with no counterparty risk is made possible by the distributed nature of the network. Every individual who chooses to run a copy of the Bitcoin software is storing a copy of every transaction ever executed in its global online ledger and the parameters by which all transactions must adhere to be considered valid. Mostly, if anyone tries to do something outside of consensus rules (e.g., creating more Bitcoin or reversing a transaction), it will simply be ignored by the network participants (IBM, 2020).

With the execution of crimes using Bitcoin, the immutable record of transactions is incredibly essential. Contrary to popular belief, Bitcoin transactions are not anonymous. They are, at best pseudo-anonymous.

Anyone can create a Bitcoin wallet on their phone or computer in moments and receive funds from anywhere globally. However, every action of that individual is amended to Bitcoin's blockchain and scrutinized for all time moving forward.

How does this matter, given that the wallet itself is not attached to an identity? Well, there are many ways to associate yourself with a pool of funds on the Bitcoin network. The most common sticking point is the on/off ramps into traditional fiat currency. As regulation around this industry continues to be implemented, KYC/AML (know your customer/anti-money laundering) laws require identification (Shah, 2021) when buying and or selling Bitcoin. Coins associated with a crime and subsequently sold to local currency through a trusted third party will almost certainly be tied to an identity at this point, drawing law enforcement's attention.

Perhaps someone might try to spend their ill-gotten gains on goods and Services? This can easily be tracked by authorities when an e-mail address/shipping information is included in said orders (IBM, 2020).

The inverse is also true: if one were to purchase Bitcoin through a regulated Exchange, move the coins around to various wallets, partake in illicit activities at some point, then use the remaining Change with any Service containing any KYC information at any point in the future - they would effectively be outing their crimes, regardless of how many wallets the funds hopped between from their initial purchase.

Outside of simple money tracing on the blockchain, criminals further risk identifying themselves by sending any transactions on Clearnet - any unencrypted connection to the Internet. Every time you interact with the Internet, your traffic can be identified as coming from your IP address. This information can effectively communicate your exact location and tie this activity to you. Of course, there are tools to mitigate this risk, like using a VPN or Tor - but a single slip-up can undo it all. Forget to use Tor or flip on your VPN before executing a Bitcoin transaction with illicitly used funds? Too late - that record will be kept forever.

## **SEEING THE BIGGER PICTURE**

Despite the reasons mentioned above, Bitcoin is still used in the facilitation of criminal activity. While any attempt to state why this is the case would be mere conjecture, one must imagine that immutable, censorship-resistant transactions have something to do with it. Currently, information asymmetry can be exploited as many people do not understand Bitcoin transactions' irreversibility. This means victims of scams have zero recourse regarding reversing funds sent to a malicious third party.

## **Dark Web**

Do we have any indication of whether Bitcoin itself is a hotbed of criminal activity than other mediums of Exchange?

The United Nations Office on Drugs and Crime estimates 2-5% of global GDP is laundered each year - putting that figure at around \$2 trillion on the high end. The bulk of this is done in cash. However, there are examples of extensive money laundering using the traditional banking system (Sinha, 2021; Gupta & Biswas, 2021; Jayasekara, 2021). The Troika Laundromat revelations included Citigroup, Deutsche Bank, Danske Bank and more, laundering \$8.8 Billion yearly through much of the last two decades (UN, 2020).

What's Bitcoin's share of this? Blockchain analytics firm Chainalysis (a company specializing in tracking and deciphering cryptocurrency-related transactions) found that throughout 2019 criminal individuals or groups laundered USD 2.8 billion worth of Bitcoin through Exchanges OTC (over the counter) desks. This number accounts for money laundering in any form, not strictly in the drug markets. In terms of darknet market overall sales, 2019 accounted for around \$790 million of Bitcoin and other cryptocurrencies - roughly 0.08% of all crypto transactions.

## **THROWING THE BABY OUT WITH THE BATHWATER**

While it can be easy to highlight illicit uses of Bitcoin and other digital currencies, it is essential to examine the positives that can be accomplished. As with any new technology, anyone can use it in any way they see fit. The Internet was villainized for the type of content that can be shared, but today one would be hard-pressed to find someone blaming a global communication network for a crime executed on it. It would be equally ridiculous to blame paper money in the wake of a bank robbery. It is easy to conflate the crime with the medium, but it does not make much sense in practice. Demonizing Bitcoin because some use it to purchase illicit goods is equally misdirected.

At its core, Bitcoin is a tool through which the world can achieve the separation of money and state. While this may not be of interest to those living in 1<sup>st</sup> world countries with relatively stable currencies, it can be quite another story in totalitarian regimes with capital controls, disastrous monetary policy, and hyperinflation.

In mid-2019, Venezuela saw its hyperinflation reach a staggering 10 million percent. A promising developing nation sitting atop one of the world's largest oil reserves was devastated in less than a decade. Citizens saw their life savings' purchasing power disappear as they rushed with wheelbarrows full of cash to purchase goods before the paper became worthless. For those who understood the promise, Bitcoin became a conduit through which they could preserve wealth, escape capital controls, and participate in the global economy without the state's oppression.

While not as extreme, Argentina sees its second currency crisis of the 21<sup>st</sup> century as the peso is devalued at breakneck speed. Curiously (or perhaps not), the volume on local bitcoin trades has spent the better part of the past two years breaking new records as locals find ways to escape the opportunity costs of holding the local money. Further examples of this can be seen in Lebanon, Turkey, Iran, Zimbabwe, and others.

Given the above, if the collective impression and subsequent regulation of Bitcoin are informed only to the headline-grabbing negative uses, we could put ourselves in a position where many people in need could be deprived of a potentially life-saving tool in the process.



## **NO ONE CAN SHUT DOWN BITCOIN**

Thus far, with the information provided, one might assume that Bitcoin could be turned off or potentially regulated out of existence, given we came to a global agreement. At this doubtful point. With each passing day, it becomes increasingly difficult (Coinbase, 2020).

As previously mentioned, Bitcoin is a distributed network governed by a set of consensus rules enforced by users running software and secured by the world's most robust computer network. The absolute indifference of network peers would simply meet an attempt to reverse or censor transactions.

An attempt to attack the network by obtaining most of its computing network would cost in the realm of USD 10 million per day, assuming one acquired the billions of dollars worth of hardware to execute the attack in the first place. These costs would rise over time as the network grows.

An attempt to prevent network traffic from happening at all would presumably require the Internet to be effectively shut off. This type of attack would, of course, stunt the network - but only temporarily. Bitcoin transactions can be executed via satellite and short-wave radio and 100% offline via cryptographically secured bearer bonds.

What could be attempted is an overbearing regulatory attack on a global scale - outlawing Bitcoin's ownership and use altogether with strict penalties for transgressions. To be sure, this would grind much innovation to a halt. However, the network would continue to chug along, processing transactions whenever they were broadcast to the system.

Bitcoin itself is unaware of the law. It is a protocol that will continue to execute as designed if people support the network. People would still find ways to run the software (much like people still use BitTorrent despite the illegality of piracy and file sharing). Besides, those who most needed it would indeed utilize Bitcoin as a method to transact as they please - whether it be to buy illicit substances or evade crushing monetary policy. In an age where money has transcended physicality and becomes speech, the speculator becomes indecipherable from the drug pusher and the financial refugee. It has all simply become a new global language for value.

## **ANALYSIS AND CONCLUSION**

The emerging trends surrounding blockchain and digital fraud demonstrate a fundamental misunderstanding of the digital world's perils and depths (Sujit & H., 2019). It is of the opinion of the authors of this chapter that primary legislative intervention is introduced. While regulating the marketplace of digital currencies and decentralized technologies seem opportune, legislative action should focus on educating these technologies and innovations. As demonstrated by the research cited, the weakest chain in the digital age's future security is humans. Focusing legislative action around education strengthens the metaphorical "weak chain" in the digital revolution equation. Providing constituents with the tools necessary to identify TFA fraud, as an example, would stifle the growing costs mentioned surrounding this trending crime. The cost of resources to disseminate the digital world's fundamentals would seem to be the biggest hurdle politically. However, in reality (in the opinion of the authors of this chapter), the costs of educating would not only reduce the overall cost of fraud theoretically; but it would stimulate the economy by providing future incentive to keep IoT and household electronics up to date.

In conclusion, the information laid out was done to demonstrate a particular point: Blockchain technology created cryptocurrency, and cryptocurrency is what fuelled DW trade to the levels they have

reached today, where fraud guides are sold on platforms for a few dollars and cents through digital currency. The best course of action to mitigate these types of frauds or defend against social engineering is to be cautious of the information you share on digital platforms or even in person. Publicly sharing information can cause a butterfly effect should provide a lousy actor cross-path. It is important to note, before paranoia sets in, that reports also suggest that, ironically, many dark fraud guides are fraudulent in and of themselves (Potter, 2018). Understanding blockchain technology and knowing the ins and outs of fraudulent behaviour are crucial to the success of a digital, cashless future. The authors believe that government-subsidized education should be provided globally, as education is one of the most powerful tools we possess (Rahman et al., 2020). If there is any chance to fight those who choose to sell and profit from exploitation and deception, we must be armed with the education needed to defend against it.

## DISCLAIMER

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## ACKNOWLEDGMENT

The author extends sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and fine-tuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the author to complete this task.

## REFERENCES

- Abdulai, A. M. (2020). Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud. *International Journal of Cyber Crime*, 14(1), 157–174. doi:10.5281/zenodo.3749468
- Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, 100, 408–427. doi:10.1016/j.future.2019.03.041
- Apple. (2020). *Families*. Retrieved from <https://www.apple.com/ca/families/>

- Asif, S. (2020, April 18). Fraud & hacking guides are the most sold item on the dark web. *Hack Read*. Retrieved from <https://www.hackread.com/fraud-hacking-guides-most-sold-item-dark-web/>
- Asokan, A. (2020, April 18). What's Hot on Dark Net Forums? 'Fraud Guides'. *Data Breach Today*. Retrieved from <https://www.databreachtoday.com/whats-hot-on-dark-net-forums-fraud-guides-a-14142>
- Bacon, M. (2018). Social Engineering, TechTarget. *SearchSecurity*. Retrieved from <https://searchsecurity.techtarget.com/definition/social-engineering>
- Bolton, R. J., & Hand, J. D. (2002). Statistica; Fraud Detection: A Review. *Statistical Science*, 17(3), 235–355. doi:10.1214s/1042727940
- Bradley, R. (2020). Blockchain explained... in under 100 words. *Deloitte*. Retrieved from: <https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/blockchain-explained.html#>
- Brown, D. B. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal: Theory. Practice and Principles*, 89(4), 327–339. doi:10.1177/0032258X16658927
- CAFC. (2020). *Canadian Anti-Fraud Centre*. Retrieved from <https://www.antifraudcentre-centreanti-fraude.ca/>
- CBC. (2020a, July 16). FBI probing high-profile Twitter hack that experts say undermines trust in the platform. *CBC News*. Retrieved from <https://www.CBC.ca/news/technology/twitter-breach-hack-1.5651675>
- CBC. (2020b, July 31). 3 charged in high-profile Twitter hack targeting Barack Obama, Bill Gates, others. *CBC News*. Retrieved from [https://www.CBC.ca/amp/1.5670061?\\_\\_twitter\\_\\_impression=true](https://www.CBC.ca/amp/1.5670061?__twitter__impression=true).
- Chang, Y., Lakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research*, 58(7), 2082–2099. doi:10.1080/00207543.2019.1651946
- Chertoff, M., & Simon, T. (2015, February). *The Impact of the Dark Web on Internet Governance and Cyber Security* (Paper Series: No. 6). The Centre for International Governance Innovation and Chatham House. Retrieved from: [https://www.cigionline.org/sites/default/files/gcig\\_paper\\_no6.pdf](https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf)
- Coinbase. (2020). *What is Bitcoin?* Retrieved from: <https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin>
- Coindesk. (2020). *Dogecoin*. Retrieved from: <https://www.coindesk.com/crypto/dogecoin>
- Conrad, N. P., & Wahsheh, L. A. (2020). Simon Says: “Send Money.” *Journal of Systemics, Cybernetics and Informatics*, 18(3), 54-55. Retrieved from <http://www.iiisci.org/journal/sci/FullText.asp?var=&id=ZA380TJ20>
- Cox, J. (2019 October 8). Twitter Took Phone Numbers for Security and Used Them for Advertising. *Vice*. Retrieved from: <https://www.vice.com/en/article/9kez8d/twitter-took-phone-numbers-for-security-used-for-advertising>
- Dark Reading Staff. (2020). FBI Warns on New E-Commerce Fraud. *Dark Reading*. Retrieved from <https://www.darkreading.com/attacks-breaches/fbi-warns-on-new-e-commerce-fraud/d/d-id/1338534>

FATF. (2020). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Financial Action Task Force. Retrieved from: <https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>

Ferguson, R. H. (2017). Offline ‘stranger’ and online lurker: Methods for an ethnography of illicit transactions on the darknet. *Qualitative Research*, 17(6), 683–698. doi:10.1177/1468794117718894

Fraud.net. (2020). *Fraud definitions*. Retrieved from: <https://fraud.net/d/fraud-definition/>

Gogan, M. (2018, April 4). Man-in-the-Middle (MITM) Attacks: What They Are And How To Prevent Them? *Equities*. Retrieved from <https://www.equities.com/news/man-in-the-middle-mitm-attacks-what-they-are-and-how-to-prevent-them>

Graham, R., & Pitman, B. (2020). Freedom in the wilderness: A study of a Darknet space. *Convergence (London)*, 26(3), 593–619. doi:10.1177/1354856518806636

Gupta, R. P., & Biswas, B. (2021). Banking Scams in India: A Case Based Analysis. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Hacquebord, F., & Pernet, C. (2017). *Drilling Deep*. Retrieved from <http://www.a51.nl/sites/default/files/pdf/wp-drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry.pdf>

Hadnagy, C. (2018). *Social Engineering* (2nd ed.). Wiley. doi:10.1002/9781119433729

IBM. (2020). *Blockchain*. Retrieved from <https://www.ibm.com/blockchain/what-is-blockchain>

Insurance Information Institute. (2020). *Facts + Statistics: Identity theft and cybercrime*. Retrieved from: <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>

Javelin. (2020). *Javelin Strategy & Research*. Retrieved from <https://www.javelinstrategy.com/>

Jayasekara, S. F. S. D. (2021). Risk-based AML/CFT Regulations for Effective Supervision. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Karpoff, J. M. (2020). The future of financial fraud. *Journal of Corporate Finance*, 101694. doi:10.1016/j.jcorpfin.2020.101694

Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2018). ATM Card Cloning and Ethical Considerations. *Science and Engineering Ethics*, 25(5), 1311–1320. doi:10.1007/11948-018-0049-x PMID:29717470

Kay, M. M. C., & King, M. C. (November 2019). *Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm*. Paper presented at the 2019 IEEE International Symposium on Technology and Society (ISTAS), Medford, MA. Retrieved from <https://ieeexplore.ieee.org/abstract/document/8938009> doi:10.1109/ISTAS48451.2019.8938009

Kemp, S., Miro-Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, 26(3), 293–312. doi:10.1007/10610-020-09439-2

Kenthineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), 325–344. doi:10.1177/1057567719827051

- Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, 55, 102018. doi:10.1016/j.scs.2020.102018
- Khan, M. T., & Kanich, C. (2017). Old is Still Gold: A Comparison of Cyber and Traditional Consumer Fraud in The United States. *IEEE*. Retrieved from <https://www.ieee-security.org/TC/SPW2017/ConPro/papers/khan-conpro17.pdf>
- Kiley, D. (2018, August 23). Wanna Buy a Lamborghini Quickly? You Can Use Cryptocurrency at the Big Auctions Now. *Forbes*. Retrieved from: <https://www.forbes.com/sites/davidkiley5/2018/08/23/wanna-buy-a-lamborghini-quickly-you-can-use-crypto-currency-at-the-bonham-auction/?sh=4957d77c4ed>
- Labs, T. (2020). *Fraud Guides 101*. Retrieved from <https://terbiumlabs.com/>
- Laleh, N., & Azgomi, M. A. (2009, March). A taxonomy of frauds and fraud detection techniques. In *International Conference on Information Systems, Technology and Management* (pp. 256-267). Berlin: Springer. 10.1007/978-3-642-00405-6\_28
- Loukas, G., Patrikakis, C. Z., & Wilbanks, L. R. (2020). Digital Deception: Cyber Fraud and Online Misinformation. *IT Professional*, 22(2), 19–20. doi:10.1109/MITP.2020.2980090
- Mayer, A. H., da Costa, C. A., & Righi, R. D. R. (2020). Electronic health records in a blockchain: A systematic review. *Health Informatics Journal*, 26(2), 1273–1288. doi:10.1177/1460458219866350 PMID:31566472
- McMillan, E. (2019, July 25). Cybercrime is going up across Canada, and most cases remain unsolved. *CBC News*. Retrieved from <https://www.CBC.ca/news/canada/nova-scotia/cyber-crime-rising-across-canada-1.5221330>
- Newman, L. H. (2019, October 9). Never Trust a Platform to Put Privacy Ahead of Profit. *Wired*. Retrieved from <https://www.wired.com/story/twitter-two-factor-advertising/>
- Onwubiko, C. (2020). Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. *Computers & Security*, 96, 101838. doi:10.1016/j.cose.2020.101900
- Owen, G., & Savage, N. (2015, September). *The Tor Dark Net* (Paper Series: No. 20). The Centre for International Governance Innovation and Chatham House. Retrieved from <https://www.cigionline.org/publications/tor-dark-net>
- Potter, K. (2018). *Increased use of two-factor authentication force new social engineering tactics*. (Publication No. 10789454) [Master's thesis, Utica College]. ProQuest Dissertations Publishing.
- Rafay, A. (Ed.). (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

## Dark Web

Rahman, N. A. A., Zizi, N. A., Sairi, I. H., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology (IJIET)*, 10(5), 378–382. doi:10.18178/ijiet.2020.10.5.1393

Reuters. (2020, July 17). Twitter says about 130 accounts were targeted in cyberattack this week. *CBC News*. Retrieved from <https://www.cbc.ca/news/technology/twitter-accounts-hacked-1.5653200>

Sarker, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Mining user interaction patterns in the dark web to predict enterprise cyber incidents. *Social Network Analysis and Mining*, 9(1), 1–28. doi:10.1007/13278-019-0603-9

Shah, S. (2021). Compliance Monitoring and Testing Seismometer to Detect Compliquake. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Sinha, A. (2021). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.

Sujit, S. (2019). A Research on Cyber Security Awareness based on Big Data. *International Journal of Recent Technology and Engineering*, 8(2S8, 2SA), 1798–1802. doi:10.35940/ijrte.B1156.0882S819

The Verge. (2020). Retrieved from <https://www.theverge.com/>

Thomas, B., Clergue, J., Schaad, A., & Dacier, M. (2004). *A comparison of conventional and online fraud*. SAP Research, Sophia Antipolis, France. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.194.1307&rep=rep1&type=pdf>

UN. (2020). *Money-Laundering and Globalization*. United Nations. Retrieved from <https://www.unodc.org/unodc/en/money-laundering/globalization.html>

Vasquez, M. H. (2017). The Financial Crimes Management of Account Takeover Fraud. *The University of Texas*. Retrieved from <https://repositories.lib.utexas.edu/bitstream/handle/2152/63762/VASQUEZ-MASTERSREPORT-2017.pdf>

Wetsman, N. (2020, September 17). Woman dies during a ransomware attack on a German hospital. *The Verge*. Retrieved from: <https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity>

Whiteman, J. R., III. (2017). *Social engineering: Humans are the prominent reason for the continuance of these types of attacks* (Doctoral dissertation). Utica College.

# Chapter 25

## Dark Web: A Breeding Ground for ID Theft and Financial Crimes

**Annamaria Szakonyi**

*Saint Louis University, USA*

**Brian Leonard**

*Civil Rights University, USA*

**Maurice Dawson**

 <https://orcid.org/0000-0003-4609-3444>

*Illinois Institute of Technology, USA*

### ABSTRACT

*The explosion of the internet has given rise to cybercrimes, online identity theft, and fraud. With the internet, these crimes are able to occur anywhere in the world and limitless to whatever selected target. The anonymity of the internet allows criminal activity to flourish, and the number of unsuspecting victims is growing. From script kiddies to nation-states, this new method of internet-enabled crimes has strained governments. This chapter provides insight into how crimes related to online identity theft and fraud are carried out. Examined within this chapter are the evolution of cybercrime, history of identity theft, applications for internet anonymity, and discussion on effects caused by romance scams and data breaches. Finally, recommendations are provided on what organizations and individuals can do to protect themselves against these vicious crimes.*

### BACKGROUND: DEFINITION AND THE RISE OF CYBERCRIME

Cybersecurity has gone through several changes that have presented new challenges in recent years, complicated by the rise of cybercrime. The technological advancements associated with the mass implementation of the Internet of Things (IoT) and Internet connectivity to everyday devices have led to an explosion in cyber-attacks such as breaches resulting in millions of accounts being compromised (Dawson

DOI: 10.4018/978-1-7998-5567-5.ch025

*et al.*, 2016). Bad actors such as those focused on criminal activities regarding human trafficking and espionage navigate the technology domains to circumvent law enforcement agencies globally. We must understand how exploitation, circumvention, and defense needs to occur in order to assure security. The threat landscape has shifted, and defenders have to become knowledgeable about how the cyber domain crosses into various areas. The traditional thinking of protecting enterprise systems locked away in a building is no longer applicable.

Executive Orders (EO), laws, policies, doctrines, and other directives have shaped the landscape of Cybersecurity. New EOs have been released that allow a cyber-attack with responsive measures such as one that involves military force. Laws created that impose rights for Personal Identifiable Information (PII) being breached, leaving millions of individuals unprotected. One of these most well-known items is the General Data Protection Regulation (GDPR) as it relates to the European Union (EU) and the evolving threats with hyper connectivity (Martínez, 2019a; Martínez, 2019b). Understanding the role of cybercrime and how it continues to shape the technological landscape is critical. These various actions change the spectrum regarding combating nefarious actors or design errors that leave systems susceptible to threats.

In today's world of ever-changing technological advances, maintaining the safety and security of personal and sensitive information via the Internet is increasingly at the forefront for most industries and government authorities alike. As a result, the prevention of cybercrime is generally the initial starting point for these agencies. To understand the significance and prevalence of cybercrime, it is necessary to begin with defining this term. In the initial instance, cybercrime may also be referred to as "computer crime," which is defined as a crime perpetrated using a computer, or with knowledge of computer technology, generally through theft of computer data (Black's Law Dictionary, 2019). Thus, an essential element of cybercrime is the use of computer technology. Since computer technology as a phenomenon is a creature of the late twentieth century it follows that the emphasis on and prosecution of cybercrime would develop around the same timeframe (Rafay, 2019).

Accordingly, beginning with the 1980's, Congress passed a series of criminal laws and amendments to "criminalize the conduct of computer 'hackers' and similar abusers of computer systems or programs" (Business Crimes, 2013). These legislative efforts reflected the sentiment among federal lawmakers as to the importance of protecting information and computers from criminal conduct. However, much of the impetus for laws that would become the initial national attempts to regulate cybercrime ironically developed primarily from the desire to create clarity as to the fourth amendment privacy protections for electronic information. This is true despite the statements by members of Congress that it was necessary to prevent hackers and to stop what they termed would be a "new breed" of criminal, one using computer technology to steal information and commit new crimes (API Tech Servs., LLC v. Francis, 2013).

## History and Development of Cybercrime Regulations

In many ways the evolution of cybercrime can be viewed through the lens of the regulations that were adopted to combat it. At the federal level for instance, Congress passed two primary laws designed to deal with cybercrime: the Stored Communications Act (SCA), (as a part of the Electronic Communications Privacy Act), and the Computer Fraud and Abuse Act (CFAA). The efficacy of these laws must be measured by the time and limitations on technology that existed almost forty years ago, when they were enacted. Thus, the SCA made the unauthorized access of an electronic communication services facility or exceeding such access a crime (Electronic Communications Privacy Act, 1986). Meanwhile



the CFAA made it illegal to gain unauthorized access to a “protected computer” and obtain information, use of the same with the intent to defraud, and obtaining value in excess of \$5,000 within a 1 year period through fraud, as well as gaining access to a protected computer intentionally and causing loss or damage (Computer Fraud and Abuse Act, 1986). Under the CFAA, a “protected computer” is one that is used in or to affect interstate or foreign commerce (Computer Fraud and Abuse Act, 1986).

Furthermore, some states also criminalized similar conduct as that under the CFAA. For instance, the Virginia Computer Crimes Act (VCCA) made it unlawful to engage in fraud, or the unauthorized use of a computer or network, to obtain property by false pretenses as well as to engage in theft of computer services, which was defined as obtaining unauthorized access to computer services (*A.V. v. iParadigms LLC*, 2009). Similarly, North Carolina’s criminal trespass law made it unlawful to intentionally and without authorization use a computer or network to disable, remove, alter, or otherwise halt data temporarily or permanently, or to make a copy of such data without permission (North Carolina Computer Trespass Act, 2016). Accordingly, the initial federal cybercrime regulations as well as those of some states, were aimed at what lawmakers saw as the rise of hackers or those seeking to access computers and engage in harmful conduct. Additionally, through a series of cases, the courts interpreted both the SCA and the CFAA as being almost identical in their application, except that the SCA also applied to a facility, while the CFAA applied to computers (*United States v. Cioni*, 2011). Furthermore, the Courts as a general rule did not apply the CFAA to the “rogue employee” who had authority to access to computers and information of the employer and then engaged in unauthorized use of the same in violation of the employer’s policy (*WEC Carolina Energy Solutions LLC v. Miller*, 2012). Thus, in the early stages of cybercrime the conduct circumscribed by criminal law was very straightforward in nature. However, as with most things with technology and the law, this would not stay that way. While the CFAA and the SCA are still primary sources of law enforcement for cybercrime, the methods and forms of attacks have shifted from primarily hackers in the beginning to things such as ransomware and malware attacks, to businesses, schools, and government agencies using public and private networks (FBI, 2020).

## Nigerian “419” Fraud

### Definition

“419” Fraud, is an advanced fee fraud that generally involves unsolicited communication, via letter, fax, and later on e-mail, with a request for assistance sending money from a foreign official, in many cases, but not exclusively, purporting to be Nigerian (Durkin & Brinkman, 2009). The “419” designation refers to the section of the Nigerian penal code that prohibits this kind of activity. While the scheme purports to have financial benefits for the recipient, eventually it requires the payment or sending of funds, generally, via wire through Western Union to an international destination (Durkin & Brinkman, 2009).

### Incidence

While the methods have changed, this type of scheme is not new nor is it necessarily limited to Nigeria. In fact, the scam only began being used in Nigeria in the last 40 years, when it faced economic challenges as a nation (Dyrud, 2005). With the advent of the Internet, perpetrators have taken to using this new medium of technology to successfully implement this scheme. The use of free e-mail accounts and services that allow perpetrators to send out mass e-mails have made it easier to execute this fraud (Rafay,

## **Dark Web**

2021). Although the 419 Fraud is popularly referred to as Nigerian, scammers have operated in various African countries besides Nigeria, such as Ghana and Sierra Leone, as well as non-African countries including the United States, Canada, Great Britain, and Japan.

The 419 Fraud angles have changed but range from a “severely ill relative” needing money to someone who is victimized by a natural disaster or other catastrophe, that needs money. However, the tactics have gotten more sophisticated, and as a result have been successful in attacking law firms, for instance, posing as a legitimate attorney using a real person, and a real company that is not actually involved in the transaction (McDonough, 2010). The law firm is generally contacted and asked to facilitate some transaction usually involving the depositing of funds in a law firm trust account and then wiring funds to another attorney or client. Unfortunately, the law firm only finds out later that the funds and the transaction is fraudulent and is now suffering a significant loss (McDonough, 2010). In addition, small law firms are not the only targets of such fraud, as some large firms have also been victimized by these types of schemes (Weiss, 2009). In fact, law firms have become such popular targets of these 419 Fraud schemes, that state bar associations and agencies have consistently issued warnings to lawyers and law firms about the potential for these scams (Tennessee Bar Association, 2009).

## **Damages**

It is estimated that a quarter of a million people have been involved in 419 Fraud (Durkin & Brinkman, 2009). As an example of the high costs to victims of this fraud, law firms have incurred losses of between \$400,000 and \$500,000 per occurrence (McDonough, 2010; Weiss, 2009). Moreover, the costs globally of 419 Fraud, were up to \$3.1 billion, with estimated losses of \$720 million in the United States alone, in 2005 (Durkin & Brinkman, 2009). The costs to individuals tend to be more devastating, with losses in the tens of thousands of dollars. Perhaps one of the most underrated costs due to 419 Fraud is on the reputation of Nigeria itself as a nation. Although this scheme is not exclusive to the country, the fact that this fraud is most closely associated with Nigeria, has resulted in a general distrust of Nigerian enterprises, particularly Internet service providers and software companies in Nigeria (Durkin & Brinkman, 2009).

## **Response**

As a direct result of the 419 Fraud, the FBI created tips to help citizens avoid becoming victims of this scheme. These tips include sending letters or e-mails from Nigeria requesting personal or banking information, to the FBI or other federal agency, and instructions not to respond (FBI, 2020). The tips also include warnings about individuals posing as officials from Nigerian or other international governments, as well as a link for registering a complaint with the Federal Trade Commission (FTC).

The FTC is the core organization in the efforts to curb cybercrime, with various resources available to consumers and business. This government agency was set out to enforce transparency and investigate wrongdoings related to individuals’ data (Kesari, 2020b). Over 20% of all fraud complaints submitted to the FTC are related to identity theft (Alagna, 2020). Their central database, the Consumer Sentinel, contains over 20 million self-reported identity theft complaints collected from a variety of different agencies and non-profit organizations (Kesari, 2020a). Their role spans from consumer reporting to the distribution of identity theft prevention practices (Tajpour & Zamani, 2020), explained in detail in the next paragraphs.

## The Federal Trade Commission: The Federal Shield from ID Theft

### History and Creation

The Federal Trade Commission was created by the Federal Trade Commission Act, (“the Act”), in 1914, with a mission to protect consumers from deceptive practices and promote fairness and competition (Federal Trade Commission Act, 1914). Accordingly, the FTC has been the one-stop source for consumers in protecting themselves from false or misleading advertising, including such tactics as “bait and switch” as well as overly aggressive selling practices including against vulnerable populations that may be easily influenced into a commercial transaction that they would not otherwise engage in. For instance, the FTC administers the Telemarketing Sales Rule, and the Equal Credit Opportunity Act (Federal Trade Commission, 2020a).

### FTC’s Role in ID Theft

Given its history, mandate, and unique powers and duties, the FTC wears multiple hats in terms of protecting consumers from Identity Theft, including Enforcement, Education, Policy, and Cooperation and Coordination.

Of all the functions of the FTC, one of its most powerful is to enforce the laws designed to protect consumers. The FTC’s authority includes investigation, subpoena power, and compiling evidence to gather information into potential violations of consumer protection law. In addition, if the FTC discovers violations, it has the authority to bring legal actions through the administrative and judicial processes to seek corrective actions. Actions taken to remedy violations include issuing administrative orders, civil penalties, and seeking injunctive relief through court order to stop the actions that the FTC deems are violations of law or administrative rules. Finally, the FTC is empowered within itself to adopt administrative regulations and rules to govern consumer protection and unfair and deceptive trade practices.

In terms of Identity Theft, specifically, the FTC can take legal action to ensure that businesses take sufficient precautions to safeguard consumer privacy and information to protect against identity theft and fraud. For example, the FTC recently sued Khol’s Department Stores in federal district court in Wisconsin, for failure to provide adequate business records to its customers that were victims of identity theft (United States of America v. Kohl’s Department Stores, Inc., 2020). In order to resolve this claim, Khol’s agreed to pay \$220,000, in civil penalties, to provide sufficient notice to victims of identity theft that Khol’s will provide a website and contact information for where they can obtain information about identity theft and sufficient business records for such victims (United States of America v. Kohl’s Department Stores, Inc., 2020).

The FTC also provides a platform for consumers to report infractions related to identity theft on their dedicated site, IdentityTheft.gov (Federal Trade Commission, n.d.). After reporting an incident, consumers can get assistance developing a personal recovery plan through this site and track their progress through the recovery process with this easy-to-use, online tool.

In addition to its enforcement efforts, the FTC plays a critical education role for protecting consumers. Specifically, the FTC provides a plethora of online resources at [ftc.gov](https://www.ftc.gov), for consumers, including public statements, blogposts, and tips and advice kits for consumers to help protect themselves. As it relates to identity theft specifically, the FTC provides and maintains the federal government’s primary website for identity theft victims, at IdentityTheft.gov. This resource includes information on filing a complaint

## **Dark Web**

with the FTC, getting sample letters and other documents that identity theft victims may need to dispute transactions with debit card and credit card institutions as well as with credit bureaus. Furthermore, this resource provides a helpful summary to consumers about their rights for protecting themselves against identity theft. Some of these rights include creating an Identity Theft report, placing fraud alerts on credit reports, and obtaining copies of documents relating to identity theft (Federal Trade Commission, n.d.).

Furthermore, the FTC plays an important role from a policymaking standpoint, not only through its own rulemaking but also providing advocacy letters, filing amicus briefs in court actions, giving Congressional testimony, and issuing advisory opinions (Federal Trade Commission, 2020a). Thus, the FTC will issue advocacy letters to other agencies or organizations that consider issues that are relevant to identity theft and consumer protection. In addition, the FTC will file amicus legal briefs with courts, where the FTC is not a party, but it determines it is necessary to highlight issues of importance in cases where a potential judicial ruling may have a broader effect on identity theft rights in the future. Furthermore, FTC officials may testify in Congressional hearings where Congress may consider legislation that affect identity theft laws and protections for consumers.

In addition to its other duties and activities, the FTC works in cooperation with its international counterparts to promote consumer protection around the globe, including protection against identity theft. Through its cooperative efforts, the FTC encourages best practices to prevent identity theft inside the U.S. and abroad. This is important, given that identity theft is considered a “borderless” crime, and international collaboration helps the FTC fulfill its mission to protect consumers to the greatest extent possible.

## **CYBERCRIME TODAY**

With the prevalence and advancement of technology, cybercrime and online identity fraud have evolved to various methods. Generally, the goal of identity fraud is financial gain, but the methods can take on different forms for execution. They can range from massive technical engagements of well-planned and executed data breaches to social engineering and falsifying online identities to gain trust and information from an individual. In this section, some examples of online identity theft will be discussed.

### **Data Breaches**

Corporate data breaches are a common type of identity theft. Data breach is an incident where confidential or protected data is exposed and accessed without permission (Symanovich, n.d.). The reasons for data breaches can be diverse. Hacking and social engineering are the top reasons for data breaches, but human error is a steadily increasing cause (Verizon, 2020). Data breaches harm both businesses and consumers (Norton, 2020). The last century has seen various notorious data breaches that affected millions of customers in the United States. Not only are these crimes occurring more often, but they also cost more for organizations to repair (Manworren *et al.*, 2016). Globally, the average cost to a company of a data breach is \$3.86 million, or \$148 on average per stolen record (Norton, 2020). This last decade has seen various high-stakes data breaches that are worth mentioning.

The Target data breach during the holiday season in 2013 was due to a malware installed on the retail chain’s security and payments system (Manworren *et al.*, 2016). Hackers stole credit card information by hacking into their point-of-sale (POS) system and recording credit card information during the holiday

shopping transactions (Manworren *et al.*, 2016). The incident resulted in roughly 40 million credit and debit card numbers and over 70 million customer records being compromised (McDaniel, 2019). Even though Target's security system should have been able to contain this malware, their security team ignored various intrusion detection alerts that led to the successful attack of 12 days (Manworren *et al.*, 2016; McDaniel, 2019). Due to this breach, Target's profits fell 46% compared to the previous year's holiday period and resulted in significant loss of reputation and trust of their customers and investors (Manworren *et al.*, 2016). Target was also forced to pay millions in customer relief funds as well as in settlements with various financial institutions, totaling about \$290 million (Manworren *et al.*, 2016).

The data breach that affected FriendFinder Networks in 2016 resulted in 412 million hacked accounts (Swinhoe, 2020). The stolen data included names, email addresses, join dates, usernames and passwords of users and contained data of 20 years (Peterson, 2016). Hackers attacked FriendFinder's systems by exploiting an injection vulnerability that gave attackers access to the source code of their sites (Dickey, 2016). This data breach was particularly sensitive due to the nature of their services offered, including casual hookup and adult content websites such as Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com (Swinhoe, 2020). FriendFinder failed on multiple levels. First of all, they stored user passwords with no protection in plaintext, or with a weak SHA1 hashing algorithm (Dickey, 2016). Second, they kept information of users who had deleted their accounts or owned accounts on retired sites they didn't run anymore (Dickey, 2016; McDaniel, 2019). Finally, they failed to report the incident in a timely manner to their users (Dickey, 2016).

The Equifax credit bureau data breach of 2017, compromising personal information such as names, Social Security Numbers, birth dates, addresses, driver's license numbers, and 200,000 credit card numbers, affected more than 147.9 million American consumers (McDaniel, 2019; Swinhoe, 2020; Symanovich, n.d.). An application vulnerability in one of their web applications led to the exposure of data (McDaniel, 2019; Swinhoe, 2020). Equifax was extremely slow in reporting the breach: it was only discovered about 2 months after the actual attack (Swinhoe, 2020). Equifax agreed to a \$425 million settlement to cover expenses for people affected by the data breach (Federal Trade Commission, 2020b).

In 2018, Marriott International was hacked, exposing the personally identifiable information of 500 million guests, including names, phone numbers, email addresses, birth dates, passport numbers and travel information (Swinhoe, 2020; Symanovich, n.d.). The attack went unreported for years: the initial breach started in the Starwood hotel systems in 2014, however, after Marriott acquired Starwood in 2016, the attackers managed to continue exploiting the system until they were discovered in 2018 (Swinhoe, 2020). Marriott believes that the credit card information of about 100 million customers were also exposed, however it was uncertain if the hackers were successful in decrypting that data (Swinhoe, 2020). An unauthorized user managed to take control of an account with administrator privileges, and was only discovered when it made an unusual database query that was flagged by Marriott's security tool (Fruhlinger, 2020). Investigation revealed that malicious Remote Access Trojan (RAT) and a tool capable of recording username/password combos in system memory were deployed, probably from a phishing email (Fruhlinger, 2020). By March 2019, Marriott reported \$28 million in expenses related to the breach, which increased by \$120 million in July 2019, when the UK imposed a fine for violating British citizens' privacy rights under the European General Data Protection Regulation (GDPR) (Fruhlinger, 2020). The New York Times reported that the breach was associated with a Chinese intelligence group that also hacked security clearance information of millions of US citizens (Fruhlinger, 2020; Sanger *et al.*, 2018; Swinhoe, 2020).

In 2019, Capital One suffered a data breach impacting 106 million credit card customers and individuals who applied for Capital One credit card products (Capital One, 2019; Symanovich, n.d.). The breach exposed about 140,000 US Social Security Numbers, 80,000 bank accounts, and 1 million Canadian Social Insurance Numbers (Capital One, 2019; Symanovich, n.d.). The largest category of data was related to credit card product applications of consumers and businesses, which included names, addresses, phone numbers, email addresses, dates of birth, and income (Capital One, 2019). A firewall misconfiguration on the company's Amazon Web Services (AWS) infrastructure enabled the intruder to access their systems (Lu, 2019). The perpetrator, a previous AWS employee, was eventually captured by the FBI (Capital One, 2019; Lu, 2019). Capital One estimated that the breach would reach \$100-150 million for 2019, but total estimates state the breach will exceed \$200 to \$300 million (Lu, 2019).

## **Online Dating Scams**

Online dating is a prime platform for identity fraud. Online dating offers a fast and convenient way to establish new potential romantic connections from the safety and convenience of one's home, together with a level of anonymity. However, with this anonymity, it also opens opportunities for fraud (Rege, 2009). According to the FTC, people reported losing \$201 million to romance scams in 2019 (Federal Trade Commission, 2019a). The median individual loss to a romance scam in 2018 was \$2,600 (Federal Trade Commission, 2019b). The losses reported related to romance scams are higher than any other type of fraud reported to authorities (Federal Trade Commission, 2019a, 2019b).

The process of online scams generally goes by the following script. The perpetrator sets up a fake profile on an online dating app, or contacts their targets through a fake profile on social media such as Facebook (Federal Trade Commission, 2019a; National Consumers League, 2011). Often, they steal attractive photos and the identity of a real person from other sites (Federal Trade Commission, 2019c). They slowly build the trust of the victim by constant communication, showering them with continued affection and sometimes even with gifts (National Consumers League, 2011). Their lies generally include a foreign job or assignment, such as being deployed abroad through the military or being a doctor with an international organization (Federal Trade Commission, 2019a). Once the target's trust is gained, perpetrators invent an emergency or hardship and request money from their victim for expenses such as plane tickets, medical expenses, paying off debts, or other made-up excuses, often continuing the cycle of financial abuse of their victims (Federal Trade Commission, 2019a; National Consumers League, 2011).

The difficulty with these romance scams, or "sweetheart swindles", is multifold (Fraud.org, 2020). First of all, with the prevalence of online dating, finding targets is extremely easy for perpetrators. With the help of technology, they can reach across continents and time zones, and the anonymity provided makes their efforts successful due to their ability to take on false identities seamlessly. In addition, victims are often ashamed and embarrassed to turn to law enforcement after these incidents, and they often believe that they are responsible for their own victimization (Rege, 2009). When these crimes don't get reported in a timely manner, other victims can be targeted and successfully tricked by the same offenders. Due to the international nature of this crime, it is sometimes also difficult to investigate, since cross-border cooperation may be necessary to hold the responsible parties accountable.

Finally, extortion and emotional blackmail are also common during these interactions (Rege, 2009). Criminals often play on the emotions of the victim when they are unwilling to send money, accusing them of not caring for or not truly loving their partner (Rege, 2009). Sextortion is another tool often used by offenders to get victims to comply. During the 'honeymoon' phase of the new relationship, perpetra-

tors convince victims to perform intimate or sexual acts in front of their webcams, which the offenders record and later use to blackmail their prey into adhering to their demands (National Crime Agency, n.d.).

It is apparent that one must be mindful of trusting online identities. This is no different in the online dating game. It is becoming more and more popular on dating sites to require verification of profiles. Tinder implemented a photo verification process, making it possible for users to verify their photo identities by taking real-time selfies in certain poses and matching those to their Tinder profile pictures using facial recognition technology (Tinder, n.d.). Other apps may rely on outside verification, such as providing copies of identity documents such as driver's license. However, these can also present some flaws, namely, when not only profile information but other personal information related to the individual are also abused.

## The Art Behind Identity Fraud: Social Engineering

Social engineering is the basis of various identity theft and fraud type scenarios, such as the online dating incidents mentioned in the previous section. Social engineering is the art and science of skillfully manipulating a person to take action in some aspect of their lives that may or may not be in the target's best interest (Hadnagy, 2010). Due to social engineering not always serving the target's best interest, in today's society this phenomenon gets a bad reputation. However, social engineering itself is actually part of our everyday lives, used in all aspects of our social relations. In cybercrime, social engineering is generally related to gaining confidential information or access to certain tools and resources.

Identity thieves often use social engineering as their tool for exploiting victims. The process of social engineering starts with information gathering (Hadnagy, 2010). Information is crucial for developing social engineering efforts (Stewart & Dawson, 2018), therefore information gathering is the foundation of a successful social engineering endeavor. In the online dating scenario, the perpetrator would seek various information from the victim to understand their character, their values and vulnerabilities.

Another important phase in the process of social engineering is elicitation, or the process of drawing people out and stimulating them to engage in certain behaviors (Hadnagy, 2010). In the online dating scenario, this is where the cybercriminal would confirm the views or mutual interests, heighten the self-worth of their target and create a comfortable setting so the target opens up and establishes trust towards the perpetrator, and therefore engages in continued conversations where more and more information can be shared.

Pretexting is the creation of an invented scenario to entice the victim to share information or perform certain actions (Hadnagy, 2010). Pretexting is the background story and personality of the social engineer, i.e. immersing oneself in the role of a certain character to execute the social engineering endeavor (Hadnagy, 2010). In online dating scenarios, this is when the criminal would engage in presenting themselves as the perfect mate for their victim, bringing all the desired traits and affection, to assure the attack is successful. Of course, information gathering is crucial for this to be successful, since they need to mold their personality to fit the needs of their target. Finally, various psychological principles can be used to assist the social engineering attack and to influence and persuade the victim to perform certain actions (Hadnagy, 2010).

Social media pages such as Facebook, Instagram, Twitter, and others create an environment that enables personalized social engineering (Stewart & Dawson, 2018). Information such as a birth month, home address, location, and even a public network allows an attacker to begin working on exploitation techniques. These can be in the form of someone carefully selecting a target to a third-party having ac-

## **Dark Web**

cess to the account through a developed application in which you have granted rights to your information to use it. Researchers have looked at what factors lead to gullibility in an individual faced with social engineering threats based on personality traits. When you have multiple social media pages, Internet of Things (IoT) devices, public information, and data revealed through breaches, it allows someone to become a target through careful analysis of that information. Unprotected and uncontrolled data enable an attacker to target entities through careful selection (Martinez & Dawson, 2019).

## **THE DARK WEB AND THE MARKET OF ONLINE IDENTITY THEFT**

The Internet is a profitable playground for cybercriminals, whose motivation is financial gain (Ablon, 2018). Stolen information and identities are often shared and distributed online for profit. A commonly used subset of the Internet is the Dark Web, which is the hidden encrypted layer below the regular web that is only accessible by special tools such as Tor or The Onion Router (Faizan & Khan, 2019). These tools apply encryption and hidden IP addresses that enable users and sites to stay anonymous while accessing the Dark Web, making them completely hidden and untraceable (Faizan & Khan, 2019). Sites on the Dark Web are not indexed by traditional search engines like Google, and one cannot access them without these tools. Cybercriminals often use digital currencies, such as Bitcoin, to undertake these illegal transactions for further anonymity (Ablon, 2018). The Dark Web functions as the underground market for the dissemination of illegally acquired identity theft assets. The Dark Web isn't used only for illegal purposes, but illegal activity is a significant portion of its content, ranging from drug sales to identity theft and child pornography. Not only is the Dark Web a flourishing underground platform to purchase stolen products such as personal data, user credentials or credit card information, but cybercrime services can also be hired on these platforms (Ablon, 2018).

## **Navigating the Dark Web**

Former sites such as the Silk Road served as a crypto market for illegal drug trading until it was closed two years later (Maddox *et al.*, 2016). Since Silk Road has been taken down, numerous pages have taken its place. The problem with shutting down the operations on these pages is that the Dark Web consists of unindexed pages that are not found using an everyday browser such as Firefox, Chrome, or Internet Explorer. To access these Dark Web pages, The Onion Router (or Tor) is required to be installed on the system. While installing the browser allows someone to be safe, the other issues remain around the privacy of an Internet Service Provider (ISP) viewing activities. So the installation and the use of additional services such as Virtual Private Network (VPN), encryption, and other security tools to altogether cloak activities is recommended. If the user uses Ubuntu or another Debian based Linux distribution, then installing the necessary Personal Package Archives (PPAs) must be done through the Command Line Interface (CLI). After that, typing the below installs runs Tor.

```
sudo apt update  
sudo apt install torbrowser-launcher
```

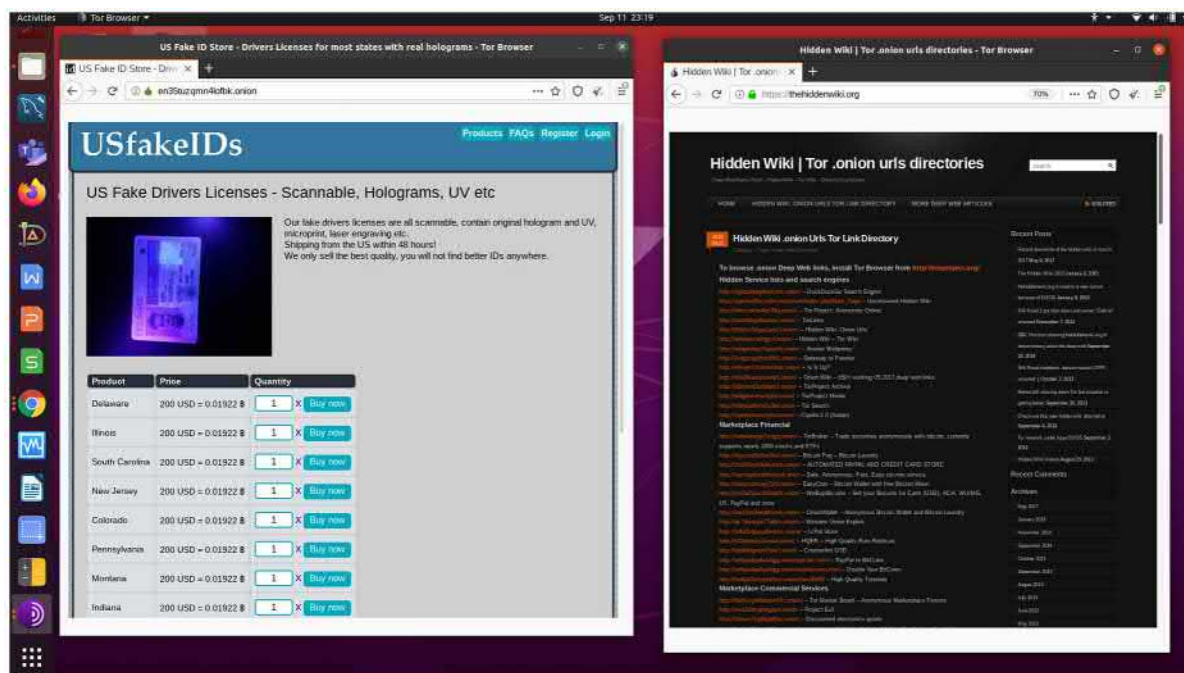
Once Tor Browser is installed, then in the CLI typing torbrowser-launcher will launch Tor. Navigating to show the application, then one could locate the application as well. Operating Systems (OS) such as



Kali Linux and Tails have a number of these applications prebuilt. These OSs can do more than navigating the Dark Web while others are developed with digital crime and cyber warfare (Dawson & Omar, 2015).

Figure 1 displays a screenshot of an onion page accessed with the Tor Browser using Hidden Wiki to locate the page. The Hidden Wiki serves as a guide to pages on the Dark Web to be accessed, describing its service (Sinha, 2017).

Figure 1. Example of online marketplace on the Dark Web



Sites such as USfakeIDs provide their customers the ability to purchase a driver's license from any state. These licenses are advertised as being near authentic to including the hologram. This site could serve underage teens in the purchase of alcohol, illegals who require proper documentation, or individuals who seek something much more sinister as maintaining an identity to plan a terrorist attack. Other items sold are passports, birth certificates, and other government-provided documents that are used to establish an identity on similar sites.

While the Hidden Wiki is not all-inclusive, it does provide a starting point for those getting familiarized with this hidden marketplace. Some sites that provide auctions and other services require Bitcoin payment before giving the actual onion link. This action is to show a real desire to participate rather than just browsing a storefront of illegal services and goods.

Another important aspect of the Dark Web is online forums. Countries have laws in place to protect and provide rights, such as freedom of speech. Therefore, online forums provide a medium where people can freely share how they feel with likeminded people. This is especially important in certain countries, where the freedom of information is not well supported by current regimes. However, alt-right groups, nationalists, and domestic terrorist groups use these forums routinely to spread violence and hatred

## **Dark Web**

filled messages, as well as disinformation (Sambo & Sule, 2021; Memdani, Kademi & Rafay, 2021). Other forums may not give into online disinformation or spread hate but instead, inform individuals on how to obtain information for a service or good that may be deemed illegal, such as the sale of illegally acquired credit card data or other personally identifiable information - making the Dark Web an attractive platform for those engaged in similar activities.

## **Financial Transactions on the Dark Web**

### **Supply and Demand on the Dark Web**

Prices on the Dark Web can vary. Some factors determining the prices of these illegal assets is the type of the data being sold, the balance associated with the accounts, and the limits of possibilities of reuse of the stolen information (Stack, 2018). The economic concept of the fluctuation of supply and demand exists in this underground market: a set of account credentials is going to be cheaper than purchasing intellectual property information illegally; and newly hacked credit card numbers will be bought for higher prices than records from breaches that happened months ago (Ablon, 2018). Credit card account information can be purchased either individually or in bulk (Spalevic & Ilic, 2017). In addition, Stack suggests that there are often bundle offers containing various types of data bundled together to provide a valuable package for identity thieves (Stack, 2018). To be exact, Social Security numbers can be bought for about \$1, credit or debit cards range somewhere between \$5-\$100 (the higher end being the bundle packages with other important information such as SSN and name), online accounts such as PayPal are sold for \$20-\$200, drivers licenses for about \$20, US passports for \$1000-\$2000 (this is usually lower for other countries), diplomas for \$100-\$400, and medical records for \$1-\$1000 (Stack, 2018).

### **Cryptocurrencies and Blockchain**

One attractive payment method on the Dark Web is cryptocurrency. In recent years, cryptocurrency has been the rave, but that has been surrounding the exploding growth in Bitcoin's value. There are only aspirations and hopes of regulating cryptocurrencies (Narayanan *et al.*, 2016; Iqbal, *et al.*, 2019). In the meantime, this form of payment is extremely popular for the exchange of illegal goods and services. One researcher takes an in-depth look into Bitcoin money laundering, exploring the negatives and positive outcomes of using cryptocurrency (Bryans, 2014).

Even though the hype is dying down around cryptocurrency, this is still the currency of choice to evade law enforcement (Wolfson, 2018). Among the largest unregulated markets in the world are cryptocurrencies. Researchers estimate approximately \$76 billion of illegal activities per year, with one-quarter of Bitcoin users involved (Foley *et al.*, 2019). These numbers are astronomical and transforming the known black markets by enabling new e-commerce.

There has been a movement to trace criminal activity across the Bitcoin blockchain. By examining the blockchain activity through a process called clustering, discovering accounts purpose uncovers what type of storefront it is linked to. For example, if an account is used to make purchases on a Dark Web marketplace, we can begin to pinpoint appearances tied to the same Bitcoin wallet. This action may mean the same entity also controls them. Once that entity becomes known, then analysis can be done to begin uncovering who that entity is through methods such as Open Source Intelligence (OSINT) and other forms of intelligence analysis coupled with data-driven tools.

The activities that were once considered in the shadows over the years were brought into the light. For a moment, law enforcement agencies globally were able to, at the least, understand what needed to be done and begin to use resources to combat these issues. With the emergence of the Dark Web and cryptocurrencies, Internet-driven illicit activities have a refuge. To combat this problem, sufficient resources must be made available. Another action is educating people early enough to become aware of safe and secure Internet use to minimize the risk and exposure associated with their Personal Identifiable Information (PII). When individuals know how to properly lock down their pages and understand how to limit their threat landscape, it will be more difficult for predators to prey upon them.

Bad actors have shown the ability to quickly move people and goods largely undetected, which demonstrates multiple holes in a supply chain, policing, and detecting abnormalities in a more extensive system that is built to protect its citizens. But with online websites that provide access to various illegal products and services in an almost untraceable manner with a click of a button, fighting these crimes is an ambitious effort. Through the use of cryptocurrencies, the funds used for illegal activities become difficult to track. Internet-driven illicit activities can undermine what governments have set up to build confidence among its citizens to include circumventing established laws.

## **SOLUTIONS AND RECOMMENDATIONS**

Throughout this chapter, insight into how crimes related to online identity theft and fraud are carried out after a thorough examination of the evolution of cybercrime, history of identity theft, applications for Internet anonymity, and discussion on effects caused by romance scams and data breaches. Discovered are that several states require the disclosure of data breaches by companies to customers. Even though the real efficacy of similar legal requirements is debated, it is apparent that the sooner victims are informed of the misuse of their information, the more effectively they can prevent further harm (Romanosky *et al.*, 2011). The lack of corporate responsibility is an important roadblock: when the costs of mitigating a data breach cost less than 1% of an organization's total revenue, such as in the case of the Target data breach, there is a minimal incentive for them to make a long-lasting change (Manworren *et al.*, 2016).

The lack of federal regulations requires organizations to follow state and local policies and regulations, resulting in complicated, inefficient, and non-standard requirements for companies to follow (Manworren *et al.*, 2016). Organizations should only collect data they truly need for their operations and only store it while it is essential (Manworren *et al.*, 2016). Therefore, organizations should implement technologies that protect this data from ongoing monitoring. Federal laws that require compliance with Cybersecurity frameworks could mitigate risks to an acceptable level. Thus, the requirement to be compliant with the National Institute of Standards and Technology (NIST) Cybersecurity Framework at a minimum would provide standard Cybersecurity controls that is a baseline for deploying systems that have security. Ultimately, Internet identity theft and fraud can only be deterred by educating people, holding organizations accountable that fail to protect their data, and deploying Cybersecurity controls.

## **CONCLUSION**

This chapter investigated previous and current trends of online identity theft and fraud. With the prevalence of technology, online criminal activity blooms to exploit individuals and organizations alike. These

## **Dark Web**

crimes can be committed in an organized fashion by exploiting technology vulnerabilities, or by social engineering practices that target individuals. From corporate data breaches to romance scams, virtually anybody can become a target. The hidden crevices of our networked data, such as the Dark Web, provide a breeding ground for the transmission of products and services of these illegal activities. These types of crimes can only be fought with a complex, regulated effort, including more standardized federal regulations that organizations must abide by, incentives for organizations to act in a responsible manner to be good stewards of consumer data, and by educating consumers to safe Internet and data practices to protect themselves against these vicious crimes.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## **REFERENCES**

- Ablon, L. (2018, March 15). *A Close Look at Data Thieves*. Retrieved from <https://www.rand.org/pubs/testimonies/CT490.html>
- Alagna, V. (2020). *A Comparative Analysis of Identity Theft within America and Australia*. Retrieved from Criminal Justice: [https://scholarsarchive.library.albany.edu/honorscollege\\_cj/24/](https://scholarsarchive.library.albany.edu/honorscollege_cj/24/)
- API Tech Servs., LLC v. Francis, 4: 13-cv-142-AWA-DEM (E.D. V.A., 2013).
- A.V. v. iParadigms, LLC, No. 08-1424, No. 08-1480 (4th Cir., 2009).
- Black's Law Dictionary. (2019). Cybercrime (11th Ed.). Toronto: West (Thompson Reuters).
- Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal (Indianapolis, Ind.)*, 441–472.

- Business Crimes. (2013). *Computer Fraud and Abuse Act 18 USC Sec. 1030*. Matthew Bender & Co.
- Capital One. (2019, September 23). *Information on the Capital One Cyber Incident*. Capital One. Retrieved from <https://www.capitalone.com/facts2019>
- Computer Fraud and Abuse Act of 1986, Pub. L. 99-474 (1986). Retrieved from <https://www.congress.gov/bill/99th-congress/house-bill/4718>
- Dawson, M., Eltayeb, M., & Omar, M. (Eds.). (2016). *Security Solutions for Hyperconnectivity and the Internet of Things*. IGI Global. doi:10.4018/978-1-5225-0741-3
- Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. IGI Global. doi:10.4018/978-1-4666-8345-7
- Dickey, M. R. (2016, November 13). FriendFinder Networks Hack Reportedly Exposed Over 412 Million Accounts. *TechCrunch*. Retrieved from <https://techcrunch.com/2016/11/13/friendfinder-hack-412-million-accounts-breached/>
- Durkin, K., & Brinkman, R. (2009). 419 FRAUD: A Crime Without Borders in A Postmodern World. *International Review of Modern Sociology*, 35(2), 271–283.
- Dyrud, M. A. (2005). I Brought You Good News: An Analysis of Nigerian 419 Letters. *Proceedings of the 2005 Association for Business Communication Annual Convention*.
- Electronic Communications Privacy Act of 1986, Pub. L. 99-508 (1986). Retrieved from <https://www.congress.gov/bill/99th-congress/house-bill/4952>
- Faizan, M., & Khan, R. A. (2019). Exploring and analyzing the dark Web: A new alchemy. *First Monday*, 24(5). Advance online publication. doi:10.5210/fm.v24i5.9473
- FBI. (2020). *What We Investigate, Cyber Crime*. Federal Bureau of Investigation. Retrieved from <https://www.fbi.gov/investigate/cyber>
- Federal Trade Commission. (2019a). *What You Need to Know About Romance Scams*. Federal Trade Commission. Retrieved from <https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams>
- Federal Trade Commission. (2019b, February 12). *Romance Scams Rank Number One On Total Reported Losses*. Federal Trade Commission. Retrieved from <https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses>
- Federal Trade Commission. (2019c, February 12). *Romance Scams Will Cost You*. Federal Trade Commission. Retrieved from <https://www.consumer.ftc.gov/blog/2019/02/romance-scams-will-cost-you>
- Federal Trade Commission. (2020a). *Policy*. Federal Trade Commission. Retrieved from <https://www.ftc.gov/policy>
- Federal Trade Commission. (2020b, January). *Equifax Data Breach Settlement*. Federal Trade Commission. Retrieved from <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>

## Dark Web

Federal Trade Commission. (n.d.). *Report Identity Theft and Get a Recovery Plan*. Federal Trade Commission. Retrieved from <https://www.identitytheft.gov/>

Federal Trade Commission Act. 15 U.S.C. §§ 41-58, et. seq. (1914).

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies? *Review of Financial Studies*, 32(5), 1798–1853. doi:10.1093/rfs/hhz015

Fraud.org. (2020). *Scams of the Heart: Sweetheart Swindles*. Fraud.org. Retrieved from <https://fraud.org/sweetheart-swindles/>

Fruhlinger, J. (2020, February 12). Marriott Data Breach FAQ: How Did It Happen and What Was the Impact? *CSO*. Retrieved from <https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html>

Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.

Iqbal, S., Hussain, M., Munir, M. U., Hussain, Z., Mehrban, S., Ashraf, A., & Ayubi, S. (2019). Cryptocurrency: Future of FinTech. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 1–13). IGI Global. doi:10.4018/978-1-5225-7805-5.ch001

Kesari, A. (2020a). The Effect of State Data Breach Notification Laws on Medical Identity Theft. University of California, Berkeley - D-Lab (Data-Intensive Social Science Lab); Yale Law School. doi:10.2139/ssrn.3700248

Kesari, A. (2020b). Predicting Cybersecurity Incidents Through Mandatory Disclosure Regulation. University of California, Berkeley - D-Lab (Data-Intensive Social Science Lab); Yale Law School. doi:10.2139/ssrn.3700243

Lu, J. (2019, August). *Assessing the Cost, Legal Fallout of Capital One Data Breach*. Retrieved from [https://www.researchgate.net/publication/335210159\\_Assessing\\_The\\_Cost\\_Legal\\_FalloutOf\\_Capital\\_One\\_Data\\_Breach](https://www.researchgate.net/publication/335210159_Assessing_The_Cost_Legal_FalloutOf_Capital_One_Data_Breach)

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital ‘Demimonde’. *Information Communication and Society*, 19(1), 111–126. doi:10.1080/1369118X.2015.1093531

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, 59(3), 257–266. doi:10.1016/j.bushor.2016.01.002

Martínez, F. G. (2019a). *Special Problems in Information Security: From Privacy to Emerging Technologies for Hyperconnected Systems* (Master’s thesis). Madrid: Universidad Politécnica de Madrid.

Martínez, F. G. (2019b). Analysis of the US Privacy Model: Implications of the GDPR in the US. *International Journal of Hyperconnectivity and the Internet of Things*, 3(1), 43–52. doi:10.4018/IJHIoT.2019010103

Martinez, F. G., & Dawson, M. (2019). Unprotected Data: Review of Internet Enabled Psychological and Information Warfare. *Land Forces Academy Review*, 24(3), 187–198. doi:10.2478/raft-2019-0022

- McDaniel, D. (2019). *Data Breaches: Who is Behind Them, Why They Do It, and How to Protect Your Data*. Infosecwriters. Retrieved from [http://www.infosecwriters.com/Papers/dmcdaniel\\_databreaches.pdf](http://www.infosecwriters.com/Papers/dmcdaniel_databreaches.pdf)
- McDonough, M. (2010, February 25). Bad Check Schemes Targeting Lawyers are Increasingly Sophisticated. *ABA Journal*. Retrieved from [https://www.abajournal.com/news/article/bad\\_check\\_schemes\\_targeting\\_lawyers\\_are\\_increasingly\\_sophisticated/](https://www.abajournal.com/news/article/bad_check_schemes_targeting_lawyers_are_increasingly_sophisticated/)
- Memdani, L., Kademi, T. T., & Rafay, A. (2021). Effect of Terrorism Financing on selected Global Indices: The Case of 2015 Paris Attacks. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
- National Consumers League. (2011, February 7). *Scams, Shams, and Predators: Online Dating in a Digital Age*. National Consumers League. Retrieved from [https://www.nclnet.org/scams\\_shams\\_and\\_predators\\_online\\_dating\\_in\\_a\\_digital\\_age](https://www.nclnet.org/scams_shams_and_predators_online_dating_in_a_digital_age)
- National Crime Agency. (n.d.). *Sextortion (Webcam Blackmail)*. National Crime Agency. Retrieved from <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail>
- North Carolina Computer Trespass Act N.C.G.S. §14-458. (2016).
- Norton. (2020, March 10). *What is a Data Breach?* Norton. Retrieved from <https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html>
- Peterson, A. (2016, November 14). Adult FriendFinder Hit With One of the Biggest Data Breaches Ever, Report Says. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says/>
- Rafay, A. (Ed.). (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, 3(2), 494–412.
- Romanosky, S., Telang, R., & Acquisti, A. (2011). Do Data Breach Disclosure Laws Reduce Identity Theft? *Journal of Policy Analysis and Management*, 30(2), 256–286. doi:10.1002/pam.20567
- Sambo, U., & Sule, B. (2021). Financing as a Livewire for Terrorism: The Case of North-Eastern Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Sanger, D. E., Perlroth, N., Thrush, G., & Rappeport, A. (2018, December 11). Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>
- Sinha, S. (2017). Dark Web and Tor. In *Beginning Ethical Hacking with Python* (pp. 173–177). Apress. doi:10.1007/978-1-4842-2541-7\_26

## Dark Web

Spalevic, Z., & Ilic, M. (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika, Journal for Economic Theory and Practice and Social Issues*, 63, 73-82.

Stack, B. (2018, March 11). *Here's How Much Your Personal Information Is Selling for on the Dark Web*. Retrieved from <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

Stewart, J., & Dawson, M. (2018). How the modification of personality traits leave one vulnerable to manipulation in social engineering. *International Journal of Information Privacy, Security and Integrity*, 3(3), 187–208.

Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. *CSO Online*. Retrieved from <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

Tajpour, A., & Zamani, M. (2020). Identity Theft and Prevention. In *Information Security and Optimization* (pp. 25–42). Chapman and Hall/CRC. doi:10.1201/9781003045854-3

Tennessee Bar Association. (2009). *Internet Scams Target Attorneys*. Retrieved from <http://www.tba2.org/tbatoday/2009/TBAtoday06-09-2009.htm>

Tinder. (n.d.). *What is Photo Verification?* Retrieved from <https://www.help.tinder.com/hc/en-us/articles/360034941812-What-is-Photo-Verification->

*United States of America (For the Federal Trade Commission), v. Kohl's Department Stores, Inc., No. 2:20-cv-859*. (2020). E.D. Wisc.

*United States v. Cioni*, 649 F.3d 276, 282 (4th Cir. 2011)

Verizon. (2020). *2020 Data Breach Investigations Report*. Retrieved from <https://enterprise.verizon.com/resources/reports/dbir/>

*WEC Carolina Energy Solutions LLC v. Miller*, 687 F. 3d 199 (4th Cir. 2012)

Weiss, D. C. (2009). Bradley Arant Reportedly Scammed Out of More Than \$400K. *ABA Journal*. Retrieved from [https://www.abajournal.com/news/article/bradley\\_arant\\_reportedly\\_scammed\\_out\\_of\\_more\\_than\\_400k](https://www.abajournal.com/news/article/bradley_arant_reportedly_scammed_out_of_more_than_400k)

Wolfson, R. (2018, December 15). Tracing Illegal Activity through the Bitcoin Blockchain To Combat Cryptocurrency-Related Crimes. *Forbes*. Retrieved from <https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/>

## ADDITIONAL READINGS

Berghel, H. (2000). Identity theft, social security numbers, and the web. *Communications of the ACM*, 43(2), 17–21. doi:10.1145/328236.328114



- Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of information. Law and Technology*, 1(1), 1–20.
- Grazioli, S., & Jarvenpaa, S. L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. *IEEE Transactions on Systems, Man, and Cybernetics. Part A, Systems and Humans*, 30(4), 395–410. doi:10.1109/3468.852434
- Isacenkova, J., Thonnard, O., Costin, A., Francillon, A., & Balzarotti, D. (2014). Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security*, 2014(1), 4. doi:10.1186/1687-417X-2014-4
- Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, 52(2), 353–363. doi:10.1016/j.dss.2011.09.002
- Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., & Elovici, Y. (2009, June). Identity theft, computers and behavioral biometrics. In *2009 IEEE International Conference on Intelligence and Security Informatics* (pp. 155–160). IEEE. 10.1109/ISI.2009.5137288
- Romain, M., & Bjerke, P. (2006). *U.S. Patent Application No. 11/139,021*.
- Rusch, J. J. (1999, June). The “social engineering” of internet fraud. In *Internet Society Annual Conference*. [http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g\\_2.htm](http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm)
- Solove, D. J. (2002). Identity theft, privacy, and the architecture of vulnerability. *Hastings Lj*, 54, 1227.
- Teraguchi, N. C. R. L. Y., & Mitchell, J. C. (2004). Client-side defense against web-based identity theft. *Computer Science Department, Stanford University*. <https://crypto.stanford.edu/SpoofGuard/webspoof.pdf>

## KEY TERMS AND DEFINITIONS

**Cryptocurrency:** A digital currency secured by cryptography and managed by blockchain technology that is run on distributed computer networks.

**Dark Web:** The hidden layer of the Internet comprising of sites that are only accessible with specific technologies and encryption processes to protect the identity of the individual browsing or posting content.

**Data Breach:** The unauthorized access and dissemination of data sourced from corporate databases. Data breaches can happen either via exploiting a technical vulnerability, or by human factors, such as social engineering or insider threat.

**Identity Fraud:** The fraudulent use of illegally acquired personal information of an individual. It is generally interchangeably used with identity theft.

**Identity Theft:** The unauthorized access or stealing of an individual’s personal information, such as Social Security Number, name, or credit card information by an outside party. It is generally used interchangeably with identify fraud.

**Romance Scam:** The activity of establishing an online romantic relationship with an individual based on false pretenses, using a fake identity, with the goals of later exploiting them for financial gain.

**Social Engineering:** The art of influencing and manipulating an individual into acting a certain way that they may or may not intend to do otherwise, and that may or may not be in their best interest.

## Chapter 26

# Tech-Based Enterprise Control and Audit for Financial Crimes: The Case of State-Owned Global Financial Predators (SOGFP)

**Antoine Trad**

 <https://orcid.org/0000-0002-4199-6970>

*Institute of Business and Information Systems Transformation Management, France*

**Marie Goretti Nakitende**

*Uganda Martyrs University, Uganda*

**Tayo Oke**

*Afe Babalola University, Nigeria*

### ABSTRACT

*Due to the global financial and societal crisis, a societal or business transformation project is important. A well-designed financial services automation process is the need of the hour. This automation process depends on measurable critical success factors (CSF) which characterize the progress and evaluation of societal or organizational transformation processes. This chapter discussed in detail the concept of an applied tech-based enterprise control and audit for financial crimes (ECAFC) framework, which is significant for the detection of financial crimes. In the context of financial crimes analysis (FCA), a strategic vision is required for the integration of financial engineering related to risk and controls. This analysis is fundamental for the enterprise's long-term business longevity and to avoid/combat state organized global financial predators (SOGFP). Moreover, the chapter also highlighted that the detection mechanisms are essential for the enterprise, in order to integrate the local and global economies in a sustainable, controlled, and iterative manner.*

DOI: 10.4018/978-1-7998-5567-5.ch026

## INTRODUCTION

Actually, and probably because of the ongoing global financial crisis and uncertainty, these finance related risk and related legal standards are not mature enough and are even chaotic. These presented facts can damage the transformation initiative or an enterprise architecture project (or simply a *Project*). The proposed strategic approach and vision, which is, in this case, applied to financial risk management, aimed to support the detection of financial irregularities, locked-in traps and crimes, which can be fatal for an organization or country (or simply an *Entity*). Gigantic financial crimes like the ones, which are related to fraud and money laundering, damage many business organizations, business entities and countries. In this chapter it is related to cases like, the Swiss, Union des Banques Suisse (UBS) (Stupples, Sazonov & Woolley, 2019), in which 32 trillion US dollars were simply hidden and another gigantic fraud organized by the Swiss Fidusuisse, which shows the state of mind of such a state and its predator accountants, who promote a State Organized Global Financial Predators (SOGFP) approach (Cornevin, 2020). This chapter is about global organized fraud which is a financial crime and the author considers that nobody, *Entity* or institution are above the law. Some of the major states who are related to SOGFP, enjoy excellent world class reputations, so questions arise: What are the real roles of ranking, control/ethics and audit organizations? And are they corrupt? Are politicians, in so-called ethical and advanced countries corrupt?

## BACKGROUND

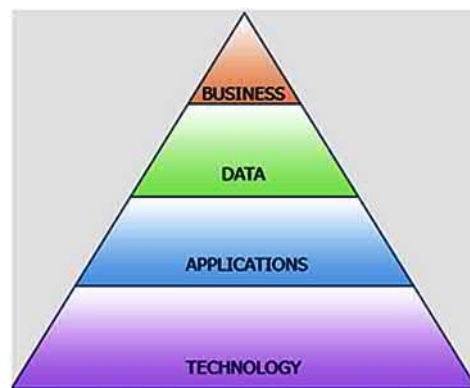
This chapter<sup>1</sup> primarily focuses on:

1. The Financial Crime Analysis Concept (FCAC's) Vision (FCAV) that can be used to support Enterprise Control and Audit for Financial Crimes (ECAFC) in its essence;
2. Use of ECAFC with existing standards;
3. The support of various types of financial strategies
4. The selection of a ECAFC expert's profile.
5. The use of the Applied Holistic Mathematical Model for FCA (AHMM4FCA) as a stub for the ECAFC;
6. the concept of Neural Networks.
7. Holisms, generics and global ECAFC;
8. The application of risk management to support complex financial systems;
9. the ECAFC as the kernel of the financial system.
10. Artificial Intelligence (AI) as a generic interface for all possible problems;
11. The use of the intelligent Knowledge Management System for FCA (KMS4FCA) as a holistic strategic knowledge environment to support he ECAFC; and
12. Continuous design, development, deployment, transformation and innovation, using an agile iterative development and operations approaches.

Searching with the scholar engine, within Google's online search portal, in which the author combined the previously mentioned keywords and key topics; the results show very clearly the uniqueness and the absolute lead of the author's works/framework, methodology, research and recommendations

in the mentioned scientific fields and that can be considered as an important jumpstart for the future industrial use (Trad, 2019c). The AHMM4FCA based ECAFC for *Projects*, can be used for scripting and prototyping Finance for Technologies (FinTech) environments using a set of atomic Building Blocks (aBB) in the form of microartefacts. The use of the ECAFC is achieved by the instantiation (in  $n$  instances) using the author's proposed framework that uses an integrated Financial Control and Technology Concept (FCTC), to create a reusable blueprint, that is composed of the main four building levels, in which the ECAFC is on the highest (the business level), as shown in Figure 1. Where in this chapter the level interfaces the others: 1) Technology; 2) Applications; and 3) Data; using the FCTC. The fourth level, the business one that includes finance's strategy is presented in this chapter which relates to other chapters like FCTC (Trad, 2020). These various levels are glued using a Natural Programming Language for FCA (NLP4FCA).

*Figure 1. The Project blueprint*  
(The Open Group, 2011).



The ECAFC is based on a concrete Applied Case Study for FCA (ACS4FCA); where the central point is FinTech related to financial (trans)actions and the related transformation process of the existing no-strategy system into a modern based ECAFC one. Such a *Project* is managed by the Business Transformation Managers (BTM), FCA experts, Financial Officers/Auditors or an Enterprise Architecture Manager (EAM) (from now on, simply a *Manager*); who, in this case, are supported with a methodology and a framework that can estimate the risks of the implementation of such *Projects*'. The *Manager* is responsible for the implementation of complex *Projects* using various types/levels of patterns, like the ECAFC. The ECAFC supports him or her (for simplicity, in further text – him) in a just-in-time manner in the area where he should have a solid background in existing FCAC strategies.

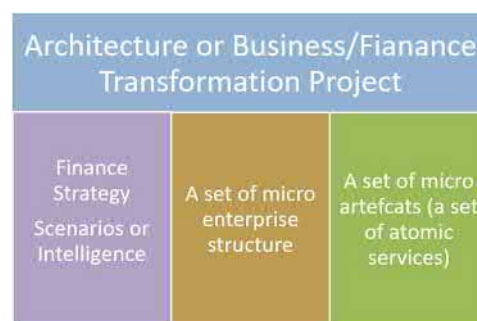
## MAIN FOCUS OF THE CHAPTER

To implement such a financial engineering risk and control mechanisms, the author's, Transformation, Research and Architecture Development framework (*TRADf*) proposed default factors, can be used to evaluate risk and control of the *Project's* financial estimates, budgets and misdeeds (IFRS, 2017). The

*Project* Critical Success Factors (CSF) can be configured to measure the influence of the complexities in managing asynchronous financial flows and controls of its local and international financial environments. A *Project* needs to integrate complex technologies to facilitate the strategic financial planning process of a business and to prepare it to integrate the globally interconnected financial endpoints in a holistic manner. The integration of Finance for Technologies (FinTech) and Information and Communication Technologies (ICS) is crucial for such financial critical systems (Rafay, 2019). Today FinTech standards and fields are robust, resilient and can be applied as automated synchronized (block) chains; to enable the traditional financial environments to become a part of a networked and controlled financial *Entity* (Hussain *et al.*, 2019). A FinTech platform can be applied to support a financial risk engineering concept and vision, in order to avoid locked-in situations (Trad, 2020; Trad & Kalpić, 2018a). To apply the ECAFC concept, Critical Success Areas (CSA) (and their corresponding CSFs) and the Key Performance Indicators (KPI) must be selected and weighted to evaluate possible pitfalls and problems' risk. A resilient ECAFC, includes a process, which incorporates a set of automated standardized NLP4FCA procedures that can be applied to evaluate the real value of the targeted ECAFC's implementation (IFRS, 2017). The applied valuation process is complex that depends on the applied *Project* (KYTE, 2010). ECAFC supports a standardized and fully integrated *Project*, technology stacks, governance and monitoring subsystems (Kowall & Fletcher, 2013). ECAFC promotes FinTech driven strategic financial environments that use technology stacks/fields like the Service Oriented Architecture (SOA) for block-chain automation process (Kabzeva, Niemann, Müller & Steinmetz, 2010). ECAFC is a part of the Financial management module (Fm); Fm is also a part of the Selection management, Architecture-modelling, Control-monitoring, Decision-making, Training management, Project management, and Finance management Framework (SmAmCmDmTmPmFmF, for simplification in further text the term the *TRADf*, will be used), that is the major support for of *Project*'s activities; in fact the proposed *TRADf* is a pioneering initiative and for the moment a leader in this domain (Trad & Kalpić, 2020).

This a complex framework, *TRADf*, relates to other works related to the author and this work is just another brick in wall; so, it is important to understand the structure of the proposed structured, like in other known complex holistic frameworks, like for example The Open Group's Architecture Framework (TOGAF)... *TRADf* is not a simplistic quantitative excel analysis, which for such cases and topics is limited. Finance related topics are mainly treated by finance/accounting and business experts, who graduated business schools, whereas the author's Framework treats various domains in simultaneously and in parallel.

*Figure 2. The relation between ECAFC and aBBs.*



## THE STRATEGY AND VISION

A *Project* must establish ECAFC's vision for a built-in automated block-chain controls as a global support, capable of recognizing financial collective crimes and financial black swan effects (Trad & Kalpić, 2019), bad investments, *Project* budget slips, loss of transactions, illegal activities and fraud/tax evasions (Trad & Kalpić, 2016). The ECAFC is based on the author's authentic and proprietary Research and Development Project's for FCA (RDP4FCA) method that is supported by an underlining mainly qualitative holistic reasoning module. The ECAFC is an AI based empirical concept that uses an NLP4FCA; which can be adapted by the project teams (Myers, Pane, & Ko, 2004). The ECAFC is implemented in an experiment or in other words, a Proof of Concept (PoC), in order to check the feasibility of its integration capacities and the resultant risks.

## OUTCOME OF RELATED RESEARCH WORKS

The ECAFC related research is made up of the following inter-related approaches (in the form of works) that are:

- The research concept describing the RDP4FCA for the FCTC and ECAFC, as shown in Figure 2.
- The FCTC's CSFs are presented in Tables 1 to 12, which encapsulates all the results from the related sections' results which include the basic parts, which are valid for this chapter.
- The RDP4FCA's CSFs are presented in Table 13, which encapsulates all the results from the related FCTC which include the strategy parts that are valid for this chapter. These facts enable the RDP4FCA to inspect the FCTC's basics.

Table 1.

Critical Success Factors	KPIs	Weightings
CSF_RDP_Modelling	HighlyFeasible	From 1 to 10. 09 Selected
CSF_RDP_Factors	PossibleClassification	From 1 to 10. 10 Selected
CSF_RDP_References	AutomatedExists	From 1 to 10. 09 Selected
CSF_RDP_ADM	IntegrationPossible	From 1 to 10. 09 Selected
CSF_RDP_Technologies4iSASDev	AdvancedStage	From 1 to 10. 09 Selected
CSF_RDP_Governance	Advanced	From 1 to 10. 09 Selected
CSF_RDP_Transformation_iASbDMS	IntegrationPossible	From 1 to 10. 10 Selected
CSF_RDP_Leading_TRADf	Possible	From 1 to 10. 10 Selected

valuation

Table 2.

Critical Success Factors	KPIs	Weightings
CSF_AHMM4iASbDMS_TRADE_Integration	Feasible	From 1 to 10. 09 Selected
CSF_AHMM4iASbDMS_InitialPhase	Stable	From 1 to 10. 10 Selected
CSF_AHMM4iASbDMS_PoC	Feasible	From 1 to 10. 09 Selected
CSF_AHMM4iASbDMS_Qualitative&Quantitative	Possible	From 1 to 10. 09 Selected
CSF_AHMM4iASbDMS_Final_Instance	VerifiedModel	From 1 to 10. 10 Selected
CSF_AHMM4iASbDMS_ADM_Integration	Synchronized	From 1 to 10. 10 Selected
CSF_AHMM4iASbDMS_iASDev_Interfacing	Stable	From 1 to 10. 10 Selected

valuation

Table 3.

Critical Success Factors	KPIs	Weightings
CSF_iASbDMS_ACS_Modelling	Complex	From 1 to 10. 09 Selected
CSF_iASbDMS_ACS_Factors	PossibleClassification	From 1 to 10. 10 Selected
CSF_iASbDMS_ACS_References	Exists	From 1 to 10. 09 Selected
CSF_iASbDMS_ACS_ADM	IntegrationPossible	From 1 to 10. 10 Selected
CSF_iASbDMS_ACS_Technologies4iASDev	AdvancedStage	From 1 to 10. 09 Selected
CSF_iASbDMS_ACS_Governance	Advanced	From 1 to 10. 09 Selected
CSF_iASbDMS_ACS_Transformation_TRADE	IntegrationPossible	From 1 to 10. 10 Selected
CSF_iASbDMS_ACS_Leading	Possible	From 1 to 10. 10 Selected

valuation

Table 4.

Critical Success Factors	HMM enhances: KPIs	Weightings
CSF_ICS_GUID_IntegrationProcessesModels	Standard	From 1 to 10. 09 Selected
CSF_ICS_TRADE_StandardIntegration	AdvancedState	From 1 to 10. 10 Selected
CSF_ICS_aBB_Microeffects	Supported	From 1 to 10. 10 Selected
CSF_ICS_Performance	Exists	From 1 to 10. 08 Selected
CSF_ICS_DistributedCommunication	Stable	From 1 to 10. 10 Selected
CSF_ICS_Finance	ExistingSupport	From 1 to 10. 09 Selected
CSF_ICS_Security	Complex	From 1 to 10. 08 Selected
CSF_ICS_Automation	Supported	From 1 to 10. 09 Selected
CSF_ICS_Pattern_StandardIntegration	Supported	From 1 to 10. 09 Selected
CSF_ICS_Procedures	Supported	From 1 to 10. 10 Selected

valuation

Table 5.

Critical Success Factors	HMM enhances: KPIs	Weightings
CSF_ADM_CSF_Initialization&Setup	Feasible	From 1 to 10. 10 Selected
CSF_ADM_aBB_IntegrationProcesses	Supported	From 1 to 10. 10 Selected
CSF_ADM_PhasesSynchronization	Supported	From 1 to 10. 10 Selected
CSF_ADM_Requirements	MappingAutomated	From 1 to 10. 10 Selected
CSF_ADM_Concept4iASbDMS_Interface	Supported	From 1 to 10. 10 Selected

valuation

## Tech-Based Enterprise Control and Audit for Financial Crimes

Table 6.

Critical Success Factors	HMM enhances: KPIs	Weightings
CSF_AutomatedFinance_CSF_Initialization&Setup	Feasible	From 1 to 10. 10 Selected
CSF_AutomatedFinance_aBB_Transactions	Supported	From 1 to 10. 10 Selected
CSF_AutomatedFinance_Synchronization	Supported	From 1 to 10. 09 Selected
CSF_AutomatedFinance_Requirements	MappingAutomated	From 1 to 10. 10 Selected
CSF_AutomatedFinance_iASbDMS_Interface	Supported	From 1 to 10. 08 Selected

valuation

Table 7.

Critical Success Factors	HMM enhances: KPIs	Weightings
CSF_HR_RDP	Supported	From 1 to 10. 09 Selected
CSF_HR_CSA_CSF	Implementable	From 1 to 10. 10 Selected
CSF_HR_Surveying	Implementable	From 1 to 10. 10 Selected
CSF_HR_SkillsProfile	Defined	From 1 to 10. 09 Selected
CSF_HR_TRADf	StandardIntegration	From 1 to 10. 10 Selected
CSF_HR_TechocraProfile	Defined	From 1 to 10. 09 Selected
CSF_HR_HolisticApproach	Possible	From 1 to 10. 08 Selected
CSF_HR_EducationalRequirements	Defined	From 1 to 10. 09 Selected
CSF_HR_Recommendations	Implementable	From 1 to 10. 10 Selected

valuation

Table 8.

Critical Success Factors	AHMM enhances: KPIs	Weightings
CSF_iASbKMS_AgileManagement	Supported	From 1 to 10. 09 Selected
CSF_iASbKMS_aBB_microartefacts_Mapping	Implementable	From 1 to 10. 09 Selected
CSF_iASbKMS_Pattern_Design	Implementable	From 1 to 10. 09 Selected
CSF_iASbKMS_Functional_Environments_Integration	EasyImplementable	From 1 to 10. 10 Selected
CSF_iASbKMS_MainGoals	Acheivable	From 1 to 10. 10 Selected

valuation

Table 9.

Critical Success Factors	AHMM enhances: KPIs	Weightings
CSF_iASbDMS_ComplexSystemIntegration	Possible	From 1 to 10. 09 Selected
CSF_iASbDMS_aBB_Microartefacts_Interfacing	Supported	From 1 to 10. 10 Selected
CSF_iASbDMS_iASbKMS_Interfacing	Possible	From 1 to 10. 09 Selected
CSF_iASbDMS_DecisionProcessing	IntegratesAsKernel	From 1 to 10. 10 Selected
CSF_iASbKMS_HolisticApproach	Complex	From 1 to 10. 08 Selected

valuation



Table 10.

Critical Success Factors	AHMM enhances: KPIs	Weightings
CSF_IASbKMS/IASbDMS_SystemsIntegration	Possible	From 1 to 10. 10 Selected
CSF_IASbKMS/IASbDMS_EA_Structure	Feasible	From 1 to 10. 09 Selected
CSF_IASbKMS/IASbDMS_(un)_Tangible_Values	ManagementEnabled	From 1 to 10. 10 Selected
CSF_IASbKMS/IASbDMS_DMP_Capacities	Feasible	From 1 to 10. 09 Selected
CSF_IASbKMS/IASbDMS_HolisticApproach	Supported	From 1 to 10. 09 Selected
CSF_IASbKMS/IASbDMS_TRADf_Support	ComplexButFeasible	From 1 to 10. 09 Selected
CSF_IASbKMS/IASbDMS_RoleOfPatterns	Possible	From 1 to 10. 09 Selected
CSF_IASbKMS/IASbDMS_Skills	Existing	From 1 to 10. 10 Selected
CSF_IASbKMS/IASbDMS_ExistingStatus	Transformable	From 1 to 10. 08 Selected
CSF_IASbKMS/IASbDMS_Automation	Supported	From 1 to 10. 09 Selected
CSF_IASbKMS/IASbDMS_Tracking_Auditing	Feasible	From 1 to 10. 09 Selected

valuation

Table 11.

Critical Success Factors	KPIs	Weightings
CSF_FinTechBasics_HolisticAgileView	ManagementView	From 1 to 10. 10 Selected
CSF_FinTechBasics_RoleOfStandards	Mandatory	From 1 to 10. 09 Selected
CSF_FinTechBasics_ServicesArchitecture	SOA	From 1 to 10. 09 Selected
CSF_FinTechBasics_ADM	TOGAF	From 1 to 10. 09 Selected
CSF_FinTechBasics_LoggingSystem	SYSLOG	From 1 to 10. 09 Selected
CSF_FinTechBasics_DecisionSupport	QUALITATIVE_AR	From 1 to 10. 09 Selected
CSF_FinTechBasics_MicroarchitectureDesign	DDD	From 1 to 10. 09 Selected

Table 12.

Critical Success Factors	KPIs	Weightings
CSF_FinTechAutomation_RadicalBusinessTransformation	Possible	From 1 to 10. 09 Selected
CSF_FinTechAutomation_BitcoinBlock-chain	Mature	From 1 to 10. 08 Selected
CSF_FinTechAutomation_Block-chainTransaction	Errors	From 1 to 10. 08 Selected
CSF_FinTechAutomation_Bitcoin_Block-chainStatus	Automated	From 1 to 10. 09 Selected

## ECAFC BASICS

### The Applied Mathematical Model

The ECAFC uses the author's AHMM4FCA and its underlying CSF management structure; to support *Projects* in domains related to the development of a strategic vision; where in this chapter it is supported by an adapted and extended insurance case (Jonkers, Band & Quartel, 2012). In this case the ECAFC's experiment, tries to show the unbundling process of business financial services; which forms the dynamic platform for a financial strategic vision for a proactive recognition of collective financial crimes (Farhoomand, 2004). The implementation of a related ECAFC, which is supported by the FCAV (Trad, & Kalpić, 2020), can be used to model organisational, business, architecture and technology problem solving, or knowledge management activities related to complex financial issues and their background.

Table 13.

CSA Category of CSFs/KPIs	Influences transformation management	Average Result
The Research Development Project	CredibleStable	From 1 to 10 9.48
The Applied Case Study Integration	CredibleStable	From 1 to 10 9.69
The Usage of the Architecture Development Method	FullyIntegrated	From 1 to 10 10.00
The Information and Communication Technology System	Transformable	From 1 to 10 9.19
The Mathematical Model's Integration	Applicable	From 1 to 10 8.76
The Financial Engineering Concepts	CredibleStable	From 1 to 10 10.00
The Human Resources Effect	CredibleStable	From 1 to 10 9.20
The iASbKMS Integration	CredibleStable	From 1 to 10 9.48
The iASbDMS Integration	Implementable	From 1 to 10 9.20
The iASbBO Integration	Implementable	From 1 to 10 8.75

ECAFC's vision supports the *Entity's* financial engineering risk management, legal controls and integration in a complex automatized globalized environment (Grewal-Carr & Marshall, 2016).

## A Decision Making Approach

The *Manager's* decisions can be made in a just-in-time manner by using outputs from the business environment's existing tracing, monitoring and logging systems; and an internal Decision Making System for FCA (DMS4FCA) to confirm a strategy and vision for assessing the risk and legally assert, govern or control the *Project's* various resources and components; as shown in Figure 3.

Figure 3. The finance strategy and vision for a Project.

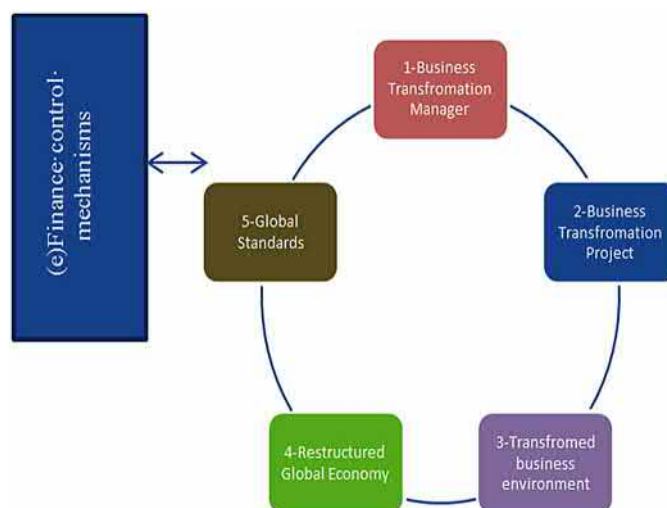
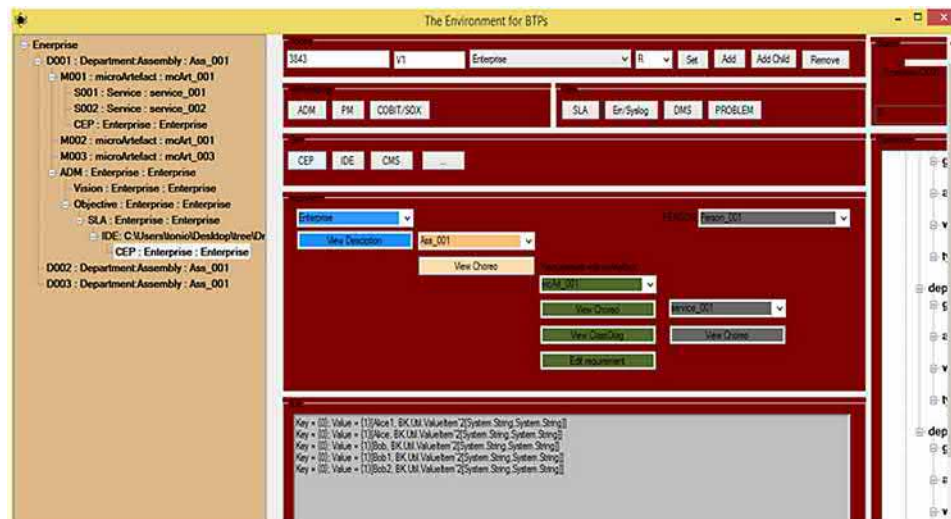


Figure 4. The TRADf environment and client.



The ECAFC is optimal for the architecture and design of control mechanisms' integration in the *Project* (Daellenbach & McNickle, 2005). The ECAFC is based on the (re)use of aBB microartefacts. In this research, the focus is on the ECAFC for the financial controlling module (Trad & Kalpić, 2019), as shown in Figure 4 where it interacts with the external world via an implemented real-world framework, like the *TRADf*. The *Project's* global RDP4FCA's topic' and final Research Question (RQ) is: "Which business transformation manager characteristics and which type of support should be assured in the implementation phase of a business transformation project?" The targeted business domain is any business environment that uses: 1) FinTech, internet and engineering technologies; 2) an enterprise architecture methodology for finance; and 3) frequent transformation iterations. For this phase of RD-P4FCA the sub-question is: "What is the impact of the ECAFC on Projects to support it to predict and eradicate collective financial crimes?".

## The Role and Risks of Intermediaries

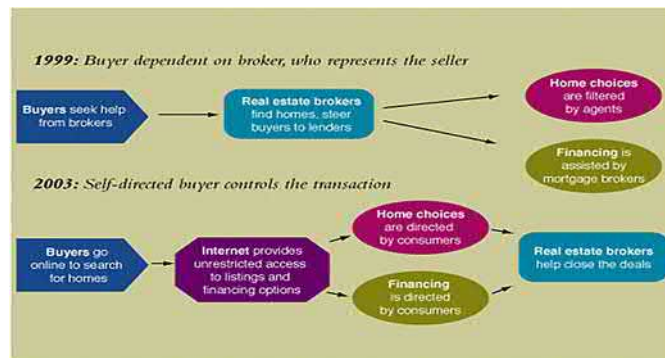
Today many companies have standardized their audit, governance, control and monitoring architecture; comparing to less than 10% before 10 years. This proves that the ECAFC is crucial for all *Projects* and financial subsystems for their availability and tracing criminal acts (Kowall & Fletcher, 2013). The *Manager* should be a member of the company's strategy team should diligently work with the company's risks and legal teams, where he can bring in an effective view to changes in the financial vision on engineering risk and legal regulations, control and governance integration issues; that stimulates the reduction of the number of intermediaries, especially the risky ones, like the Swiss financial institutions which are a major risk factor, as shown in Figure 5. The actual models use the following financial intermediaries:

1. Banks
2. Insurance companies (Yildirim, 2019)
3. Mutual funds

4. Non-Banking Financial institutions; and
5. Other financial services providers (Assay, 2019; Shahrokhi, 2008).

ECAFC combines management sciences, business administration, law and economics with FinTech and other engineering fields (Rafay, 2019; Universität St. Gallen, 2015).

*Figure 5. The ECAFC needed to reduce the number of intermediaries.*



## The Role of Financial Services

An important part of existing business/financial models, provide financial services over FinTech based online frontends. *Projects* can help banks and financial institutions reshape their business programmes, like during the 2008 financial crisis, where the ECAFC focus was on geographical reach, redefining global initiatives and reorganizing the trade services and prioritizing a customer-centric approach. Citibank restructured its activity centres and redefined its global strategy to assist customers in solving financial problems. Citibank's *Project* was very quick and the landscape for treasury and trade services was deeply modified to stand up again after the financial crisis. Multi-functional banking is a form of block-chaining, based on web technologies that enabled low cost and efficient financial operations. Citibank was the first financial institution to finalize a *Project* and that had a significant impact on the business domain models that in turn are based on sets of CSFs (Farhoomand & Lentini, 2008).

## Dangers Related to ECAFC

Dangers that can affect the ECAFC (Shahrokhi, 2008):

- *Project's* complexity can lead to significant financial losses.
- The *Project* is a major paradigm shift and there would be a need to adopt a new and different way of working.
- The business and finance environments complete policy issues should be controlled, verified and transformed.
- Important business and financial environments are often reluctant to execute radical *Projects*.

- Business and finance environments in most cases are resistant and reject major organizational and technological changes.
- Legal support for financial pitfalls.

## **Finance, Transactions, Security and Legal Constraints**

The CSFs manage the differences in Cyberbusiness', local and international laws. Cyberbusiness/finance environments must have the capacity to proactively recognize erroneous and suspicious financial Cybertransactions (Daellenbach & McNickle, 2005). Looking from the ECAFC view and related aspects, uniform bodies promulgate transaction governance acts on the global level and propagate these acts to legal enforcement in FinTech fields, like in the following cases:

- Many countries and regions have adopted financial standards to support the mentioned fields, like for example, financial transactions and digital signature's legislation. The vast majority of surveyed enterprises expressed the importance of developing a valid financial plan and a related legal framework; where they faced various types of legal problems (CEU, 2004; EC, 2013).
- Regarding financial Cybertransactions' security violations, the European commission defines a legislation to govern Cyberbusiness and progress has been done in its assertion. European commission's member states have implemented and enforced FinTech related national practices. Cybertransactions outcomes have to be continually legally asserted, traced, and their periodic summaries are reported to the executive management (Fu & Mittnight, 2015; EU, 2014).
- Cybertransaction is influenced by the Uniform Law Commissioners who promulgated the Uniform Electronic Transactions Act in 1999. It is the first adaptable effort to prepare a Cyberlaw for Cyberbusiness. Many countries have adopted Cyberbusiness regulations. The Uniform Electronic Transactions Act represents the first effort in providing some standardized rules to govern financial Cybertransactions.
- ECAFC's legislation assertion and integration of FinTech modules is done by using standardized legal module, like The Open Group's Architecture Framework (TOGAF). This legal supports data protection laws, contract law, procurement law, fraud law and many other legislation domains to counter organized financial crimes (Trad & Kalpić, 2019).
- Collective financial crimes schemes are a form of collective (or even state organized) crime(s), brutal dictators like neo-Nazi brigands have a special status in such states where the ownership of substantial financial assets can remain anonymous under a so-called banking secrecy and an opaque legal system. Some third world dictators maintain strong financial relationship to banks in financial havens, like Switzerland. Some of these banks have even been established by criminals emerged from former wars, like the example of the notorious Swiss Nazi banker Francois Genoud (Brown, 2016). A country where the money cannot be transparently audited can provide security to dubious collective crime schemes, investors, although otherwise the same country may serve as role model of law obeying common citizens. Some of financial havens and their financial institutions have been the main leaders in worldwide financial crimes/scandals, misdeeds, and criminal acts including; igniting civil wars, the LIBOR manipulation, currency manipulations, credits manipulations, supporting arms dealing transactions, hijacking people's wealth, subprime crisis, war victim wealth confiscation, organized tax evasion, drug dealing financial support, support against

future financial competitors, forced confiscations, drastic fines, financial spying, immigrants plundering and arms dealing (Clarke & Tigue, 1975; Parker, 2016).

- FinTech Cybersecurity international law shows that international law on cybersecurity is inefficient and agonizing; and even controlled by financial crimes states.

## **Structural, Behavioural and Cultural Predisposition**

The major problem with combating collective financial criminality is that some SOGFP countries, like Switzerland, have a hermetically closed system, characterised by the following characteristics:

- The legal system, used to ignore any attempt to investigate financial criminal acts; and would even look into making their financial institutions look as victims, like in the case of the UBS (and practically all Swiss banks) and tax fraud crimes against France and many other countries. Added to that, the legal costs and the attitude lawyers makes it impossible to search for justice. It must be noted that a Swiss lawyer would protect the financial institution and not his client.
- ECAFC should be capable of finding and tracing the cases of complex financial crimes like the ones committed by Swiss politicians, bankers and accountants (Cornevin, 2020).
- In such countries, legal support is too expensive, this fact discourages any action of law enforcement; like in the case of the Tunisian government's deposits and the Victims of the second World War.
- Psychological collective harassment, that is a part of the Swiss culture, is used to discriminate by using even racism, legal violence and other form of brutality, in order to discredit and discourage investigators and people seeking to be refunded.
- Intolerance and misunderstanding processes are used, in order to block any foreign request.
- A powerful global network, to embed and hide various dubious operations and to corrupt any politician anywhere in the world.
- Financial guerrilla-like and hit and run tactics, to confiscate wealth.
- Occurrence of financial locked-in situations and seizure of wealth.
- Financial haven states target to become leaders in FinTech, which is not very assuring; because FinTech should combat state criminality and enforce cybersecurity international law.
- Some states, like Switzerland, targets to be a leader in FinTech, which is definitely not very assuring; because FinTech should combat collective state's criminality and enforce international law.
- Police and information services are used to block any attempt to pursue financial criminal acts. They even will attack the parties looking for deposits, like in the Libyan case.
- It is strongly recommended to avoid any form of financial collaboration with SOGFP (financial havens) organizations, who use the above-described scenarios.

## **Locked-in Situations and Vision**

The ECAFC must define rules and objectives, in order to avoid financial locked-in situations. Locked-in situation can be defined as follows, *“a situation where an investor is unwilling or unable to exit a position because of the regulations, taxes or penalties associated with doing so. This may be an investment vehicle, such as a retirement plan, which cannot be accessed until a specified retirement date”*.

Financial locked-in, is when building the financial structure of the future transformed business environment, the *Project* team and *Manager* must be cautious of eventual financial locked-in situation(s). Even though some countries like Switzerland offer attractive financial and tax package(s), this country applies a coordinated legal and financial locked-in trap; it is sealed and represents an unwritten concept that can at any moment sweep out the financial resources from a business environment and even powerful countries like, the USA and France. This locked-in Swiss financial crimes model, combines Specific culture and mentality, the power of Swiss law, *Too Big to Fail* state banks, Banking secrecy that protects financial crimes, Ultraliberal economy, Rejection of local and global standards, Isolationism and racism and a supportive political environment for collective plundering.

Swiss banks and other Swiss financial institutions are under no supervision, whatsoever; and they are free to operate hit and run tactics. That indirectly makes this country, the financial industry's super protector that sets up fortifications against any possible legal intrusion; even when these institutions are executing massive irregular, criminal and illegal activities. The author refers to this phenomenon as an instance of the SOGFP based Black Swan phenomena or simply the directed Swiss Black Swan, which business environments and countries should try to avoid and should penalize. It is probably wiser to pay more taxes and social services than to face such phenomena and traps (International Monetary Fund, 2009).

FinTech locked-in, that implies that technologies in the actual financial domain influence is immense and it influences its productivity, growth and monetary policy; and supports sophisticated SOGFP crime schemes. It is a technology-driven domain and because of its hyper evolution depends on technology, the financial institution can be driven easily in a locked-in situation (Balling, Lierman & Mullineux, 2003). ECAFC should avoid to adopt a unique tool, the so-called all-in-one FinTech tools. Such FinTech tools request frequent commercial product upgrades that adds to complexity of the implementation and maintenance phases. FinTech Tools needed important features are frequently delayed or never finished, what can provoke failure to deliver fundamental *Project* modules. These all-in-one FinTech tools vary significantly from the defined open standards; and if a change is to be done for the system's reintegration, it is often incurring very high costs and *Project* risks.

The ECAFC must deliver an anti-locked-in strategy, where the ECAFC requires a holistic approach that must be supported by a global business environment and powerful international laws, which should combat locked-in situations by applying laws and standards against SOGFP attempts.

## **Financial Resources/Currencies and Usage Strategy**

The ECAFC must propose a unique currency to be used in its financial transactions. In the last few years, we have seen a convergence of the major industrial electronic currencies. This fact clearly shows the will to adapt to an incoming electronic and unique currency; and it is strongly recommended to avoid the usage Swiss Franc and any financial institution linked to Switzerland.

## **The Role of Accounting**

Concerning SOGFP, the most damaging fact, is that the business environment loses its transformational momentum, what can negatively affect its business sustainability and it can leave it to become prone to rigorous accounting austerity procedures. In this chapter, the author proposes a set of managerial recommendations on how to avoid such blocking situations. Today many advanced ECAFC related finance and accounting automation concepts exist. This chapter can support the *Project* of the traditional business

environment through the automation of all its financial operations and the related accounting processes. That also enables the underlying ECAFC to control the accounting subsystem which interacts with the local and global eco-systems. Transforming a traditional environment, the ECAFC accounting subsystem and the related accountants' behaviours are important to be controlled, because, it is probable that the accountant team(s) generate locked-in situations and resist to apply initiatives for major changes. An automated and controlled accounting subsystem may provide the base for flexible financial services and functions for the future business environment, in order to ignore the human dependency. That makes these services robust and precise. This main aim of this chapter is to support the *Managers* or enterprise architects in managing frequent changes of business environments and the integration of automated enterprise accounting procedures. To achieve this goal, the author offers *Managers* or enterprise architects, a set of managerial recommendations and an accounting automation pattern that could support a high volume of accounting requests and support their respective maintenance and implementation costs.

## The ECAFC Basics Critical Success Factors

This section's CSA set of filtered CSFs and their weightings are:

*Table 14. ECAFC's basic critical success factors that have the average of 9.00*

Critical Success Factors	AHMM based KPIs	Weightings
CSF_FRMSV_Basics_DecisionMakingApproach	ManagementView ▾	From 1 to 10. 10 Selected
CSF_FRMSV_Basics_RoleOfRisksIntermediaries	Mandatory ▾	From 1 to 10. 09 Selected
CSF_FRMSV_Basics_ServicesArchitecture	MicroartefactsBased ▾	From 1 to 10. 09 Selected
CSF_FRMSV_Basics_LegalConstraints	Chaotic ▾	From 1 to 10. 08 Selected
CSF_FRMSV_Basics_LockedInVision	Possible ▾	From 1 to 10. 09 Selected
CSF_FRMSV_Basics_CurrencyUsage	Controlled ▾	From 1 to 10. 09 Selected

Evaluate

## ECAFC'S STANDARDS AND CONCEPTS ADOPTIONS

### Fintech Standards for Integration

Nowadays there are many standards, and this section presents the most important ones; and tries to show how they help integration process of the ECAFC in *Projects*; like the Financial products Markup Language (FpML) which is an industry-standard protocol for complex financial products.

### Strategy and Vision for the Integration

ECAFC's strategy needs a specific approach for the integration of concepts that is based on the following facts:



- A strategy needs a multimodal finance model that minimizes the dependencies between various business and financial partners; where finance connections are established between the consumer and the end business environment with minimal risks and directly traces financial crimes.
- An important CSF that can be integrated in the ECAFC is the Financial Cost Ratio (FCR); which can be used before and after the *Project's* completion. To calculate costs related to financial operations, there is a need to add-up the total costs of providing financial services and to divide it by the total number of successfully executed financial transactions. *Projects'* finances' outcomes should be controlled in real-time and routine financial reports must be reported to the *Manager* and to the business enterprise's executive management. Financial impacts of *Projects* depend on security violations (Fu & Mittnight, 2015; Xiaohong, 2011).
- The ECAFC defines security violations' schemes, where business environment's functions and financial transactions are orthogonal to enterprise security requirements.
- The business' financial functions and transactions define the responsibility of the enterprise's financial results.
- Timestamps based regulations of the financial security requirements need qualified time-stamps to build robust certification techniques. When a signature is not used, then the *Project* team must prototype and develop qualified trust financial services to support the conformity and assessment of finance services. These trusted services should support an adequate level of financial security to comply with the rules like the ones of the European Union's regulations (EU, 2014).
- The *Project* proposes the use of timestamp servers that work on the basis of taking a hash of a block of items to be timestamped and to expose widely the hash container to all the *Project's* microartefacts (Nakamoto, 2008).

## **Valuation Concept**

The ECAFC defines business and financial valuation processes that are related to a set of procedures that can be applied to estimate the value of the business' financial capabilities, as shown in Figure 6.

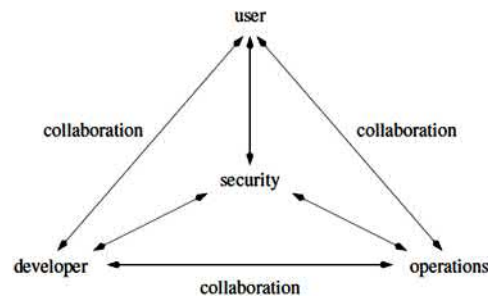
## **Standard and Cyber Securities**

The *Project* of a modern business/financial environment needs a well-designed Information and cyber Technology Security Automation Concept (ITSAC) (Trad & Kalpić, 2018b) that includes:

- A holistic cybersecurity architecture, where the *Manager's* role is important and his decisions are aided by using a framework like *TRADf*.
- The Cybersecurity Domains, as shown Figure 6, where governance defines the interaction between various components and their cyber or information technology requirements.
- The ECAFC Cybersecurity requirements settings use an optimal cybersecurity architecture that should fit in the company's global framework that in turn is based on best practices. The resultant cybersecurity architecture is a mixture of technical solutions, business engineering, and security concepts. TOGAF includes sub-frameworks, like the Sherwood Applied Business Security Architecture (SABSA) to handle Cybersecurity requirements.
- A unified control and logging subsystem, for FinTech for Cyberbusiness platforms which are not dedicated to any specific business/finance environment.

- ITSAC's microartefact is an instance of the building block that can interact with other *Project's* microartefacts in a traced and synchronized manner and uses TOGAF's ADM to assist it in the grouping of the needed services (The Open Group, 2011).

Figure 6. The architecture interface with security modules.



## The Standards' CSFS

This section's CSA set of filtered CSFs and their weightings are shown in Table 15.

Table 15. The security critical success factors 8.5

Critical Success Factors	AHMM based KPIs	Weightings
CSF_FRMSV_Standards_Integration	Possible	From 1 to 10. 08 Selected
CSF_FRMSV_Standards_Strategy	Mandatory	From 1 to 10. 09 Selected
CSF_FRMSV_Standards_ValuationConcept	Advanced	From 1 to 10. 09 Selected
CSF_FRMSV_Standards_Security	Complex	From 1 to 10. 08 Selected

Evaluate

## FINANCIAL CRIMES AND IRREGULARITIES

The ECAFC is adapted to model SOGFP influences on financial problems, crimes and even irregularities, in the form of state financial crime, that look as follows:

### Hit, Hide and Run Tactics... and Hiding Trillions...

ECAFC tries also to explain the damages done to various financial ecosystems by using its reasoning model. The proposed ECAFC uses various types of information sources like state organized financial crime references, banks' influence and legal processes, business/financial valuation, currency value manipulation, global domestic growth indices, finance institutions and global financial and influence networks. These used sources are needed to construct the ECAFC's CSFs (Trad, 2019), where financial

crimes, like fraud related to the UBS (Stupples, Sazonov & Woolley, 2019), in which 32 trillion US dollars are *hidden* and cases of complex financial crimes like the ones committed by Swiss accountants (Cornevin, 2020).

## Geopolitics

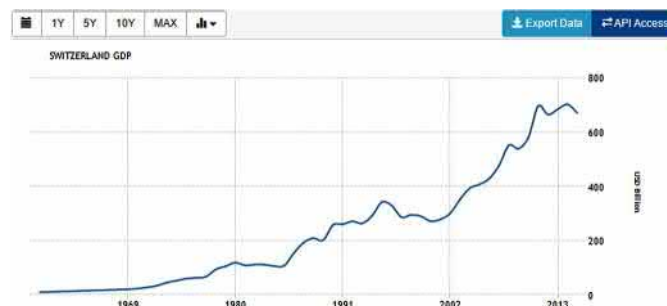
The ECAFC must be aware of the influence of geopolitics that can be categorized as follows:

- Many CSFs can influence geopolitical factors that can include the role of the local financial law enforcement agencies e.g. in Switzerland, which totally supports its banks, even it needs to break the law. Other factors are geopolitical relations' factors, political, ethnic and cultural setup, level of education, standard of life, financial competition and financial and legal control mechanisms.
- The need to localise possible geopolitical frontends for directed financial influence that is based on elite networks. For example, Switzerland builds elite networks, through good paid jobs, elite schools and financial business summits... These networks are often (mis)used for achieving SOGFP financial goals.
- The influence of geopolitics can be used to destabilize fragile countries like the Lebanon in which its democracy is unstable; that makes an easy target for SOGFP intentions (D'Amato, 1995).

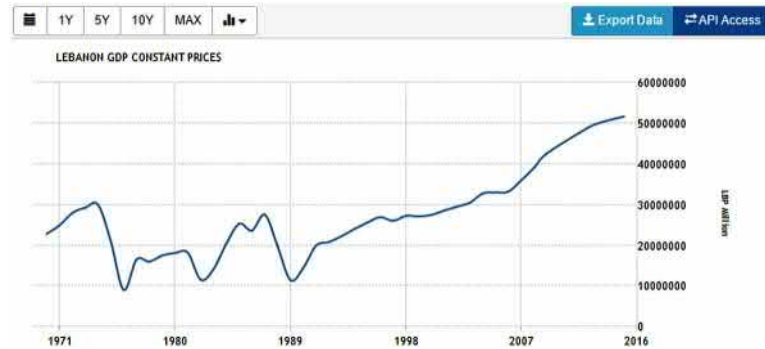
## Economic Growth of Switzerland

This section inspects if Switzerland took advantage of the Lebanese civil war, by looking and comparing Growth Domestic Product (GDP) diagrams. As shown in Figures 10 and 11, analysing the GDP diagrams' slopes and it seems obvious that the Lebanese declining GDP slope is inversely equivalent to the Swiss financial takeover. Switzerland is the unique country that gained financial advantage of the Lebanese tragedy, with the Lebanese GDP slide weakening its national currency. A perfect case to show a SOGFP scenario.

*Figure 7. Switzerland's economy growth*  
(Trading Economics, 2017a).



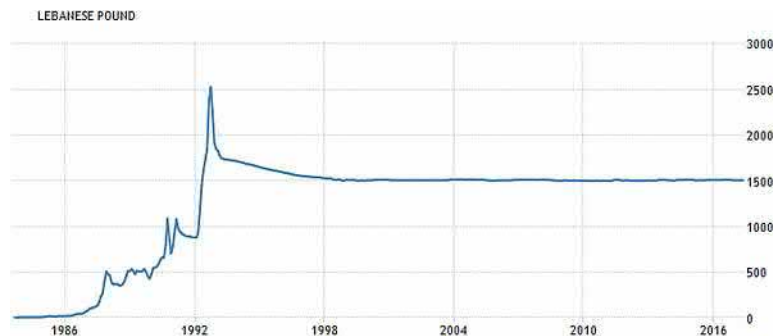
*Figure 8. Lebanon's economy growth  
(Trading Economics, 2017b).*



*Figure 9. Switzerland's currency evolution  
(Trading Economics, 2017c).*



*Figure 10. Lebanon's currency evolution  
(Trading Economics, 2017d).*



At the beginning of the Lebanese 1975 directed war, the Lebanon had its GDP drop to one third of its GDP of the early '70s. Although its currency before the 1975 war evolved to become a worldwide solid currency, there were speculations on replacing the legendary petrodollar with the Lebanese petrolira. Lebanon's fast enrichment placed it in the shooting range of the SOGFP hunter and enabled the Lebanon's replacement with its Western clone (Rolland, 2004). The SOGFP rumours-based collapse of the Intra

Bank and other Lebanese financial giants caused the migration of financial assets from the Lebanon to its Western clone (AMInfo, 2014). As shown in Figures 9 and 10, the Lebanese currency was replaced with the Swiss hard currency. More precisely, the Lebanon was replaced by its unique competitor, the Swiss Helvetic Confederation.

## **State Financial Crime-A Strategy and a Geo-political Phenomena**

The State Organized Global Financial Predators (SOGFP) is based on the following facts and assumptions:

- The Cartago-Phoenician General, Hannibal Barca, who tried to conquer Rome by crossing the Helvetic Swiss Alps, was slowed down by ambushes for collective and organized looting. These ambushes and looting schemes were launched by Germanic Helvetic tribes, who are the ancestors of modern peaceful Swiss nation. Such looting schemes became the moral founders of today's Swiss financial system, based on SOGFP. This historical cultural heritage and geopolitical construct can be considered as a typical Swiss behavior SOGFP.
- Financial crime is in general considered as the financial aspects used in the support of religious terrorist acts. The notion of states applying state crime exists (Agger & Jensen, 1996), so various types of means are used to support state crime, like religion, ideology... and in the case of Switzerland it is SOGFP. So, the term of SOGFP, can be labelled as states plundering other states or/and peoples by the means of financial and even adapted legal brutality, like organized looting. What is astonishing about the case of Switzerland, is that it is even considered an honest and as a moral example; and it seems as if it is above the law...
- SOGFP destroyed the Lebanon where Yasser Arafat's and Switzerland secretly agreed in the 1970s to support calls for Palestinian statehood, in return for not being targeted by Palestinian militants, according to a new book. Written by Marcel Gyr, a journalist with the Zurich-based Neue Zürcher Zeitung, the book alleges that the Swiss government took the unprecedented step of contacting Palestinian militants in 1970 (Fitsanakis, 2016). Such acts resulted in the following:
  - Switzerland violates the Lebanese sovereignty and pushes it into destruction... (Izzo, 2019).
  - In 1968, Intra Bank's founder a SOGFP legend and the destroyer of the Lebanese financial establishment, Youssef Beidas, dies in Switzerland in particular circumstances. At the time of his death he was classified by the Lebanese government as a notorious criminal and international terrorist.
  - Competition through destruction scenarios, like in the case of the Lebanon which had a jet-set tourism, which crated close ties with the Arab Gulf monarchies, and a loose and liberal banking system that was designed by Michel Sursock.
  - In 1973, the U.S. secretary of state Henry Kissinger accounts Assad's aggressive ambitions in the rich Lebanon and observes a possible solution to the Middle East confusion (El Hashem, 1990). The behaviour of Assad's Syria towards Lebanon's drive to the unknown and his Swiss bank accounts, may seal the conclusion that the Lebanese civil war had SOGFP external transformer.
  - Many valuable objects from Lebanon, were transferred and finished in Switzerland, starting with the 1975 civil war (Duparc, 2010)
- SOGFP placed role in the Sri-Lanka civil war (Chandrasekhar, 2018) where Swiss bankers in massive fraud, false documentation, money laundering, drugs dealing, arms dealing, and extortion.

## ***Tech-Based Enterprise Control and Audit for Financial Crimes***

- Credit Suisse backs SOGFP tactics in fraud worth \$2 billion in loans to Mozambique (Reuters, 2019).
- In the case of Greece more 200 billion were plundered, while Greece is extremely suffering.
- In the case Gadaffi and Libya the SOGFP looted over 100 billion and probably they will be never returned (Paravicini, 2018)
- The use of psychology to stop all possible legal initiatives and even make SOGFP related banks make substantial gains.
- The Nobel prize winner, the British economist, Angus Deaton, warns about the destructive predator's professional graduating business schools and to stop this type of brutalities. The leading school with such a perception is the Chicago school and the Swiss HEC (Le Monde, 2019). Such profiles can be classified as SOGFP profiles.

There are too many cases of ruthless and immoral SOGFP acts that can be all listed.

### **Ruthless and Immoral Attitudes**

SOGFP's cases of immorality and unhuman attitude are based on the following facts:

- Assisting in euthanasia cases, SOGFP, has found a new, very lucrative, business/financial model that is based on assisting people in committing suicides; a phenomenon that provoked countries to open penal cases in these suspicious Swiss deeds. The main suspicion is related to the deaths categorizing, by the Swiss officials, as natural death... But very lucrative ones. Two Swiss, *extremely human* foundations, Exit and Dignitas, will help anybody for 10000 euros, to end their lives and take care of their belongings... The main question here is, what happens to their wealth and inheritance? The Swiss swallows them all...
- Swallowing inheritance, is the Swiss financial pillar in which national banks make billions per year and their judicial system makes it impossible to make any claims... Many Swiss SOGFP dilapidations cases are very known, like the World War II dilapidation of refugees... All these looted resources make Swiss banks influences' greater in the world.

### **Banks' Influence**

The SOGFP based banks' influence strategy is based on:

- Destroying, various banking and financial institutions worldwide, which might be a menace for the SOGFP oriented banks. Like in the case of Lebanon, which attracted many regional and international institutions and personalities, who were interested in promoting their financial activities.
- Prevent financial concurrent to get close to the immense Arab oil-based wealth and their petrodollar dividends of which can be pouring into other banks.
- Sabotage of elite tourism that can endanger the Swiss one (Trad, 2019).

### **FinTech Fraud and Cybercriminal**

FinTech can enable massive fraud through:

- FinTech aims to change the traditional financial environment in the delivery of interactive financial services. The usage of intelligent financial endpoints provides some of the technologies intended to make financial services open to many external endpoints. Although FinTech can be used to tackle financial Cybercriminal, it seems that the countries that support massive financial crimes are making the largest investment in these innovative technologies (Ravanetti, 2016).
- It would make cash money more abstract and difficult to trace; individuals and institutions in GFP oriented countries that have the culture of financial secrecy and arbitral confiscation, would be tempted to use FinTech to obfuscate the origins of money transfers.
- With the rapid emergence of FinTech, blockchain technologies will dominate the leading financial giants and will probably cause the domination of the Bitcoin (or something similar). This new media would lead to the disappearance of leading currencies like the Swiss Franc and Euro; such an event would be a major problem for tracing financial fraud. This scenario is not assured and the possibility that the bulb of Cryptocurrencies might blow, should not be completely excluded.
- Blockchains is the technology framework that supports Cryptocurrency like the Bitcoin (Iqbal *et al.*, 2019). Where Bitcoin supports the exchange of currencies in a digital encryption form. FinTech automation causes, the synchronization of various Cyberfinance services that need specific regulation, law enforcements and cybersecurity mechanisms.
- Knowing that today, the most important phenomena are Cybercriminality as in emerging type of criminality and on the other hand, we have the apparent disappearance of traditional currencies.

## **State, Collective Behaviour and Culture Oriented Fraud**

This section analyzes the notions of fraud organized by SOGFP:

- The UBS, a state in a state, applies SOGFP and that is due to the following facts:
  - The Swiss UBS, is not just a bank, it is the skeleton of the Swiss financial system and closely related to the Swiss government apparatus...
  - Due to the 2008 financial crisis, the Swiss government gave this bank, with no obligation to return, 70 billion Swiss Francs, to help it to get out of the financial crisis...
  - The Swiss UBS, in which 32 trillion US dollars are *hidden* in only one remote island, so the question is, how much money this so-called bank illegally detains? ... (Stupples, Sazonov & Woolley, 2019).
  - The Swiss government ignores international claims on Fraud and even becomes a part of a state organized fraud, like the case of major Fraud case related to France and many other countries.
- The Swiss locked-in Swiss model combines: 1) the power and blockage of the Swiss law; 2) Too Big to Fail banks are untouchable; 3) Banking secrecy; 4) Ultraliberal economy; 5) Rejection of local and global standards; and 6) A specific political environment.
- The banks and other Swiss financial institutions are under no supervision whatsoever. That makes the country the financial industry protector. It has setup fortifications against any possible intrusion; even if these institutions officially known to execute irregular and illegal financial activities (Trad & Kalpić, 2017).
- The peak of such a SOGFP's behavior is the Fraud scandal related to the UBS that was hit with a historic fine and this incredible Fraud crime, was openly supported and protected by the Swiss

Federal Court that makes the SOGFP a state model. This model is officially protected by the penal law... Here there is a major dilemma and a question can be asked, how can such a country can be a synonym of honesty and anti-corruption... (Alderman, 2019; Tagliabuejune, 1986). Are Judges and politicians corrupt, by supporting major financial crimes?

- Accountancy crimes, like the ones committed by Swiss accountants are routine daily business (Cornevin, 2020).

## **Tax and Global Fraud**

This section analyzes the notions of the SOGFP's global fraud mechanisms (Trad & Kalpić, 2018c):

- There many SOGFP Fraud cases that damage practically all countries, like the USA, France, Germany, Greece, Lebanon... The hidden capital is reused as a credit to some poor countries.
- Transparency and black swans, which makes it impossible to calculate the risks of consequential rare events and predicting their occurrence (Taleb, 2007).
- The Swiss accountancy phenomena which define a complex locked-in, by using: 1) legal; and 2) financial and accounting national mentality or system; to blur financial flows and to disable any type of transparency or attempt of recuperation.
- Foreign business environments can easily slip in a complex locked-in situation and should try to avoid that.
- Shy steps have been taken to improve the transparency of how Switzerland's financial institutions should work. However, there is a lot to be done to fulfil various commitments on transparency conditions that Switzerland has committed itself to respect; like for example the ones defined by the international standards on transparency and exchange of information for tax purposes.
- Some credible sources like the Global Forum on Transparency and Exchange of Information for Tax Purposes peer review in 2011, has identified important deficiencies in the legal foundations for transparency and corruption in Switzerland, especially in relation with effective exchange of information (OECD 2011, 2014).

## **Mortgage Fraud and Manipulation**

This section analyzes the notions of mortgage manipulations and related fraud activities, which can be described as follows:

- In the USA, a federal judge accused the UBS of causing *catastrophic* investor losses in residential mortgage-backed securities sold before the 2008 financial crisis that caused more than \$41 billion of damage of subprime and other risky loans in 40 offerings (Stempel, 2019).
- The financial crisis of 2007 (that lasted to the year 2009) was marked by widespread fraud in the mortgage securitization industry. As the supply of mortgages began to decline around 2003, mortgage originators lowered credit standards and engaged in predatory lending to shore up profits. In turn, vertically integrated mortgage-backed securities issuers and underwriters committed illegal securities fraud to conceal this malfeasance and enhance the value of other financial products (Fligstein & Roehrkasse, 2019).



- Paula Ramada estimated the amount of lost money due to the benchmark of interest rates debacle is estimated at \$300 trillion in financial instruments, ranging from mortgages to student loans. Where a trillion represents 1 billion of billions ( $10^9 \times 10^9$ ) or  $10^{18}$ , a change or manipulation of a mere 0.1% has a damage of  $10^{15}$  of euros per year; this is the mechanism that banks used to cover the decrease of loans and save their investments at the cost of ruining middle and lower-class households; whereby some banks like the Swiss UBS got much richer. FinTech would make such operations more embedded and abstract (Trad, 2019). Especially the ones related to gigantic accountancy crimes, like the ones committed by Swiss accountants (Cornevin, 2020).

## **The Swiss Ruthless Competitor, a Global Predator**

This section analyses SOGFP as a financial threat because of the following facts:

- The unique and specific Swiss collective behaviour.
- Switzerland colonises many rich regions, like the Gulf countries, by means of wealth management and private banking.
- Switzerland's main political and ruling party, the Schweizer Volks Partie (SVP), a hate party, is an extreme far-right racist and anti-Semitic fascist entity that has a 1933-like attitude; where even Europeans are considered as an inferior race (Maurisse, 2016; Miller, 2017; Le News, 2015, 2017).
- Many of Swiss top leading politicians were convicted for racist hate crimes. A nation of collective hate, where Christian Levrat, compares the SVP party to fascist Nazi regimes (Tribune de Geneve, 2014). Where the SVP based Switzerland, uses the hate and xenophobe attitude as a moral factor for plundering.
- The latest world financial crisis main and only winner is Switzerland, who applied the SOGFP, who stayed loyal to its very long tradition of looting that is based on the motto: ... when a country goes bad, collect its fortune from its fleeing and desperate immigrating population; the same conduct was observed during World War II and in the latest immigration waves, where the Swiss police stripped the immigrants from all they have owned. As shown in Figure 11, the Swiss wealth deposits kept rising although the worldwide situation was declining.
- Switzerland and its most famous banks orchestrated the deportation and dilapidation of the victims of the Second World War (Rickman, 1999). This collaboration with the Nazi German Reich and other dictators raises extreme doubts regarding the Swiss government, mentality, and financial institutions and leads one to conclude they will do anything for financial profit.
- As already mentioned, the SOGFP applies discriminatory policies towards various categories, aiming their looting using the following:
- Marie Maurisse, a journalist describes the discriminatory behavior of the Swiss population, towards French and European citizens (Maurisse, 2016).
  - Edward Snowden's describes Switzerland as the most racist state in the world (Snowden, 2015).
  - The Swiss Federal Court accused leading members of the far right-wing Swiss People's Party (SVP) that is Switzerland's ruling party, guilty of racism and anti-Semitism, over propagating extreme racism, using racist symbols (The Local, 2017). Racism based on the color of skin as shown in Figure 15.

## Tech-Based Enterprise Control and Audit for Financial Crimes

- Plundering the Second World War II refugees, of which were expelled from Switzerland and perished in concentration camps.
- Switzerland requires from asylum seekers to hand over their assets, a similar behavior to the one in World War II (BBC, 2016).
- Special hate towards the intellectual elite, that Switzerland population is not university literate.
- Brutal and genocidal dictators like the Syria's Bashar al-Assad and his private brigands have a special status in Switzerland, where he owns a more than a billion-dollar bank account (Brown, 2016). Assad has a strong financial relationship to the Swiss Banque Commerciale Arabe, which was created and managed by the notorious Swiss Nazi banker Francois Genoud (Johnson, 1983), who was supported by Antoine Kamouh and Wafic Said, who financed and organized the Lebanese downslide (Brown, 2016).

This chapter can help governments and people in their daily activities in that they avoid the SOGFP and related Swiss financial products and services.

Figure 11. Swiss wealth management keeps rising  
(Trad, & Kalpić, 2019b).

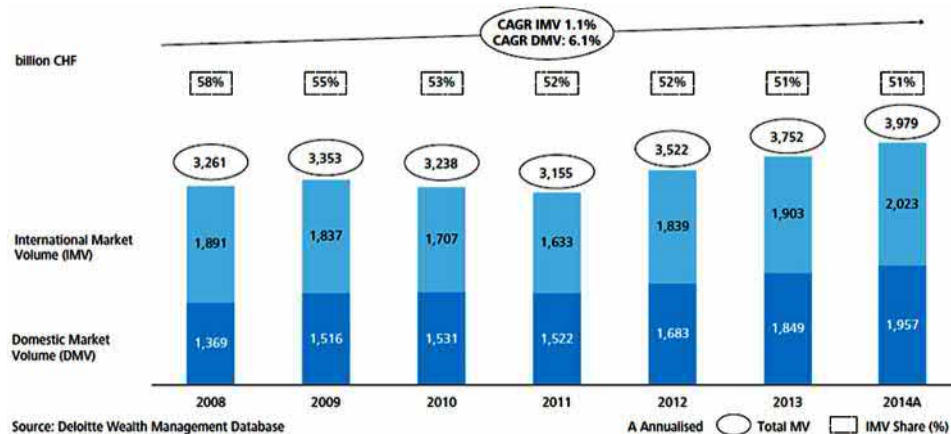


Figure 12. Racist swiss ruling party poster  
(The Local, 2017).



## **Slavery and Financial Aggressiveness**

Germanic (mainly Germans and Austrians) hatred of Semites and their support of the great Ottoman genocides; added to that fact, major Nazi officers became consultants of pan-Arab genocidal dictators and executive bankers in Swiss banks. The case of slavery, discrimination and racism in Germanic central Europe and more specifically in the regions of the peace-loving Helvetic Confederation, is studied by Swiss historians, who are supported by dozens of major public figures, together have launched a committee that inspects the case for *organized and structured worldwide slavery* managed by Swiss bankers and political leaders. This committee's main aim is to estimate reparations in the context of Switzerland's related organize slavery related crimes against humanities. In these crimes' major Swiss high-level politicians, trading companies, world class banks, cantons (like the Canton of Vaud, who still carry a slavery mentality), predatory family enterprises, mercenary contractors, soldiers and private individuals; all of them profited from the slave trade. Swiss organized financial links to the slave trade, makes them global predators of manhood and nationhood, this fact shows this nation's culture of greediness that comes out always, exactly like in the period of major plundering of victims of the Holocaust (Swissinfo, 2019).

## **The Automated Accounting Component**

The ECAFC promotes financial engineering driven business environments that use references to various types of asset management financial activities, like in this case of *Project* accounting, that are conducted by using different types of avant-garde governance, ICS and business service technologies; where the current form of integration is based on block-chains' automation. The ECAFC can be applied to many types of *Project* accounting engineering subfields. Today business enterprises are encountering massive pressure to manage their enterprise assets proactively and holistically, in order to ensure their ethical integrity, avoid SOGFP scenarios, business sustainability, reduce costs, and to integrate the continuously transformed legal, regulatory and economic environments. For a *Project* there is a need for a just in time decision making, planning and optimization activities; and to achieve that goal, the designed *Project's* process manages the inventory of the enterprise's assets, as shown in Figure 13 (Soft Expert, 2018).

## **LIBOR, Subprime, Fuzzy Loans and other form of Criminal Acts**

### **2008-... Ongoing Financial Crisis**

The actual major financial crisis and unbundling process which started in the year 2008, was ignited by many SOGFP misdeeds and the following are their subset:

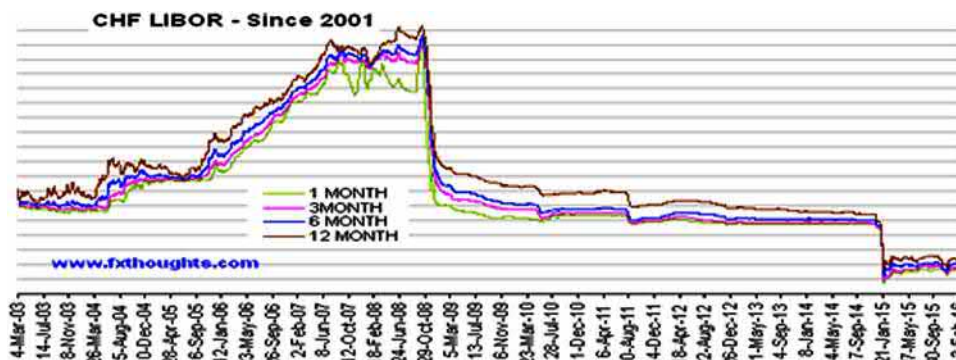
- Cash in Cash Out (CICO) overflow and disruption affected the modern global financial system that is based on a virtual asset management system. Such a system is based on money input and output flows, which with time created a gap. The gap created a CICO suspicion that in turn generated panic and in the traditional human silo logic, it was translated simply in the Subprime, LIBOR and many other financial crack syndromes. Added to that the lack of oil-generated money widened the CICO gap.
- LIBOR's down slide is an important CSF in the crisis that has been dropping sharply for a long time since begin of 2009 and that is one of the greatest SOGFP's misdeeds (Utt, 2008).

- The Subprime debacle, which was closely linked to the LIBOR and mortgage debt-based system. Where the LIBOR was adapted to cover the Subprime and other loses (Utt, 2008). The deterministic LIBOR fictive product caused major financial products to collapse and it seems that the applied governance methods were defiant, and the legal systems have been totally handicapped. The resultant multitude of global crises generated a global growth and employment downslide.
- The *Paradise papers fallout*, which evokes criminal financial deals that are done by SOGFP related countries and entities (Allen, 2017). And of course, nothing was done.

*Figure 13. Enterprise Asset Management*  
(Soft Expert, 2018).



*Figure 14. LIBOR interest rate's system degradation*  
(Minarchiste, 2015; Utt, 2008)



## Legal and Regulatory Constraints to Integrate

To design and implement an adequate regulatory component, there is a need to implement an AHMM4FCA based legal intelligence module that can be easily integrated with any framework, or tool standards (Gray, 1997). The International Organization of Securities Commissions (IOSCO) identified eight areas that actually constitute what is currently called FinTech. Such areas are payments, insurance, planning, trading and investments, blockchain, lending/crowdfunding, data and analytics, and security. The growth of the FinTech market implies a number of relevant issues and risks from a legal and governance perspectives. In this respect, financial regulation is increasingly complex with major financial entities required to comply with strict regulations in various jurisdictions. Like in various sectors, the complexity for regulators is to find the right balance between FinTech, national cultures and the need to regulate them correctly. Based on the European Banking Authority's report on prudential risks and opportunities, there are five legal issues that have to be considered when dealing with FinTech (and new technologies), these legal issues (Schiavo, 2019):

- Data protection and Cybersecurity.
- Distributed Ledger Technology (DLT) and smart contracts.
- DLT is an amount of shared and synchronized digital data spread across multiple sites or institutions, with no central administrator or data storage.
- An example of a DLT is a blockchain system.
- Automated-advisors and legal responsibility
- Outsourcing core financial activities to public clouds
- Biometric authentication using fingerprint recognition.

There are today many regulatory, governance, legal and audit frameworks, like for example, ISACA's COBIT; (Fu & Mittnight, 2015); but they are many hurdles for the integration process, because of the following reasons:

- As already presented some countries and institutions seem to be above the law...
- The complexity and incapacities of international laws, especially in the financial topics.
- The complexity the integration and automation of various complex frameworks.
- A discriminatory approach, where the rules are applied only to weak entities and never to the entities behind gigantic financial crimes, which are related to fraud and money laundering (Stupples, Sazonov & Woolley, 2019).

## The SOGFP Critical Success Factors

This section's CSA set of filtered CSFs and their weightings are shown in Table 16.

Table 16. The security critical success factors 10.00

Critical Success Factors	AHMM based KPIs	Weightings
CSF_SFT_BanksInfluence	Confirmed <input type="button" value="v"/>	From 1 to 10. 10 Selected
CSF_SFT_Brutality_CriminalActs	Confirmed <input type="button" value="v"/>	From 1 to 10. 10 Selected
CSF_SFT_DiscriminationPlundering	Confirmed <input type="button" value="v"/>	From 1 to 10. 10 Selected
CSF_SFT_GeopoliticalInfluence	Confirmed <input type="button" value="v"/>	From 1 to 10. 10 Selected
CSF_SFT_FinancialCrimes	Confirmed <input type="button" value="v"/>	From 1 to 10. 10 Selected

Evaluate

## THE PROOF OF CONCEPT OR PROTOTYPE'S INTEGRATION

### The Implementation Environment

The Proof of Concept (PoC) is implemented using the *TRADf* which was developed exclusively by the author, who owns the total copyrights. The PoC implementation uses aBBs based microartefacts on the basis of the granularity approach of the “1:1” mapping concept

### The Literature Review's Outcome

The literature review process' (or Phase 1) outcome that supports the PoC's background, by the use of an archive of an important set of references and links that are analysed using a specific interface. After selecting the CSA/CSFs tag is linked to various aBB microartefacts scenarios; which is implemented as an item, in an Excel file; where all its details are defined; this concludes Phase 1. In this chapter related PoC (or Phase 2), the grounded hyper-heuristics to process solutions.

### From Phase 1 to Phase 2

The *Project's* enumeration of CSAs is presented in the related works. The *TRADf* and the AHMM4FCA's main constraint, is to implement the PoC using simple *Projects* components, having a constraint, that is the CSA's average must be higher than 7.5. In the case, of the current CSA/CSFs evaluation, has an average result higher than 9, as shown in Tables 1 to 16.

### The Graphical User Interface for Intelligence Microartefacts

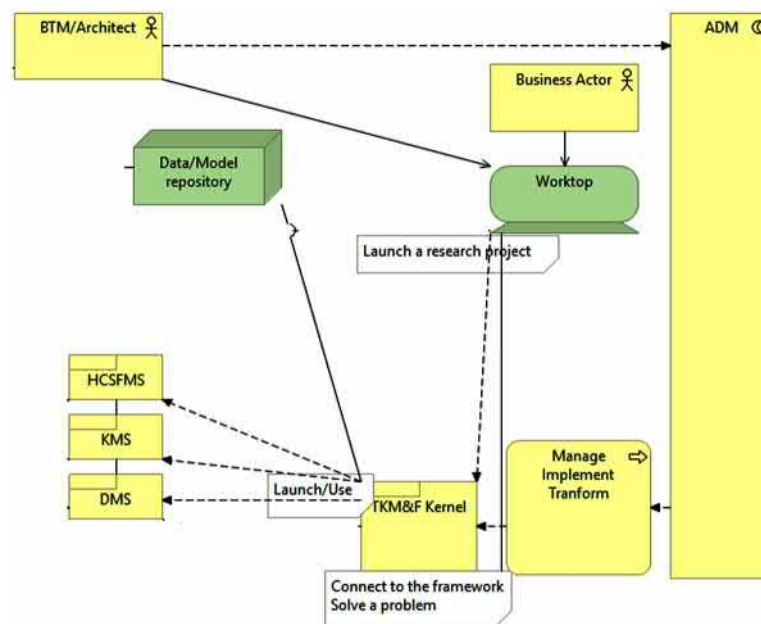
The PoC's main interface, as shown in Figure 15, links the aBB microartefact identifier to the list of *Project* resources where each resource has a its own Global User Identifier (GUID) and instance. A GUID links the aBB microartefact to an NLP4FCA implementation scenario that is choreography of aBB microartefacts. The previously defined user interface interaction also defines the management of aBB microartefacts.



Figure 17. The CSFs/CSAs selection/weighting from the main GUI.



Figure 18. The phase 2 interactions with factors, between all the components to enable problems solving.



## Linking the Applied Case Study – Integration and Unification

The PoC and the ArchiSurance ACS4FCA, with *Project* goals as shown in Figure 19; analyses a merger, of an old business system’s landscape that has become siloed, that results in abundant data and code. For this PoC, a financial auditing approach is tested to detect possible financial crimes.

For Phase 2, ECAFC’s goals, establishes a data architecture; as shown in Figure 20.

## Experiment’s Processing on a Concrete Tree Node

In Phase 2, the hyper-heuristics approach is used, to find a combination of heuristics’ action, used to solve a problem related to this chapter’s RQ. A specifically selected CSF is linked to a problem type and a related set of actions where the processing starts in the root node. Each problem, like this case the PRB\_SingleDataRecordSystem problem, has the following set of actions:



Figure 19. Transformation goals  
(Jonkers, Band & Quartel, 2012).

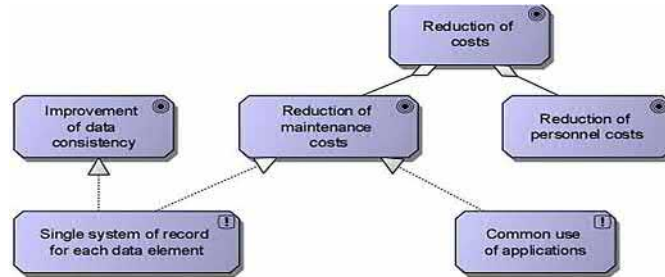
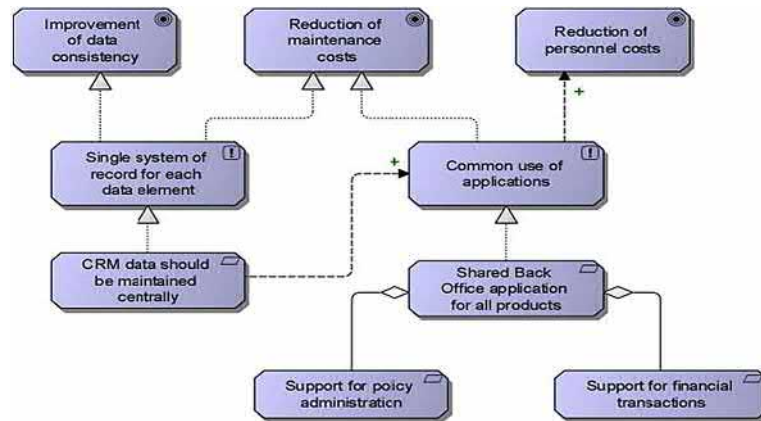


Figure 20. Data goals and principles  
(Jonkers, Band & Quartel, 2012).



- ACT\_SingleDataRecordSystem\_DefinePossibleAuditProcessing
- ACT\_SingleDataRecordSystem\_VerifyConstraintSet
- ACT\_SingleDataRecordSystem\_LocaliseOriginsOfResources
- ACT\_SingleDataRecordSystem\_IsSFT\_Related
- ...

For this KMS4FCA/DMS4FCA related PoC, the author has selected the CSF\_SingleDataRecordSystem\_Validation as the active CSF, taken from the CSFs pool. In this PoC the goal is to find solutions related to this selected CSF's related problems. The author has decided to apply the AHMM4FCA based reasoning to try to solve the CSF\_SingleDataRecordSystem\_Validation issues and the related problem or the PRB\_SingleDataRecordSystem\_Validation, which is solved by using the following steps:

- Relating the ACS4FCA infrastructure and financial transactions' integration capabilities to CSF\_SingleDataRecordSystem\_Validation capabilities is done in Phase 1.
- Link the processing of this node to the pseudo-quantitative modules, then by using qualitative modules, filter and deliver the initial state that is the root node of the *TRADf*'s decision tree.

- The internal heuristics engine is configured, weighted and tuned using configuration information.
- The set of possible solutions results from the hyper-heuristics decision model. Then the reasoning engine is launched to find the set of possible solutions in the form of possible improvements.
- Then follows the CSF attachment to a specific node of the *TRADf*'s graphical tree; to link later the aBB microartefacts.
- The processing tree (or the qualitative/hyper-heuristics decision tree) is a beam search heuristics model that uses the input from the previous phases to propose an optimal solution by using a common data bus.
- From the *TRADf* client's interface, the NLP4FCA development setup and editing interface can be launched to develop the finance related data services to be used in microartefacts.

## Selected Node Solution in Phase 2

The NLP4FCA scripts make up the processing logic of the ECAFC's defined problems and is supported by a set of actions. Where these actions are processed in the *TRADf* background to support aBB microartefacts that are called by the engine's actions, which deliver the solution and the flow of steps, as shown in Figure 21.

Figure 21. The *TRADf* heuristics tree configuration

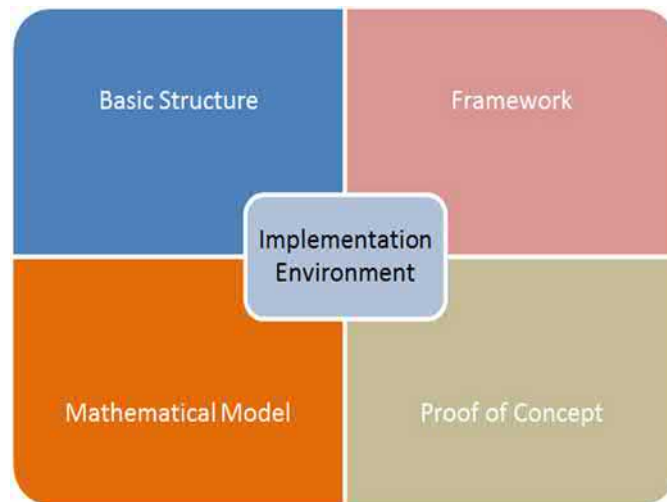


This RDP4FCA, the AHMM4FCA and its related CSAs/CSFs were selected as demonstrated previously and are shown in Figure 22.

## SOLUTIONS AND RECOMMENDATIONS

The ECAFC is a concept and a vision that can be used to transform a financial environment. Many industries have been implementing financial visions to respond to probable risks, legal problems and challenges in combatting financial crimes; especially the complex ones that are related to SOGFP. In

Figure 22. The TRADf's components' interaction.



this chapter, the main issue is how to define the optimal ECAFC using relevant resources discovered in the literature review phase and the *TRADf*'s PoC proved the feasibility of this approach and defined a related set of recommendations that are sorted by their importance:

- The proof of concept (PoC) proved the research project's feasibility by implementing the defined ECAFC CSFs concept.
- The *Manager* must deploy a microartefact based strategy and an anti-locked-in approach.
- The *Project* team skills should encompass knowledge of: 1) Financial engineering and the needed logging, monitoring and assertion architectures; 2) automated real-time business environments; and 4) governance and controls integration to detect SOGFP misdeeds.
- To design and implement an adequate ECAFC component: For a *Project* there is a need to implement a decision system that can be easily integrated with any framework or tool (Gray, 1997).
- Legal intelligence, decision making module and critical success factors: The decision-making module uses the *Project*'s logging system's database.
- Integrating other frameworks: Operations library and other standard frameworks can be integrated in the *Project* through the use of CSFs.
- Implement a global financial subsystem's approach for the control to block SOGFP's intrusions.
- The business environment must choose a currency strategy to be used in its financial transactions.

## CONCLUSION

ECAFC is part of a series of publications related to *Projects*; where its kernel, is based on CSAs and CSFs that support transformation activities. In this chapter the focus is on the ECAFC, which proposes a strategy to avoid financial crimes and locked-in situations that for financial predators, like major Swiss banks made impressive dirty trillions gains. These trillions are gained by Swiss banks, caused, civil wars and various looting schemes. Concerning, global financial predators and SOGFP, the Nobel prize winner,

the British economist, Angus Deatoun, warns about the destructive predator's professionals graduating from business schools, who cause major financial crimes. Deatoun recommends stopping this type of financial brutalities (Le Monde, 2019). Such profiles can be classified as SOGFP profiles. Ultimately, existing worldwide and international laws cannot prevent such an attitude, which has immense dimensions (Clarke & Tigue, 1975); which can imply that the world governing organism are corrupt and participating in this global crime. The evolution of ethics in finance might bring an end to such financial manipulations and eventually bring to trial countries and their financial system for committing major crimes against humanity. These crimes caused the deaths of hundreds of thousands of people and the looting of their goods. The Swiss prosecutor Carla Del Ponte a Swiss prosecutor, who was also the Chief prosecutor for war crimes committed in ex-Yugoslavia, hinted generals for alleged war crimes (Del Ponte & Sudetic, 2009). The astonishing fact is that why Carla Del Ponte did not prosecute Swiss financial circles who financed these war crimes and arms smuggling in these regions and other global crimes (Hamel, 2003). To make it even worse, the so called Del Ponte's Helvetic kingdom, harbours trillions that belong to stakeholders who organized the massacres in Bosnia and Croatia. Some countries, like France, have convicted the Swiss UBS with a multi-billion euros fine for fraud and tax evasion.

## **FUTURE RESEARCH DIRECTIONS**

The *TRADf* future research will focus on the *Business Transformation and Enterprise Architecture Framework as an Applied Mathematical Model-The Multidimensional Artificial Intelligence Concept* and the application in robotics.

## **DISCLAIMER**

The contents and views of this chapter are expressed by the authors in their personal capacities. It is not necessary for the Editor and the Publisher to agree with these viewpoints and they are not responsible for any duty of care in this regard.

## **ACKNOWLEDGMENT**

The authors extend sincere gratitude to:

- The Editor-in-Chief and International Editorial Advisory Board (IEAB) of this book who initially desk reviewed, arranged a rigorous double/triple blind review process and conducted a thorough, minute and critical final review before accepting the chapter for publication.
- All anonymous reviewers who provided very constructive feedbacks for thorough revision, improvement, extension and finetuning of the chapter.
- All colleagues, assistants and well-wishers who assisted the authors to complete this task.

## REFERENCES

- Agger, I., & Jensen, S. (1996). *Trauma and Healing Under State Terrorism*. ZEB Books.
- Alderman, L. (2019). French Court Fines UBS \$4.2 Billion for Helping Clients Evade Taxes. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/02/20/business/ubs-france-tax-evasion.html>
- Allen, M. (2017, November 12). *Swiss justice minister calls for commodities crackdown*. SWI. Retrieved from [https://www.swissinfo.ch/eng/paradise-papers-fallout\\_swiss-justice-minister-calls-for-commodities-crack-down/43669572](https://www.swissinfo.ch/eng/paradise-papers-fallout_swiss-justice-minister-calls-for-commodities-crack-down/43669572)
- AMInfo. (2014). Middle Eastern clients in the HSBC Switzerland leaks. *Swiss Leaks*. Retrieved from <http://ameinfo.com/luxury-lifestyle/list-middle-eastern-clients-in-the-hsbc-switzerland-leaks/>
- Assay, B. E. (2019). FinTech for Digital Financial Services: The African Case. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 61–80). IGI Global. doi:10.4018/978-1-5225-7805-5.ch004
- Balling, M., Lierman, F., & Mullineux, A. (2003). *Technology and Finance: Challenges for Financial Markets, Business Strategies and Policy Makers*. Routledge.
- BBC. (2016, January 15). Migrant crisis: Switzerland defends asset seizure law. *BBC*. Retrieved from <https://www.bbc.com/news/world-europe-35323315>
- Brown, J. (2016). Wafic Said: businessman, philanthropist and political fixer. *Financial Times*. Retrieved from <https://www.ft.com/content/a3cb764a-ecf1-11e5-bb79-2303682345c8>
- CEU. (2004). *Legal barriers in e-business: the results of an open consultation of enterprises* (Working Paper SEC (2004) 498). Brussels: Commission of the European Communities, Council of the European Union. Retrieved from <https://data.consilium.europa.eu/doc/document/ST-8997-2004-INIT/en/pdf>
- Chandrasekhar, A. (2018). Trial of LTTE Financiers Begins in Switzerland. *The Wire*. Retrieved from <https://thewire.in/external-affairs/trial-of-ltte-financiers-begins-in-switzerland>
- Clarke, Th., & Tigue, J. (1975). *Dirty money: Swiss banks, the Mafia, money laundering, and white-collar crime*. Simon and Schuster.
- Cornevin, Ch. (2020). La police démantèle un vaste système de blanchiment de fraude fiscale... [Police dismantles massive tax fraud laundering scheme]. *Le Figaro*. Retrieved from <https://www.lefigaro.fr/actualite-france/la-police-demantele-un-vaste-systeme-de-blanchiment-de-fraude-fiscale-20200110>
- D’Amato, G. (1995). Switzerland: A Multicultural Country without Multicultural Policies? In S. Vertovec & S. Wessendorf (Eds.), *The Multiculturalism Backlash: European Discourses, Policies and Practices*. Routledge.
- Daellenbach, H., McNickle, D., & Dye, Sh. (2012). *Management Science - Decision-making through systems thinking*. Palgrave Macmillan.
- Del Ponte, C., & Sudetic, C. (2009). *La traque, les criminels de guerre et moi: autobiographie* [The hunt, the war criminals and me: autobiography]. Éditions Héloïse d’Ormesson.

Duparc, P. A. (2010). La Suisse restitue au Liban les archives du fonds Dunand [Switzerland returns the archives of the Dunand collection to Lebanon]. *Le Monde*. Retrieved from [https://www.lemonde.fr/culture/article/2010/08/30/la-suisse-restitue-au-liban-les-archives-du-fonds-dunand\\_1404389\\_3246.html](https://www.lemonde.fr/culture/article/2010/08/30/la-suisse-restitue-au-liban-les-archives-du-fonds-dunand_1404389_3246.html)

EC. (2013). *Evaluating and improving existing laws*. Brussels: European Commission. Retrieved from [https://ec.europa.eu/smart-regulation/evaluation/docs/syn\\_pub\\_rf\\_mode\\_en.pdf](https://ec.europa.eu/smart-regulation/evaluation/docs/syn_pub_rf_mode_en.pdf)

El Hashem, B. (1990). *It was Kissinger who destroyed the nation of Lebanon*. EIR Feature.

EU. (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council - on electronic identification and trust services for electronic transactions in the internal market and repealing Directive. 1999/93/EC*. Brussels: Council of European Union. Retrieved from [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG)

Farhoomand, A. (2004). *Managing (e) business transformation*. Palgrave Macmillan. doi:10.1007/978-1-137-08380-7

Farhoomand, A., & Lentini, D. (2008). *e-Business Transformation in the Banking Industry: The Case of Citibank*. Asia Case Research Centre. The University of Hong Kong. Retrieved from [http://www.acrc.hku.hk/case/case\\_showdetails.asp?ct=newly&c=944&cp=1949&pt=1](http://www.acrc.hku.hk/case/case_showdetails.asp?ct=newly&c=944&cp=1949&pt=1)

Fitsanakis, J. (2016, January 25). Switzerland made secret deal with PLO in the 1970s, new book alleges. *Intelnews*. Retrieved from <https://intelnews.org/2016/01/25/01-1849/>

Fligstein, N., & Roehrkasse, A. F. (2016). The causes of fraud in the financial crisis of 2007 to 2009: Evidence from the mortgage-backed securities industry. *American Sociological Review*, 81(4), 617–643. doi:10.1177/0003122416645594

Fu, Zh., & Mitnight, E. (2015). *Critical Success Factors for Continually Monitoring, Evaluating and Assessing Management of Enterprise IT*. ISACA.

Gray, P. (1997). *Artificial legal intelligence*. Dartmouth Publishing Co.

Grewal-Carr, V., & Marshall, S. (2016). *Block-chain Enigma. Paradox. Opportunity*. London: Deloitte LLP. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf>

Hamel, I. (2003). Victoire à l'arraché d'un trafiquant d'armes [Victory in the snatch of an arms dealer]. *Swissinfo*. Retrieved October 2019, from <https://www.Swissinfo.ch/fre/victoire-%C3%A0-l-arrach%C3%A9-d-un-trafiquant-d-armes/3212952>

Hussain, M., Nadeem, M. W., Iqbal, S., Mehrban, S., Fatima, S. N., Hakeem, O., & Mustafa, G. (2019). Security and Privacy in FinTech: A Policy Enforcement Framework. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 81–97). IGI Global. doi:10.4018/978-1-5225-7805-5.ch005

IFRS. (2017). *IFRS Standards*. Retrieved from <http://www.IFRS.org/Pages/default.aspx>

International Monetary Fund. (2009). *Switzerland: Financial Sector Assessment Program - Detailed Assessment of Observance of Financial Sector Standards and Codes*. International Monetary Fund.

- Iqbal, S., Hussain, M., Munir, M. U., Hussain, Z., Mehrban, S., Ashraf, A., & Ayubi, S. (2019). Crypto-Currency: Future of FinTech. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 1–13). IGI Global. doi:10.4018/978-1-5225-7805-5.ch001
- Izzo, S. (2019). *Karl-Heinz Hoffmann's Secret History Links Neo-Nazis With Palestinian Terror*. Tablet Magazine. Retrieved from <https://www.tabletmag.com/jewish-arts-and-culture/culture-news/286220/karl-heinz-hoffmann-far-right> 1/11
- Johnson, S. (1983). Francois Genoud: Terrorist controller for Swiss banks. *Executive Intelligence Review*.
- Jonkers, H., Band, I., & Quartel, D. (2012). ArchiSurance Case Study. *The Open Group*. Retrieved from <https://publications.opengroup.org/y163>
- Kabzeva, A., Niemann, M., Müller, P., & Steinmetz, P. (2010). Applying TOGAF to Define and Govern a Service-oriented Architecture in a Large-scale research & development (R&D). *Proceedings of the Sixteenth Americas Conference on Information Systems*.
- Kowall, J., & Fletcher, C. (2013). *Modernize Your Monitoring Strategy by Combining Unified Monitoring and Log Analytics Tools*. Gartner Inc.
- Kyte, A. (2010). *Nine Critical Success Factors for Business Value -Through Application Overhaul*. Gartner Inc.
- Le Monde. (2019). Le Prix Nobel d'économie Angus Deaton: Quand l'Etat produit une élite prédatrice [Nobel Laureate in Economics Angus Deaton: "When the state produces a predatory elite]. *Le Monde*. Retrieved from [https://www.lemonde.fr/idees/article/2019/12/27/angus-deaton-quand-l-etat-produit-une-elite-predatrice\\_6024205\\_3232.html](https://www.lemonde.fr/idees/article/2019/12/27/angus-deaton-quand-l-etat-produit-une-elite-predatrice_6024205_3232.html)
- Le News. (2015). Swiss People's Party (UDC) leaders found guilty of racism. *Le News*. Retrieved from <https://lenews.ch/2015/04/30/two-swiss-peoples-party-udc-leaders-found-guilty-of-racism/>
- Le News. (2017). Racism sentence upheld against former Swiss People's Party secretary general. *Le News*. Retrieved from <https://lenews.ch/2017/04/13/racism-sentence-upheld-against-former-swiss-peoples-party-secretary-general/>
- Maurisse, M. (2016). L'enfer des expatriés français en Suisse: une «enquête». [The hell of French expatriates in Switzerland: an "investigation"]. *Le Temps*. Retrieved from <https://www.letemps.ch/opinions/lenfer-expatries-francais-suisse-une-enquete>
- Miller, J. (2017). Swiss high court rules anti-immigration SVP ad broke racism laws. *Reuters*. Retrieved from <https://www.reuters.com/article/us-swiss-racism-svp-idUSKBN17F1UT>
- Minarchiste, P. L. (2015). Quelles sont les causes de la crise de 2008? [What are the causes of the 2008 crisis?] *Contrepoints*. Retrieved from <https://www.Contrepoints.org/2015/03/14/201111-quelles-sont-les-causes-de-la-crise-de-2008>
- Myers, B. A., Pane, J. F., & Ko, A. (2004). Natural programming languages and environments. *Communications of the ACM*, 47(9), 47–52. doi:10.1145/1015864.1015888

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <https://bitcoin.org/bitcoin.pdf>

OECD. (2011). *Putting an end to offshore tax evasion*. Global Forum on Transparency and Exchange of Information for Tax Purposes, Switzerland. Retrieved from <http://www.oecd.org/tax/transparency/>

OECD. (2014). *Development Co-operation Report*. The Organisation for Economic Co-operation and Development. Retrieved from <https://www.oecd.org/dac/development-cooperation-report/>

Paravicini, G. (2018). Millions flow from Gaddafi's 'frozen funds' to unknown beneficiaries. *Politico*. Retrieved from <https://www.politico.eu/article/muammar-gaddafi-frozen-funds-belgium-unknown-beneficiaries/>

Parker, S. (2016). *The demise of secret bank accounts – Switzerland's private banks. face a new era of transparency*. Wolters Kluwer Financial Services, Inc.

Rafay, A. (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5

Ravanetti, A. (2016). Switzerland Bank on Fintech with Lighter Regulations. *Crowd Valley*. Retrieved from <https://news.crowdvalley.com/news/switzerland-bank-on-fintech-with-lighter-regulations>

Reuters. (2019). Swiss group files criminal complaint against Credit Suisse over Mozambique loans. *Reuters*. <https://www.Reuters.com/article/us-mozambique-creditsuisse/swiss-group-files-criminal-complaint-against-credit-suisse-over-mozambique-loans-idUSKCN1S5174>

Rickman, G. J. (1999). *Swiss Banks and Jewish Souls*. Transaction Publishers.

Rolland, J. (2004). *Lebanon: Current Issues and Background*. Nova Science Publishers Inc.

Schiavo, V. (2019). FinTech: the top five legal issues to consider. *Dentons*. Retrieved from <https://www.dentons.com/en/insights/articles/2019/february/26/fintech-the-top-five-legal-issues-to-consider>

Shahrokhi, M. (2008). E-finance: Status, Innovations, Resources and Future Challenges. *Managerial Finance*, 34(6), 365–398. doi:10.1108/03074350810872787

Snowden, E. (2015). Most Racist, Award Goes To ... Switzerland? *Skating on Stilts*. Retrieved from <https://www.skatingonstilts.com/skating-on-stilts/2015/03/and-the-edward-Snowden-most-racist-award-goes-to-switzerland.html>

Soft Expert. (2018). Enterprise Asset Management. *Soft Expert*. Retrieved from <https://www.softexpert.com/solucao/enterprise-asset-management-eam/>

Stempel, J. (2019). UBS must defend against U.S. lawsuit over 'catastrophic' mortgage losses. *Yahoo Finance*. Retrieved from <https://finance.yahoo.com/news/ubs-must-defend-against-u-214743943.html>

Stupples, B., Sazonov, A., & Woolley, S. (2019, July 26). UBS Whistle-Blower Hunts Trillions Hidden in Treasure Isles. *Bloomberg*. Retrieved from <https://www.bloomberg.com/news/articles/2019-07-26/ubs-whistle-blower-hunts-trillions-hidden-in-treasure-islands>



- Swissinfo. (2019). Swiss launch committee on slavery reparations. *Swissinfo*. [https://www.swissinfo.ch/eng/history-\\_swiss-launch-committee-on-slavery-reparations-/45421506](https://www.swissinfo.ch/eng/history-_swiss-launch-committee-on-slavery-reparations-/45421506)
- Tagliabue June, J. (1986). The Swiss stop keeping secrets. *The New York Times*. Retrieved from <https://www.nytimes.com/1986/06/01/business/the-swiss-stop-keeping-secrets.html>
- Taleb, N. (2007). *The Black Swan-The Impact of the Highly Improbable*. The Random House.
- The Local. (2017). SVP ad ruled racist by Swiss supreme court. *The Local*. <https://www.thelocal.ch/20170413/svp-ad-ruled-racist-by-swiss-supreme-court>
- The Open Group. (2011). *Architecture Development Method*. The Open Group. Retrieved from <https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap05.html>
- Trad, A. (2019). The Business Transformation and Enterprise Architecture Framework Applied to Analyze the Historically Recent Rise and the 1975 Fall of the Lebanese Business Ecosystem. In E. A. Nyam & A. H. Tunde (Eds.), *Impacts of Violent Conflicts on Resource Control and Sustainability* (pp. 75–108). IGI Global. doi:10.4018/978-1-5225-5987-0.ch004
- Trad, A. (2019c). *Using Google analytics to determine the leading business transformation framework that are based on enterprise architecture*. IBISTM.
- Trad, A. (2020). *The Business Transformation Framework and Enterprise Architecture Framework-The Financial Control and Technology Concept (FCTC)*. IGI Global.
- Trad, A., & Kalpić, D. (2016). The Business Engineering Transformation Framework for (e)commerce Architecture-Modelling Projects. In I. Lee (Ed.), *Encyclopaedia of E-Commerce Development, Implementation, and Management*. IGI Global. doi:10.4018/978-1-4666-9787-4.ch052
- Trad, A., & Kalpić, D. (2018a). The Business Transformation and Enterprise Architecture Framework: The Financial Engineering Technology Concept. In B. Sergi, F. Fidanoski, M. Ziolo, & V. Naumovski (Eds.), *Regaining Global Stability After the Financial Crisis* (pp. 23–45). IGI Global. doi:10.4018/978-1-5225-4026-7.ch002
- Trad, A., & Kalpić, D. (2018b). The Business Transformation Framework and Enterprise Architecture Framework for Managers in Business Innovation: The Role of Cyber and Information Technology Security in Automated Business Environments. In B. Christiansen & A. Piekarz (Eds.), *Global Cyber Security Labor Shortage and International Business Risk* (pp. 19–37). IGI Global.
- Trad, A., & Kalpić, D. (2018c). The Business Transformation Framework and Enterprise Architecture Framework for Managers in Business Innovation. The role of legacy processes in automated business environments. *The Proceedings of E-LEADER 2017 Berlin, 1*.
- Trad, A., & Kalpić, D. (2019). The Business Transformation Framework and its Business Engineering Law support for (e)transactions. In M. Khosrow-Pour (Ed.), *Advanced Methodologies and Technologies in Business Operations and Management* (pp. 230–246). IGI Global. doi:10.4018/978-1-5225-7362-3.ch017
- Trad, A., & Kalpić, D. (2020). *Using Applied Mathematical Models for Business Transformation*. IGI Global. doi:10.4018/978-1-7998-1009-4

Trading Economics. (2017a). *Switzerland - GDP Annual Growth Rate*. Trading Economics. Retrieved from <http://www.tradingeconomics.com/>

Trading Economics. (2017b). *Lebanon - GDP Annual Growth Rate*. Trading Economics. Retrieved from <http://www.tradingeconomics.com/>

Trading Economics. (2017c). *Switzerland's currency evolution*. Trading Economics. Retrieved from <http://www.tradingeconomics.com/>

Trading Economics. (2017d). *Lebanon's currency evolution*. Trading Economics. Retrieved from <http://www.tradingeconomics.com/>

Tribune de Genève. (2014, September 14). Pour Christian Levrat, l'UDC est sur la voie du fascisme [For Christian Levrat, the SVP is on the path to fascism]. *Tribune de Geneve*. Retrieved from <https://www.lematin.ch/story/pour-christian-levrat-l-udc-est-sur-la-voie-du-fascisme-345254850803>

Universität St. Gallen. (2015). *EMBA in Financial engineering*. Executive School of Universität St. Gallen. Retrieved from <https://www.unisg.ch/>

Utt, R. (2008). The Subprime Mortgage Market Collapse: A Primer on the Causes and Possible Solutions. *Heritage Foundation*. Retrieved from <https://www.heritage.org/report/the-subprime-mortgage-market-collapse-primer-the-causes-and-possible-solutions>

Xiaohong, Ch. (2011). *Research on E-Commerce Transaction Cost-Benefit Characteristics and Evaluation Approaches*. Management and Service Science (MASS), 2011 International Conference. Wuhan. China.

Yıldırım, I. (2019). Emergence of Insurance Technologies (InsurTech): The Turkish Case. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 42–60). IGI Global. doi:10.4018/978-1-5225-7805-5.ch003

## ENDNOTE

- <sup>1</sup> The earlier versions of this concept were published in the following publications of the principal author: a) Trad, A. (2019). The Business Transformation Framework and Enterprise Architecture Framework for Managers in Business Innovation: Knowledge Management in Global Software Engineering (KMGSE). In *Human Factors in Global Software Engineering* (pp. 20-49). PA: IGI Global. b) Trad, A. (2019). The Business Transformation and Enterprise Architecture Framework Applied to Analyze the Historically Recent Rise and the 1975 Fall of the Lebanese Business Ecosystem. In *Impacts of Violent Conflicts on Resource Control and Sustainability* (pp. 75-108). PA: IGI Global. c) Trad, A., & Kalpić, D. (2017). The business transformation and enterprise architecture framework The London Interbank offered rate crisis-the model. *The Business & Management Review*, 9(2), 67-76. d) Trad, A. (2019). An Applied Mathematical Model for Business Transformation and Enterprise Architecture: The Holistic Organizational Intelligence and Knowledge Management Pattern's Integration (HOI&KMPI). *International Journal of Organizational and Collective Intelligence (IJOICI)*, 11(1), 1-25.

## Compilation of References

(2011). An Intrusive World. In Curley, R. (Ed.), *Issues in Cyberspace: From Privacy to Piracy* (pp. 45–60). Britannica Educational Publishing.

A. V. v. iParadigms, LLC, No. 08-1424, No. 08-1480 (4th Cir., 2009).

Abdallah, W. M. (2008). The Economic and Political Factors and Their Impact on Accounting and Management in the Gulf Countries. In *Accounting, Finance, and Taxation in the Gulf Countries*. Palgrave Macmillan. doi:10.1057/9780230614543\_2

Abdikhiku, L., Pugh, G., & Hashi, I. (2018). Business tax evasion in transition economies: A cross-country panel investigation. *The European Journal of Comparative Economics*, 15(1), 11–36.

Abdulai, A. M. (2020). Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud. *International Journal of Cyber Crime*, 14(1), 157–174. doi:10.5281/zenodo.3749468

Abdullahi, R., & Mansor, N. (2015). Fraud triangle theory and fraud diamond theory. understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 5(4), 38–45.

Abdulrahman, S. (2019). Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper. *International Journal of Accounting & Finance Review*, 4(2), 13–21.

Abdulrahman, S. (2019). Forensic accounting and fraud prevention in Nigerian public sector: A conceptual paper. *International Journal of Accounting & Finance Review*, 4(2), 13–21. doi:10.46281/ijaf.v4i2.389

Ablon, L. (2018, March 15). *A Close Look at Data Thieves*. Retrieved from <https://www.rand.org/pubs/testimonies/CT490.html>

Abri, A.F., Arumugam, D., & Balasingam, S. (2019) Impact of the corporate governance on the financial statement fraud: A study focused on companies in Tanzania. *International Journal of Recent Technology and Engineering*, 7(5s), 336–341.

ABS. (2020). *5506.0 - Taxation Revenue 2018-19*. Australian Bureau of Statistics. Australian Government Printer.

ACFE. (2008). *Fraud risk management: a guide to good practice*. ACFE.

ACFE. (2009). *Fraud examiners manual*. ACFE.

ACFE. (2014). *Report to the Nation on Occupational Fraud and Abuse*. ACFE. Retrieved from <https://www.acfe.com/rtn/docs/2014-report-to-nations.pdf>

ACFE. (2016). *Report to the Nations on Occupational Fraud and Abuse*. Global Fraud Study. Retrieved from <https://www.acfe.com/rtn2016/docs/2016-report-to-the-nations.pdf>

ACFE. (2020a). *Global study on occupational fraud and abuse*. ACFE Publication.

## Compilation of References

- Adler, F. (1975). *Sisters in Crime: The Rise of the New Female Criminal*. McGraw-Hill.
- Afield, W. E. (2014). A Market for Tax Compliance. *Cleveland State University Law Review*, 62(2), 315–341.
- Aggarwal, C. C., & Yu, P. S. (2005). An effective and efficient algorithm for high-dimensional outlier detection. *The VLDB Journal*, 14(2), 211–221. doi:10.1007/00778-004-0125-5
- Agger, I., & Jensen, S. (1996). *Trauma and Healing Under State Terrorism*. ZEB Books.
- Aghion, P., Akcigit, U., Cagé, J., & Kerr, W. R. (2016). *Taxation, corruption, and growth* (Working Paper Series, No. 21928). NBER.
- Ahmad, N. F. G., & Abdul-Rahman, A. (2020). Shari'ah Governance and Audit Assurance in Islamic Banks. In A. Rafay (Ed.), *Growth and Emerging Prospects of International Islamic Banking* (pp. 278–297). IGI Global. doi:10.4018/978-1-7998-1611-9.ch015
- Ahmad, S. A., Yunus, R. M., Ahmad, R. A. R., & Sanusi, Z. M. (2014). Whistleblowing behaviour: The influence of ethical climates theory. *Procedia: Social and Behavioral Sciences*, 164, 445–450. doi:10.1016/j.sbspro.2014.11.101
- Ahmed, J., Collins, P., & Meera, A. K. M. (2020). Conditional Currency Convertibility Based on Primary Commodities: The Shari'ah-Compliant Grondona System. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 61–84). IGI Global. doi:10.4018/978-1-7998-0218-1.ch004
- Aichorn, A. (1935). *Wayward Youth*. Viking Press.
- AICPA. (2008). *FVS practice aid 10-1 serving as an expert witness or consultant*. American Institute of Certified Public Accountant.
- AICPA. (2009, July). The Evolution of the CFF Credential. *The Practicing CPA- The Newsletter of the AICPA Private Companies Practice Section*, 1-8.
- AICPA. (2019). *AICPA professional standards*. Wiley.
- Ajaz, T., & Ahmad, E. (2010). The effect of corruption and governance on tax revenues. *Pakistan Development Review*, 49(4), 405–417. doi:10.30541/v49i4Ipp.405-417
- Akdede, S. H. (2006). Corruption and tax evasion. *Doğuş Üniversitesi Dergisi*, 7(2), 141–149. doi:10.31671/dogus.2019.247
- Akkeren, J. V. (2018). Fraud triangle: Cressey's fraud triangle and alternative fraud theories. In D. C. Poff & A. C. Michalos (Eds.), *Encyclopedia of business and professional ethics* (pp. 1–3). Springer. doi:10.1007/978-3-319-23514-1\_216-1
- Alagna, V. (2020). *A Comparative Analysis of Identity Theft within America and Australia*. Retrieved from Criminal Justice: [https://scholarsarchive.library.albany.edu/honorscollege\\_cj/24/](https://scholarsarchive.library.albany.edu/honorscollege_cj/24/)
- Alam, M. D., Tabash, M. I., Hassan, M. F., Hossain, N., & Javed, A. (2021). Shariah Governance Systems of Islamic Banks in Bangladesh: A Comparison with Global Governance Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Alao, A. A. (2016). Forensic auditing and financial fraud in Nigerian deposit money banks (DMBs). *European Journal of Accounting, Auditing and Finance Research*, 4(8), 1–19.
- Albrecht, C. C., Albrecht, W. S., & Dunn, J. G. (2001). Can auditors detect fraud: A review of the research evidence. *Journal of Forensic Accounting*, 2(1), 1–12.
- Albrecht, S., Howe, K., & Romney, M. (1984). *Deterring Fraud: The Internal Auditor's Perspective*. Institute of Internal Auditors Research Foundation.

- Albrecht, W. S., Albrecht, C. C., Albrecht, C., & Zimbelman, M. F. (2011). *Fraud Examination* (3rd ed.). Cengage Learning.
- Alderman, L. (2019). French Court Fines UBS \$4.2 Billion for Helping Clients Evade Taxes. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/02/20/business/ubs-france-tax-evasion.html>
- Alexander, C., & Cumming, D. (2020). *Corruption and Fraud in Financial Markets: Malpractice, Misconduct and Manipulation*. Wiley.
- Alia, M., & Branson, J. (2011). The effect of environmental factors on accounting diversity. A literature review. SSRN *Digital Library*. Retrieved from <https://ssrn.com/abstract=1780479>
- Alibert, R. (1926). *Le controle juridictionnel de l administration an moyen du recours pour exces de pouvoir* [Judicial control of the administration by means of the appeal for abuse of power]. Payot.
- Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, 100, 408–427. doi:10.1016/j.future.2019.03.041
- Al-Jibaly, M. (2005). *Inheritance Regulations & Exhortations* (2nd ed.). Al-Madinah al-Munawwarah: Al-Kitab & Sunnah Publishing.
- Allan, G. (2005). Responding to cybercrime: A delicate blend of the orthodox and the alternative. *New Zealand Law Review*, 149–178.
- Allan, R. (2003). Fraud-the human face of fraud: Understanding the suspect is vital to any investigation. *CA Magazine-Chartered Accountant*, 136(4), 39–40.
- Allen, M. (2017, November 12). *Swiss justice minister calls for commodities crackdown*. SWI. Retrieved from [https://www.swissinfo.ch/eng/paradise-papers-fallout\\_swiss-justice-minister-calls-for-commodities-crack-down/43669572](https://www.swissinfo.ch/eng/paradise-papers-fallout_swiss-justice-minister-calls-for-commodities-crack-down/43669572)
- Alleyne, B., & Amaria, P. (2013). The effectiveness of corporate culture, auditor education, and legislation in identifying, preventing, and eliminating corporate fraud. *International Journal of Business, Accounting and Finance*, 7(1), 34–62.
- Allingham, M. G., & Sandmo, A. (1972). Income tax evasion: A theoretical analysis. *Journal of Public Economics*, 1(3–4), 323–338. doi:10.1016/0047-2727(72)90010-2
- Alm, J., Martinez-Vazquez, J., & McClellan, C. (2014). *Corruption and Firm Tax Evasion*. (Working Paper, 14-22). International Center for Public Policy.
- Alm, J., Liu, Y., & Zhang, K. (2019). Financial constraints and firm tax evasion. *International Tax and Public Finance*, 26(1), 71–102. doi:10.1007/10797-018-9502-7
- Alm, J., Martinez-Vazquez, J., & McClellan, C. (2016). Corruption and firm tax evasion. *Journal of Economic Behavior & Organization*, 124, 146–163. doi:10.1016/j.jebo.2015.10.006
- Alstadsæter, A., Kopczuk, W., & Telle, K. (2019). Social networks and tax avoidance: Evidence from a well-defined Norwegian tax shelter. *International Tax and Public Finance*, 26(6), 1291–1328. doi:10.1007/10797-019-09568-3
- Amake, C. C., & Ikhatua, O. J. (2016). Forensic accounting and fraud detection in Nigerian public sector. *Igbinedion University Journal of Accounting*, 2, 148–173.
- American Psychological Association. (2009). *APA concise dictionary of psychology*. American Psychological Association.
- AMInfo. (2014). Middle Eastern clients in the HSBC Switzerland leaks. *Swiss Leaks*. Retrieved from <http://ameinfo.com/luxury-lifestyle/list-middle-eastern-clients-in-the-hsbc-switzerland-leaks/>

## Compilation of References

- Amjad, M. M., Arshed, N., & Anwar, M. A. (2021). Money Laundering and Institutional Quality: The Case of Developing Countries. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Amoah, B. (2018). Mr Ponzi with Fraud Scheme Is Knocking: Investors Who May Open. *Global Business Review*, 19(5), 1115–1128. doi:10.1177/0972150918788625
- Amorim, J. C. (Ed.). (2010). *Planeamento e Evasão Fiscal - Jornadas de Contabilidade e Fiscalidade*. Vida Económica.
- Amundsen, I. (1999). *Political Corruption: An Introduction to the Issues* (WP 1999: 7). Bergen: Chr. Michelsen Institute. Retrieved from <https://open.cmi.no/cmi-xmlui/handle/11250/2435773>
- Anderson, S., Baland, J. M., & Moene, K. O. (2003). *Sustainability and organizational design in informal groups with some evidence from Kenyan Roscasm* (Working paper No. 2003, 17). Oslo: University of Oslo. Retrieved from <http://hdl.handle.net/10419/63174>
- Andreff, W. (2019). The unintended emergence of a greed-led economic system. *Kybernetes*, 48(2), 238–252. doi:10.1108/K-01-2018-0018
- Andrews, D. A., & Bonta, J. (1994). *The Psychology of Criminal Conduct*. Anderson.
- Andrews, D. M. (2006). Monetary Power and Monetary Statecraft. In D. M. Andrews (Ed.), *International Monetary Power* (pp. 7–28). Cornell University Press.
- Andrews, D. M. (Ed.). (2006). *International monetary power*. Cornell University Press.
- Annuar, H. A., Salihu, I. A., & Obid, S. N. S. (2014). Corporate ownership, governance and tax avoidance: An interactive effects. *Procedia: Social and Behavioral Sciences*, 164, 150–160. doi:10.1016/j.sbspro.2014.11.063
- Anokhin, S., & Schulze, W. S. (2009). Entrepreneurship, innovation, and corruption. *Journal of Business Venturing*, 24(5), 465–476. doi:10.1016/j.jbusvent.2008.06.001
- Anti-Corruption Act 2009
- Anzhu, A. A., & Pshenichnikov, V. V. (2017). Phenomenon of financial pyramids: Nature and design. *Advances in Economics. Business and Management Research*, 38, 13–19. doi:10.2991/ttiess-17.2017.3
- API Tech Servs., LLC v. Francis, 4: 13-cv-142-AWA-DEM (E.D. V.A., 2013).
- Apple. (2020). *Families*. Retrieved from <https://www.apple.com/ca/families/>
- Aracchande, V. (2010). *O impacto dos impostos diferidos nas demonstrações financeiras das empresas não financeiras incluídas no PSI 20: ano de 2009*. ISCAL. Retrieved from <http://hdl.handle.net/10400.21/3419>
- Archambault, J. J., & Archambault, M. E. (2003). A multinational test of determinants of corporate disclosure. *The International Journal of Accounting*, 38(2), 173–194. doi:10.1016/S0020-7063(03)00021-9
- Arif, I., & Rawat, A. S. (2018). Corruption, governance & tax revenue: Evidence from EAGLE countries. *Journal of Transnational Management*, 23(2), 119–133. doi:10.1080/15475778.2018.1469912
- Aris, B. (2011). *Russia: Where Ponzi schemes roam*. Financial Time. Retrieved from <https://www.ft.com/content/cd31ca25-cf99-3df7-bc0a-dcb73ea2bdb9>
- Arminfo. (2013). *Revived Russian Ponzi scheme, MMM, reaches Armenia*. <https://arminfo.info/index.cfm?objectid=34A68750-ED58-11E2-A1560EB7C0D21663>
- Arnett, G. W. (2011). *Global Securities Markets*. Wiley. doi:10.1002/9781118258385

- Asher, M. G. (n.d.). The design of tax systems and corruption. Public Policy Programme, National University of Singapore.
- Asiedu, E., & Freeman, J. (2009). The Effect of Corruption on Investment Growth: Evidence from Firms in Latin America, Sub-Saharan Africa, and Transition Countries. *Review of Development Economics*, 13(2), 200–214. doi:10.1111/j.1467-9361.2009.00507.x
- Asif, S. (2020, April 18). Fraud & hacking guides are the most sold item on the dark web. *Hack Read*. Retrieved from <https://www.hackread.com/fraud-hacking-guides-most-sold-item-dark-web/>
- Asokan, A. (2020, April 18). What's Hot on Dark Net Forums? 'Fraud Guides'. *Data Breach Today*. Retrieved from <https://www.databreachtoday.com/whats-hot-on-dark-net-forums-fraud-guides-a-14142>
- Assay, B. E. (2019). FinTech for Digital Financial Services: The African Case. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 61–80). IGI Global. doi:10.4018/978-1-5225-7805-5.ch004
- Asuquo, A. (2012). An empirical analysis of the impact of information technology on forensic accounting practice in Cross-River State Nigeria. *International Journal of Scientific & Technology Research*, 1(7), 25–33.
- Atila, G. (2008). *Corruption, taxation and economic growth: theory and evidence* (Working paper E 2008.29). CERDI.
- Atkins, P. S., & Bondi, B. J. (2008). Evaluating the mission: A critical review of the history and evolution of the SEC enforcement program. *Fordham Journal of Corporate and Financial Law*, 13(3), 367–418.
- ATO. (2019). *Black Economy*. Australian Taxation Office. Retrieved from <https://www.ato.gov.au/general/black-economy/>
- ATO. (2020). *Tax in Australia: What you Need to Know*. Australian Taxation Office. Australian Government Printer.
- Atuobi, S. M. (2007). *Corruption and State Instability in West Africa: An Examination of Policy Options* (KAIPTC Occasional Paper, December 2007). Accra: Kofi Annan International Peacekeeping Training Centre. Retrieved from <https://reliefweb.int/report/world/corruption-and-state-instability-west-africa-examination-policy-options>
- Atwood, T., & Lewellen, C. (2019). The complementarity between tax avoidance and manager diversion: Evidence from tax haven firms. *Contemporary Accounting Research*, 36(1), 259–294. doi:10.1111/1911-3846.12421
- Australian Law Reform Commission. (2014). *Serious Invasions of Privacy in the Digital Era* (Report No. 1). Retrieved from <https://apo.org.au/node/41124>
- Avi-Yonah, R. S. (2008). Corporate Social Responsibility and Strategic tax Behaviour. In P. D. W. Schoen (Ed.), *Tax and Corporate Governance* (pp. 183–198). Springer. doi:10.1007/978-3-540-77276-7\_13
- Avnimelech, G., & Zelekha, Y. (2015). The Impact of Corruption on Entrepreneurship. In R. Wolf & T. Issa (Eds.), *International Business Ethics and Growth Opportunities* (pp. 981–993). IGI Global. doi:10.4018/978-1-4666-7419-6.ch013
- Avnimelech, G., Zelekha, Y., & Sharabi, E. (2014). The effect of corruption on entrepreneurship in developed vs non-developed countries. *International Journal of Entrepreneurial Behaviour & Research*, 20(3), 237–262. doi:10.1108/IJEBR-10-2012-0121
- Ayyagari, M., Demirgüç-Kunt, A., & Maksimovic, V. (2010). *Are innovating firms victims or perpetrators? Tax evasion, bribe payments, and the role of external finance in developing countries* (World Bank Policy Research Working Paper No 5389). The World Bank.
- Ayyagari, M., Demirgüç-Kunt, A., & Maksimovic, V. (2014). Bribe payments and innovation in developing countries: Are innovating firms disproportionately affected? *Journal of Financial and Quantitative Analysis*, 49(1), 51–75. doi:10.1017/S002210901400026X

## Compilation of References

- Azim, M., & Azam, M. (2016). Bernard Madoff's "Ponzi scheme": Fraudulent behaviour and the role of auditors. *Accountancy Business and the Public Interest*, 15, 122–137.
- Azim, M., & Azam, S. (2016). Bernard Madoff's 'Ponzi Scheme': Fraudulent Behaviour and the Role of Auditors. *Accountancy Business and the Public Interest*, 15(1), 122–137.
- Azman, N. L. A., & Vaicondam, Y. (2020). Behavioral Intention in Forensic Accounting Services. *International Journal of Psychosocial Rehabilitation*, 24(2), 1837–1846. doi:10.37200/IJPR/V24I2/PR200485
- Azrina, M. Y. N., Ming, L. L., & Bee, W. Y. (2014). Tax non-compliance among SMCs in Malaysia: Tax audit evidence. *Journal of Applied Accounting Research*, 15(2), 215–234. doi:10.1108/JAAR-02-2013-0016
- Bacon, M. (2018). Social Engineering, TechTarget. *SearchSecurity*. Retrieved from <https://searchsecurity.techtarget.com/definition/social-engineering>
- Bainbridge, S. M. (2001). *The Law and Economics of Insider Trading: A Comprehensive Primer*. SSRN Electronic Journal. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=261277](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=261277) doi:10.2139/ssrn.261277
- Baird, B., Baird, L. L. Jr, & Ranauro, R. P. (1987). The Moral Cracker? *Computers & Security*, 6(6), 471–478. doi:10.1016/0167-4048(87)90028-9
- Bajada, C. (2017). *Australia's Cash Economy: A Troubling Issue for Policymakers: A Troubling Issue for Policymakers*. Routledge. doi:10.4324/9781315187372
- Baker, O. (n.d.). *What is Bitcoin and why does Ransomware love it?* Retrieved from <https://www.eurostaffgroup.com/media-hub/what-is-bitcoin-and-why-does-ransomware-love-it-85435/>
- Baker, P., Rogers, K., Enrich, D., & Haberman, M. (2020, April 6). Trump's aggressive advocacy of malaria drug for treating coronavirus divides medical community. *The New York Times*. Retrieved from <https://www.nytimes.com>
- Baker, H. K., Nofsinger, J. R., & Weaver, D. G. (2002). International cross-listing and visibility. *Journal of Financial and Quantitative Analysis*, 37(3), 495–521. doi:10.2307/3594990
- Balling, M., Lierman, F., & Mullineux, A. (2003). *Technology and Finance: Challenges for Financial Markets, Business Strategies and Policy Makers*. Routledge.
- Ball, R., Robin, A., & Wu, J. S. (2003). Incentives versus standards: Properties of accounting income in four East Asian countries. *Journal of Accounting and Economics*, 36(1-3), 235–270. doi:10.1016/j.jacceco.2003.10.003
- Banerjee, A. V. (1992). A simple model of herd behavior. *The Quarterly Journal of Economics*, 107(3), 797–817. doi:10.2307/2118364
- Banerjee, A. V., & Duflo, E. (2014). Do firms want to borrow more? Testing credit constraints using a directed lending program. *The Review of Economic Studies*, 81(2), 572–607. doi:10.1093/restud/rdt046
- Barberis, J., & Arner, D. W. (2016). FinTech in China: From Shadow Banking to P2P Lending. In *Banking Beyond Banks and Money*. New Economic Windows (pp. 69-96). Springer.
- Bardhan, I., Lin, S., & Wu, S. L. (2015). The quality of internal control over financial reporting in family firms. *Accounting Horizons*, 29(1), 41–60. doi:10.2308/acch-50935
- Barnes, T. D., Beaulieu, E., & Saxton, G. W. (2018). Restoring trust in the police: Why female officers reduce suspicions of corruption. *Governance: An International Journal of Policy, Administration and Institutions*, 31(1), 143–161. doi:10.1111/gove.12281



- Baron, R. M., & Kenny, D. A. (1986). Moderator Mediator Variables Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. *Journal of Personality and Social Psychology*, 51(6), 1173–1182. doi:10.1037/0022-3514.51.6.1173 PMID:3806354
- Bassey, E. B. (2018). Effect of forensic accounting on the management of fraud in microfinance institutions in Cross River State. *Journal of Economics and Finance*, 9(4), 79–8.
- Bates v City of Little Rock*, 361 US 516 (1960).
- Batra, G., Kaufmann, D., & Stone, A. H. (2003). *Investment climate around the world: Voices of the firms from the World Business Environment Survey*. The World Bank. doi:10.1596/0-8213-5390-X
- Bauhr, M., & Charron, N. (2020). Do men and women perceive corruption differently? Gender differences in perception of need and greed corruption. *Politics and Governance*, 8(2), 92–102. doi:10.17645/pag.v8i2.2701
- Baumann, F., & Friehe, T. (2016). Competitive pressure and corporate crime. *The B.E. Journal of Economic Analysis & Policy*, 16(2), 647–687. doi:10.1515/bejeap-2015-0064
- Baumol, W. J. (1990). Entrepreneurship: Productive, Unproductive, and Destructive. *Journal of Political Economy*, 98(5, Part 1), 893–921. doi:10.1086/261712
- Baumol, W. J. (1993). *Entrepreneurship, Management, and the Structure of Payoffs*. MIT Press.
- Bazart, C., Beaud, M., & Dubois, D. (2020). Whistleblowing vs. Random Audit: An Experimental Test of Relative Efficiency. *Kyklos*, 73(1), 47–67. doi:10.1111/kykl.12215
- BBC. (2016). *Ukraine Prime Minister Arseniy Yatsenyuk to resign*. BBC News. Retrieved from <https://www.bbc.com/news/world-europe-36010511>
- BBC. (2016, January 15). Migrant crisis: Switzerland defends asset seizure law. *BBC*. Retrieved from <https://www.bbc.com/news/world-europe-35323315>
- BBC. (2018, November 30). *Marriott hack hits 500 million Starwood guests*. Retrieved from <https://www.bbc.com/news/technology-46401890>
- BBC. (2020, March 30). Coronavirus: US senator probed for alleged insider trading – reports. *BBC News*. Retrieved from <https://www.bbc.com>
- Bebchuk, L., & Fried, J. (2009). *Pay without performance: The unfulfilled promise of executive compensation*. Harvard University Press.
- Becker, J. M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models. *Long Range Planning*, 45(5/6), 359–394. doi:10.1016/j.lrp.2012.10.001
- Beck, T., Lin, C., & Ma, Y. (2014). Why do firms evade taxes? The role of information sharing and financial sector outreach. *The Journal of Finance*, 69(2), 763–817. doi:10.1111/jofi.12123
- Beeres, R., Bertrand, R., & Bollen, M. (2017). Profiling Terrorists—Using Statistics to Fight Terrorism. In P. A. Ducheine & F. P. Osinga (Eds.), *Netherlands Annual Review of Military Studies 2017: Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises* (pp. 221–235). TMC Asser Press. doi:10.1007/978-94-6265-189-0\_12
- Beeres, R., & Bollen, M. (2011). The global financial War on Terror: Analyses en cijfers. In F. P. Osinga, J. M. L. M. Soeters, & W. vanRossum (Eds.), *Nine eleven: Tien jaar later* (pp. 92–106). Boom.

## Compilation of References

- Beeres, R., & Bollen, M. (2015). Exciting Dilemma: A Defence Economics View on a US Exit from NATO. In J. Noll, D. van den Wollenberg, F. Osinga, G. Frerks, & I. van Kemenade (Eds.), *Netherlands Annual Review of Military Studies 2015: The Dilemma of Leaving: Political and Military Exit Strategies* (pp. 271–297). TMC Asser Press. doi:10.1007/978-94-6265-078-7\_11
- Beg, M. O., Awan, M. N., & Ali, S. S. (2019). Algorithmic Machine Learning for Prediction of Stock Prices. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 142–169). IGI Global. doi:10.4018/978-1-5225-7805-5.ch007
- Behrman, J. R., Mitchell, O. S., Soo, C. K., & Bravo, D. (2012). How financial literacy affects household wealth accumulation. *The American Economic Review*, 102(3), 300–304. doi:10.1257/aer.102.3.300 PMID:23355747
- Belfort, J. (2011). *The wolf of wall street*. Hachette.
- Bell, A. (2019, January 22). *How Cybercriminals Clean Their Dirty Money*. Retrieved from <https://www.darkreading.com/attacks-breaches/how-cybercriminals-clean-their-dirty-money-/a/d-id/1333670>
- Bello, W. (2010). *Is Corruption the Cause? The Poverty Trap*. TNI.org. Retrieved from <https://www.tni.org/es/node/10907>
- Bell, S. (2008). *Encyclopedia of Forensic Science* (Revised Ed.). Facts on File Inc.
- Benczúr, P., Kátay, G., & Kiss, Á. (2018). Assessing the economic and social impact of tax and benefit reforms: A general-equilibrium microsimulation approach applied to Hungary. *Economic Modelling*, 75, 441–457. doi:10.1016/j.econmod.2018.06.016
- Ben-Hassine, W., Sayadi, E., & Samaro, D. (2018, September 12). *When “Cybercrime” Laws Gag Free Expression: Stopping the Dangerous Trend Across MENA*. Retrieved from <https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/>
- Bennett Moses, L. (2013). How to Think about Law, Regulation and Technology: Problems with “Technology” as a Regulatory Target. *Law, Innovation and Technology*, 5(1), 12.
- Benson, M. L., & Simpson, S. S. (2014). *Understanding white-collar crime: An opportunity perspective*. Routledge. doi:10.4324/9780203762363
- Bentley, D. (2019). Timeless principles of taxpayer protection: how they adapt to digital disruption. *eJournal of Tax Research*, 16(3), 679–713.
- Berksoy, T., & Yıldırım, N. E. (2017). Yolsuzluk kavramına genel bir bakış: Problemler ve çözüm önerileri [An overview of the concept of corruption: Problems and solutions]. *Journal of Awareness*, 2(1), 1–18.
- Besley, T., Jensen, A., & Persson, T. (2019). Norms, enforcement, and tax evasion (No. w25575). National Bureau of Economic Research.
- Besley, T., Coate, S., & Loury, G. (1993). The Economics of Rotating Savings and Credit Associations. *The American Economic Review*, 83(4), 792–810.
- Besley, T., & Persson, T. (2014). Why do developing countries tax so little? *The Journal of Economic Perspectives*, 28(4), 99–120. doi:10.1257/jep.28.4.99
- Beyes, P., & Bhattacharya, R. (2017, March). *India’s 2016 demonetisation drive: A case study on innovation in anti-corruption policies, government communications and political integrity*. Paper presented at OECD Global Anti-Corruption & Integrity Forum, Paris, France.

- Bhargava, V. (2005). *The cancer of corruption*. World Bank Global Issues Seminar Series. Retrieved from <http://sitere-sources.worldbank.org/EXTABOUTUS/Resources/Corruption.pdf>
- Bhasin, M. (2007, January). Forensic accounting: A new paradigm for niche consulting. *The Chartered Accountant*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2703647](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2703647)
- Bhasin, M. L. (2016). Forensic Accounting in Asia: Perspectives and Prospects. *International Journal of Management and Social Sciences Research*, 5(7), 25–38.
- Bhattacharjee, D. (2016). Problems and Prospects of Network Marketing in Assam (India). *International Journal of Business and Management Studies*, 5(2), 167–182.
- Bhattacharya, U. (2003). The optimal design of Ponzi schemes in finite economies. *Journal of Financial Intermediation*, 12(1), 2–24. doi:10.1016/S1042-9573(02)00007-4
- Bholat, D., & Atz, U. (2016). *Peer-to-Peer lending and Financial Innovation in the United Kingdom* (Working paper No. 598). Bank of England. Retrieved from <https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/peer-to-peer-lending-and-financial-innovation-in-the-uk.pdf?la=en&hash=731A6951C1EEFF82BEBE281516E464139D996743>
- Bierstaker, J. L., Brody, R., & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, 21(5), 520–535. doi:10.1108/02686900610667283
- Birincioğlu, İ. (2005). *Adli Belge İncelemesinin Tarihçesi, Yazının Anatomisi - Nöro- Fizyolojisi*. İstanbul: Adli Belge İncelemesi Ed. Faruk Aşçıoğlu, Beta Yay.
- Black's Law Dictionary. (2019). *Cybercrime* (11th Ed.). Toronto: West (Thompson Reuters).
- Blackburn, K., Bose, N., & Capasso, S. (2012). Tax evasion, the underground economy and financial development. *Journal of Economic Behavior & Organization*, 83(2), 243–253. doi:10.1016/j.jebo.2012.05.019
- Bloomberg. (2015). *Coca-Cola Fights \$9.4 Billion Transfer Pricing Adjustment*. Retrieved April 11, 2016, from <http://www.bna.com/cocacola-fights-94-n57982065115/>
- Bogers, M., & Beeres, R. (2011). Burden sharing in combating terrorist financing. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, 7(12), 2992–2998.
- Bollen, J., Mao, H., & Zeng, X. (2011). Twitter mood predicts the stock market. *Journal of Computational Science*, 2(1), 1–8. doi:10.1016/j.jocs.2010.12.007
- Bolton, R. J., Hand, D. J., Provost, F., Breiman, L., Bolton, R. J., & Hand, D. J. (2002). Statistical Fraud Detection: A Review. *Statistical Science*, 17(3), 235–255. doi:10.1214/s/1042727940
- Bonny, P., Goode, S., & Lacey, D. (2015). Revisiting employee fraud: Gender, investigation outcomes and offender motivation. *Journal of Financial Crime*, 22(4), 447–467. doi:10.1108/JFC-04-2014-0018
- Bornemann, T., Jacob, M., & Sailer, M. (2019). *Do Corporate Taxes Affect Executive Compensation?* Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3403486](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3403486)
- Borrego, A. C., & Lopes, C. M. da M. (2013). Tax Noncompliance in an International Perspective: a Literature Review. *Contabilidade E Gestão*, (14), 9–43
- Bosley, S., & Knorr, M. (2018). Pyramids, Ponzis and fraud prevention: Lessons from a case study. *Journal of Financial Crime*, 25(1), 81–94. doi:10.1108/JFC-10-2016-0062

## Compilation of References

- Botrić, V., & Božić, L. (2016). Innovators' vs Non-innovators' perceptions of corruption in European post-transition economies. *International Journal of Business and Economic Sciences Applied Research*, 8(3), 47–58.
- Boyle, D. M., Boyle, J. F., & Mahoney, D. P. (2015). Avoiding the fraud mind-set. *Strategic Finance*, 96(8), 41–47.
- Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, 34(6), 578–596. doi:10.1016/j.jaccpubpol.2015.05.006
- Boys, J. (2008). Forensic Accounting in New Zealand: Exploring the Gap Between Education and Practice. *AFAANZ Conference*.
- Bracken, P. (2007). Financial warfare. *Orbis*, 51(4), 685–696. doi:10.1016/j.orbis.2007.08.010
- Bradley, R. (2020). Blockchain explained... in under 100 words. *Deloitte*. Retrieved from: <https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/blockchain-explained.html#>
- Bragg, S. M., Epstein, B. J., & Nach, R. (2009). Income Taxes. In *Wiley GAAP 2010. Interpretation and Application of Generally Accepted Accounting Principles* (pp. 875–952). John Wiley & Sons, Inc.
- Braithwaite, J. (2002). Rules and Principles: A Theory of Legal Certainty. *Australian Journal of Legal Philosophy*, 27, 47–82. doi:10.2139/ssrn.329400
- Braithwaite, J. (2005). *Markets in Vice, Markets in Virtue*. Federation Press.
- Braithwaite, J. (2013). Flipping markets to virtue with qui tam and restorative justice. *Accounting, Organizations and Society*, 38(6-7), 465. doi:10.1016/j.aos.2012.07.002
- Braithwaite, J. (2018). Minimally Sufficient Deterrence. In M. Tonry (Ed.), *Crime and Justice: A Review of Research*. University of Chicago Press.
- Braithwaite, J., & Hong, S. H. (2015). The iteration deficit in responsive regulation: Are regulatory ambassadors an answer? *Regulation & Governance*, 9(1), 16–29. doi:10.1111/rego.12049
- Braithwaite, V. (2002). *Taxing Democracy*. Ashgate.
- Braithwaite, V., Murphy, K., & Reinhart, M. (2007). Taxation threat, motivational postures, and responsive regulation. *Law & Policy*, 29(1), 137–158. doi:10.1111/j.1467-9930.2007.00250.x
- Braithwaite, V., Reinhart, M., & Job, J. (2018). Getting on or getting by? Australians in the cash economy. In C. Bajada & F. Schneider (Eds.), *Size, Causes and Consequences of the Underground Economy* (pp. 55–69). Routledge. doi:10.4324/9781351149044-4
- Branigan, S. (2004). *High-Tech Crimes Revealed: Cyberwar Stories from the Digital Front*. Addison-Wesley.
- Branisa, B., & Ziegler, M. (2010). *Reexamining the link between gender and corruption: The role of social institutions* (No. 24). Courant Research Centre: Poverty, Equity and Growth-Discussion Papers.
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. doi:10.1191/1478088706qp063oa
- Breen, R. E. H., Tasker, S. L., & Hiebert, B. (2017). How self-employed women with children manage multiple life roles. *Canadian Journal of Counselling and Psychotherapy*, 51(3), 187–206.
- Brennan, M., & Kraus, A. (1987). Efficient Financing Under Asymmetric Information. *The Journal of Finance*, 42(5), 1225–1243. doi:10.1111/j.1540-6261.1987.tb04363.x

- Brenner, S. (2004). US Cybercrime Law: Defining Offences. *Information Systems Frontiers*, 6(2), 115–132. doi:10.1023/B:ISFI.0000025780.94350.79
- Brenner, S., & Koops, B.-J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*, 4, 2–46.
- Bressler, L. (2012). The role of forensic accountants in fraud investigations: Importance of Attorney and Judge's perceptions. *Journal of Finance and Accountancy*, 9, 1–9.
- Breusch, T. S., & Pagan, A. R. (1980). The Lagrange multiplier test and its applications to model specification in econometrics. *The Review of Economic Studies*, 47(1), 239–253. doi:10.2307/2297111
- Bridi, A. (2010). *Corruption in tax administration* (U4 Expert Answer No. 229). Transparency International. Retrieved from <https://www.u4.no/publications/corruption-in-tax-administration.pdf>
- Brito, J. (2014). Agency Threats and the Rule of the Law: An Offer You Can't Refuse. *Harvard Journal of Law & Public Policy*, 37, 553–577.
- Britz, M. (2013). *Computer Forensics and Cyber Crime: An Introduction*. Pearson Education Inc.
- Brondolo, J., Bosch, F., Borgne, E. L., & Silvani, C. (2008). *Tax Administration reform and fiscal adjustment: The case of Indonesia (2001-07)* (Working Paper No: WP/08/129). International Monetary Fund.
- Bronitt, S., & Donkin, S. (2012). Australian Responses to 9/11: New World Legal Hybrids? In A. Masferrer (Ed.), *Post 9/11 and the State of Permanent Legal Emergency* (pp. 223–239). Springer. doi:10.1007/978-94-007-4062-4\_10
- Brown, J. (2016). Wafic Said: businessman, philanthropist and political fixer. *Financial Times*. Retrieved from <https://www.ft.com/content/a3cb764a-ecf1-11e5-bb79-2303682345c8>
- Brown, D. B. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal: Theory, Practice and Principles*, 89(4), 327–339. doi:10.1177/0032258X16658927
- Brown, J. O., Hays, J., & Stuebs, M. T. Jr. (2016). Modeling accountant whistleblowing intentions: Applying the theory of planned behavior and the fraud triangle. *Accounting and the Public Interest*, 16(1), 28–56. doi:10.2308/apin-51675
- Brownsword, R. (2018). Law and technology: Two modes of disruption, three legal mind-sets, and the big picture of regulatory responsibilities. *Indian Journal of Law and Technology*, 14, 1–40.
- Brownsword, R. (2019). *Law, Technology, and Society – Re-imagining the Regulatory Environment*. Routledge. doi:10.4324/9781351128186
- Brunetti, A., & Weder, B. (1998). Investment and Institutional Uncertainty: A Comparative Study of Different Uncertainty Measures. *Weltwirtschaftliches Archiv*, 134(3), 513–533. doi:10.1007/BF02707928
- Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal (Indianapolis, Ind.)*, 441–472.
- Brzoska, M. (2016). Consequences of assessments of effectiveness for counterterrorist financing policy. *Administration & Society*, 48(8), 911–930. doi:10.1177/0095399714532272
- Buchanan, D., & Badham, R. (2020). *Power, Politics, and Organizational Change*. SAGE.
- Buckley, R., Arner, D., & Barberis, J. (2016). The Evolution of Fintech: A New Post-Crisis Paradigm? *Georgetown Journal of International Law*, 47, 1271–1319. doi:10.2139/ssrn.2676553

## Compilation of References

- Buckstein, J. (2012). Forensic accounting: Far from a recent phenomenon Professional Development network. *Professional Development Network*. Retrieved from <https://docplayer.net/4231616-Forensic-accounting-part-1-far-from-a-recent-phenomenon.html>
- Buono, L. (2016). Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches. *ERA Forum*, 17(3), 343–353.
- Burg, D. (2004). *A World History of Tax Rebellions*. Taylor & Francis. doi:10.4324/9780203500897
- Bush, G. W. (2001, September 24). *President Freezes Terrorists' Assets*. The White House. Retrieved from <https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010924-4.html>
- Business Crimes. (2013). *Computer Fraud and Abuse Act 18 USC Sec. 1030*. Matthew Bender & Co.
- Bussmann, K. D., & Werle, M. M. (2006). Addressing Crime in Companies: First Findings from a Global Survey of Economic Crime I. *British Journal of Criminology*, 46(6), 1128–1144. doi:10.1093/bjc/azl072
- Buttle, F. A. (1998). Word of mouth: Understanding and managing referral marketing. *Journal of Strategic Marketing*, 6(3), 241–254. doi:10.1080/096525498346658
- Byrnes, J. P., Miller, D. C., & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. *Psychological Bulletin*, 125(3), 367–383. doi:10.1037/0033-2909.125.3.367
- CAANZ. (2017). *Submission to the Black Economy Taskforce*. Chartered Accountants Australia and New Zealand. Retrieved from <https://www.charteredaccountantsanz.com/-/media/b28ef2c51a1d42daaf9517d689d8e6a5.ashx>
- CAFC. (2020). *Canadian Anti-Fraud Centre*. Retrieved from <https://www.antifraudcentre-centreantifraude.ca/>
- Cairns, G., & Wright, G. (2018). Advanced methods in scenario development: Uncovering causality and using the Delphi method. In *Scenario thinking* (pp. 141–154). Springer. doi:10.1007/978-3-319-49067-0\_7
- Calomiris, C. W., & Rajaraman, I. (1998). The role of ROSCAs: Lumpy durables or event insurance? *Journal of Development Economics*, 56(1), 207–216. doi:10.1016/S0304-3878(98)00059-5
- Cambell, L. (2007). Theorising asset forfeiture in Ireland. *The Journal of Criminal Law*, 75(11), 441 – 460.
- Campbell, T. (2016). *Practical Information Security Management: A Complete Guide to Planning and Implementation*. Apress. doi:10.1007/978-1-4842-1685-9
- Capasso, S., & Santoro, L. (2016). *The determinants of the contract of corruption: Theory and Evidence* (Working Paper No. 429). Naples: Centre For Studies in Economics and Finance.
- Capital One. (2019, September 23). *Information on the Capital One Cyber Incident*. Capital One. Retrieved from <https://www.capitalone.com/facts2019>
- Careerride. (2015). *Poverty causes corruption*. Retrieved from <https://www.careerride.com/view/poverty-causes-corruption-26204.aspx>
- Carraro, A., Ribeiro, F. G., Costa, G. W., Menezes, G. R., Canever, M. D., & Fernandez, R. N. (2016). Does governmental corruption affect entrepreneurship in Brazil? *Ensaio FEE*, 37(3), 615–642.
- Carrillo, P., Pomeranz, D., & Singhal, M. (2017). Dodging the taxman: Firm misreporting and limits to tax enforcement. *American Economic Journal. Applied Economics*, 9(2), 144–164. doi:10.1257/app.20140495
- Carter, A., & Perry, A. (2004). Computer Crime. *The American Criminal Law Review*, 41, 313–365.

- Carvalho, C. (2010). A “Solidariedade Social” na Tributação: Realização da Justiça ou Ineficiência Económica? *Revista de Finanças Públicas E Direito Fiscal*, 3(2), 79–103
- Casey, A. J., & Niblett, A. (2016). The death of rules and standards. *Indiana Law Journal (Indianapolis, Ind.)*, 92, 1401.
- Casey, E., & Rose, C. W. (2003). Forensic Analysis. In E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology* (2nd ed.). Academic Press.
- Casey, E., & Seglem, K. (2003). Introduction. In E. Casey (Ed.), *Handbook of Computer Crime Investigation: Forensic Tools and Technology* (2nd ed.). Academic Press. doi:10.4324/9780203359105-6
- Castro, P. A. L., & Teodoro, A. R. (2019). A Method to identify anomalies in stock market trading based on Probabilistic Machine Learning. *Journal of Autonomous Intelligence*, 2(2), 42–52. doi:10.32629/jai.v2i2.44
- Catarino, J. R., & Monteiro, M. B. (2013). Fiscalidade ambiental - Um estudo sobre a relevância das provisões ambientais nas empresas do PSI 20. *Revista de Finanças Públicas E Direito Fiscal*, 6(3), 153–176.
- CaytasJ. (2017). *Regulatory Issues and Challenges Presented by Virtual Currencies*. Retrieved from <https://ssrn.com/abstract=2988367>
- CBC. (2020a, July 16). FBI probing high-profile Twitter hack that experts say undermines trust in the platform. *CBC News*. Retrieved from <https://www.CBC.ca/news/technology/twitter-breach-hack-1.5651675>
- CBC. (2020b, July 31). 3 charged in high-profile Twitter hack targeting Barack Obama, Bill Gates, others. *CBC News*. Retrieved from [https://www.CBC.ca/amp/1.5670061?\\_\\_twitter\\_\\_impression=true](https://www.CBC.ca/amp/1.5670061?__twitter__impression=true).
- CDPP. (2019). *Australian jailed for her role in international romance scam*. Retrieved from <https://www.cdpp.gov.au/case-reports/australian-jailed-her-role-international-romance-scam>
- Cendrowski, H., Martin, J., & Petro, L. W. (2007). *The Handbook of Fraud Deterrence*. John Wiley & Sons.
- CESR. (2020). *Market abuse. European Securities and Markets Authority*. Retrieved from <https://www.esma.europa.eu/sections/market-abuse>
- CEU. (2004). *Legal barriers in e-business: the results of an open consultation of enterprises* (Working Paper SEC (2004) 498). Brussels: Commission of the European Communities, Council of the European Union. Retrieved from <https://data.consilium.europa.eu/doc/document/ST-8997-2004-INIT/en/pdf>
- CFA. (2014). Retrieved from <https://www.cfainstitute.org>
- CFI. (2020). *Front Running*. Corporate Finance Institution. Retrieved from <https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/front-running/>
- Chandrasekhar, A. (2018). Trial of LTTE Financiers Begins in Switzerland. *The Wire*. Retrieved from <https://thewire.in/external-affairs/trial-of-ltte-financiers-begins-in-switzerland>
- Chang, Y., Lakovou, E., & Shi, W. (2020). Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities. *International Journal of Production Research*, 58(7), 2082–2099. doi:10.1080/00207543.2019.1651946
- Chariri, A. (2009). The relevance of forensic accounting in detecting financial fraud. *Bankers' Magazine*.
- Chen, G., Kim, K. A., Nofsinger, J. R., & Rui, O. M. (2007). Trading performance, disposition effect, overconfidence, representativeness bias, and experience of emerging market investors. *Journal of Behavioral Decision Making*, 20(4), 425–451. doi:10.1002/bdm.561

## Compilation of References

- Chen, W., Zheng, Z., Ngai, E. C. H., Zheng, P., & Zhou, Y. (2019). Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum. *IEEE Access: Practical Innovations, Open Solutions*, 7, 37575–37586. doi:10.1109/ACCESS.2019.2905769
- Chen, Y., Ge, R., Louis, H., & Zolotoy, L. (2019). Stock liquidity and corporate tax avoidance. *Review of Accounting Studies*, 24(1), 309–340. doi:10.1007/11142-018-9479-6
- Chertoff, M., & Simon, T. (2015, February). *The Impact of the Dark Web on Internet Governance and Cyber Security* (Paper Series: No. 6). The Centre for International Governance Innovation and Chatham House. Retrieved from: [https://www.cigionline.org/sites/default/files/gcig\\_paper\\_no6.pdf](https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf)
- Chetwynd, E., Chetwynd, F., & Spector, B. (2003). Corruption and poverty: A review of recent literature. *Management Systems International*, 600, 5–16.
- Chiarini, B., & Marzano, E. (2016). *Is the Severity of the Penalty an Effective Deterrent? A Strategic Approach for the Crime of Tax Evasion* (CESifo Working Paper No. 6112). Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2867304](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2867304)
- Chin, W. W., Thatcher, J. B., Wright, R. T., & Steel, D. (2013). *Controlling for common method variance in PLS analysis: The measured latent marker variable approach*. Springer.
- Christensen, J., & Murphy, R. (2004). The Social Irresponsibility of Corporate Tax Avoidance: Taking CSR to the bottom line. *Development*, 47(3), 37–44. doi:10.1057/palgrave.development.1100066
- Christian, N., Basri, Y. Z., & Arafah, W. (2019). Analysis of fraud triangle, fraud diamond and fraud pentagon theory to detecting corporate fraud in Indonesia. *International Journal of Business Management and Technology*, 3(4), 73–78.
- Chukwunedu, O. S., & Okoye, E. I. (2011). Forensic Accounting and Audit Expectation Gap – The Perception of Accounting Academics. *SSRN Working Papers*. doi:10.2139/ssrn.1920865
- Clarke, Th., & Tigue, J. (1975). *Dirty money: Swiss banks, the Mafia, money laundering, and white-collar crime*. Simon and Schuster.
- Clark, F., & Diliberto, K. (1996). *Investigating Computer Crime*. CRC Press. doi:10.1201/9781420048896
- Clor-Proell, S. M., Kaplan, S. E., & Proell, C. A. (2015). The impact of budget goal difficulty and promotion availability on employee fraud. *Journal of Business Ethics*, 131(4), 773–790. doi:10.1007/10551-013-2021-7
- Coenen, T. L. (2005, November 30). Forensic Accounting: A New Twist on the Bean Counting. *Wisconsin Law Journal*. Retrieved from <https://wislawjournal.com/2005/11/30/forensic-accounting-a-new-twist-on-bean-counting/>
- Coffin, B. (2017). A brief history of the SEC. *Compliance Week*, 14(157). Retrieved from [https://go-gale-com.wne.idm.oclc.org/ps/i.do?v=2.1&u=mclin\\_w\\_westnew&it=r&id=GALE%7CA535100987&p=GPS&sw=w](https://go-gale-com.wne.idm.oclc.org/ps/i.do?v=2.1&u=mclin_w_westnew&it=r&id=GALE%7CA535100987&p=GPS&sw=w)
- Cohen, B. J. (2000). Money and power in world politics. In *Strange Power: Shaping the Parameters of International Relations and International Political Economy* (pp. 91-113). London: Routledge.
- Cohen, D. A., & Gatta, J. D. (2020, January 19). Recent developments in charges of insider trading. *Harvard Law School Forum on Corporate Governance*. Retrieved from <https://corpgov.law.harvard.edu/2020/01/19/recent-developments-in-charges-of-insider-trading/>
- Cohen, B. J. (2018). *Currency power: Understanding monetary rivalry*. Princeton University Press.
- Cohen, J., Ding, Y., Lesage, C., & Stollowy, H. (2010). Corporate Fraud and Managers' Behavior: Evidence from the Press. *Journal of Business Ethics*, 95(2), 271–315. doi:10.1007/10551-011-0857-2



- Cohn, S. (2018, December 11). 10 years later, here's what became of Bernie Madoff's inner circle. *CNBC*. Retrieved from <https://www.cnbc.com>
- Coinbase. (2020). *What is Bitcoin?* Retrieved from: <https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin>
- Coindesk. (2020). *Dogecoin*. Retrieved from: <https://www.coindesk.com/crypto/dogecoin>
- Cojocaru, L., Falaris, E. M., Hoffman, S. D., & Miller, J. B. (2016). Financial System Development and Economic Growth in Transition Economies: New Empirical Evidence from the CEE and CIS Countries. *Emerging Markets Finance & Trade*, 52(1), 223–236. doi:10.1080/1540496X.2015.1013828
- Colbert, J. L., & Turner, B. S. (2000). Strategies for Dealing with Fraud. *The Journal of Corporate Accounting*, 11(4), 43–49. doi:10.1002/1097-0053(200005/06)11:4<43::AID-JCAF7>3.0.CO;2-Z
- Coleman, J. W. (1987). Toward an integrated theory of white-collar crime. *American Journal of Sociology*, 93(2), 406–439. doi:10.1086/228750
- Coleman, J. W. (1992). Crime and money: Motivation and opportunity in a monetarized economy. *The American Behavioral Scientist*, 35(6), 827–836. doi:10.1177/0002764292035006017
- Coleman, J. W. (2001). The causes of white-collar crime and the validity of explanation in the social sciences. In S.-A. Lindgren (Ed.), *White-collar Crime Research: Old Views and Future Potentials*. National Council for Crime Prevention.
- Comerton-Forde, C., & Putniņš, T. J. (2011). Measuring closing price manipulation. *Journal of Financial Intermediation*, 20(2), 135–158. doi:10.1016/j.jfi.2010.03.003
- Commission of the European Communities. (2001). *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*. Commission of the European Communities. Retrieved from [https://itlaw.wikia.org/wiki/Creating\\_a\\_Safer\\_Information\\_Society\\_by\\_Improving\\_the\\_Security\\_of\\_Information\\_Infrastructures\\_and\\_Combating\\_Computer-related\\_Crime](https://itlaw.wikia.org/wiki/Creating_a_Safer_Information_Society_by_Improving_the_Security_of_Information_Infrastructures_and_Combating_Computer-related_Crime)
- Commonwealth. (2017). *Black Economy Taskforce: Final Report*. Australian Government Printer.
- Computer Fraud and Abuse Act of 1986, Pub. L. 99-474 (1986). Retrieved from <https://www.congress.gov/bill/99th-congress/house-bill/4718>
- Conrad, N. P., & Wahsheh, L. A. (2020). Simon Says: “Send Money.” *Journal of Systemics, Cybernetics and Informatics*, 18(3), 54-55. Retrieved from <http://www.iiisci.org/journal/sci/FullText.asp?var=&id=ZA380TJ20>
- Coppola, D. R. (2006). Demystifying financial fraud: Forensic accountants gain in popularity. *Alaska Business Monthly*, 22(5), 79.
- Cornevin, Ch. (2020). La police démantèle un vaste système de blanchiment de fraude fiscale... [Police dismantles massive tax fraud laundering scheme]. *Le Figaro*. Retrieved from <https://www.lefigaro.fr/actualite-france/la-police-demantele-un-vaste-systeme-de-blanchiment-de-fraude-fiscale-20200110>
- Corruption Perceptions Index. (2019). Retrieved from <https://www.transparency.org/en/cpi/2019/results/table>
- Cox, J. (2019 October 8). Twitter Took Phone Numbers for Security and Used Them for Advertising. *Vice*. Retrieved from: <https://www.vice.com/en/article/9kez8d/twitter-took-phone-numbers-for-security-used-for-advertising>
- CRA. (2017). *Tax Assured and Tax Gap for the Federal Personal Income Tax System*. Canada Revenue Agency.
- Crane, S. E., & Nourzad, F. (1986). Inflation and tax evasion: An empirical analysis. *The Review of Economics and Statistics*, 68(2), 217–223. doi:10.2307/1925500

## Compilation of References

- Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review. Boston College. Law School*, 55, 93.
- Crespo, R. A. (2018). Currency warfare and cyber warfare: The emerging currency battlefield of the 21st century. *Comparative Strategy*, 37(3), 235–250. doi:10.1080/01495933.2018.1486090
- Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review*, 15(6), 738–743. doi:10.2307/2086606
- Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Free Press.
- Cressey, D. R. (1953). *Other People's Money: The social psychology of embezzlement*. The Free Press.
- Cressey, D. R. (1953). *Other people's money; a study of the social psychology of embezzlement*. Free Press.
- Croall, H. (2001). *Understanding White Collar Crime*. Open University Press.
- Croall, H. (2010). Middle-Range Business Crime: Rogue and Respectable Businesses, Family Forms and Entrepreneurs. In F. Brookman, M. Maguire, H. Pierpoint, & T. Bennett (Eds.), *Handbook on crime*. Willan Publishing.
- Crocker, K. J., & Slemrod, J. (2005). Corporate tax evasion with agency costs. *Journal of Public Economics*, 89(9-10), 1593–1610. doi:10.1016/j.jpubeco.2004.08.003
- Crown. (2012). *The Wheatley Review of LIBOR. UK Treasury Publications*. Retrieved from <https://assets.publishing.service.gov.uk/>
- Crumbley, D. L., & Apostolou, N. G. (2002). Forensic Accounting: A New Growth Area in Accounting. *The Ohio CPA Journal*, 61(3), 16–20.
- Crumbley, L. (2001). Forensic Accounting: Older Than You Think. *Journal of Forensic Accounting*, 2(2), 181–202.
- D'Amato, G. (1995). Switzerland: A Multicultural Country without Multicultural Policies? In S. Vertovec & S. Wessendorf (Eds.), *The Multiculturalism Backlash: European Discourses, Policies and Practices*. Routledge.
- D'ath, J. (2008). Forensic Accounting Is Here to Stay. *Chartered Accountants Journal*, 87(3), 12–14.
- da Silva, M. D. C. (2013). *A problemática dos impostos diferidos: grau de harmonização, nível de divulgação e seus determinantes*. Escola Superior de Gestão e Tecnologia de Santarém. Retrieved from [https://repositorio.ipsantarem.pt/bitstream/10400.15/876/6/MarisaSilva\\_MestradoCF\\_2013.pdf](https://repositorio.ipsantarem.pt/bitstream/10400.15/876/6/MarisaSilva_MestradoCF_2013.pdf)
- Dada, S. O. (2014). Forensic accounting techniques: A means of successful eradication of corruption through fraud prevention, bribery prevention and embezzlement prevention in Nigeria. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 4(1), 176–186. doi:10.12816/0018900
- Daellenbach, H., McNickle, D., & Dye, Sh. (2012). *Management Science - Decision-making through systems thinking*. Palgrave Macmillan.
- Dai, Z., Galeotti, F., & Villeval, M. C. (2017). Cheating in the lab predicts fraud in the field: An experiment in public transportation. *Management Science*, 64(3), 1081–1100. doi:10.1287/mnsc.2016.2616
- Daly, K. (1989). Gender and varieties of white-collar crime. *Criminology*, 27(4), 769–794. doi:10.1111/j.1745-9125.1989.tb01054.x
- Dark Reading Staff. (2020). FBI Warns on New E-Commerce Fraud. *Dark Reading*. Retrieved from <https://www.dark-reading.com/attacks-breaches/fbi-warns-on-new-e-commerce-fraud/d/d-id/1338534>

- David, R., & David, P. (1996). Law and Borders -The Rise of Law in Cyberspace. *Stanford Law Review*, 48(5), 1367. doi:10.2307/1229390
- Davis, K. T., & Murphy, J. (2016). Peer to Peer lending: structures, risks and regulation. *JASSA: The Finsia Journal of Applied Finance*, 2016, 3–37.
- Dawson, M., Eltayeb, M., & Omar, M. (Eds.). (2016). *Security Solutions for Hyperconnectivity and the Internet of Things*. IGI Global. doi:10.4018/978-1-5225-0741-3
- Dawson, M., & Omar, M. (2015). *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. IGI Global. doi:10.4018/978-1-4666-8345-7
- de Carvalho, F. P. M. (2008). *A divulgação voluntária de informação: A influência da adopção da estrutura da Global Reporting Initiative nas empresas da Euronext Lisboa*. Universidade Autónoma de Lisboa.
- De Groot, H. L., Linders, G. J., & Rietveld, P. (2003). *Why do OECD-countries trade more?* (No. 03-092/3). Tinbergen Institute Discussion Paper.
- De Koker, L. (2012). *Pyramids and Ponzis: Financial Scams in Developing Countries*. CGAP. Retrieved from <https://www.cgap.org/blog/pyramids-and-ponzis-financial-scams-developing-countries>
- de Laubadere, A., Venezia, J. C., & Gandement, Y. (1991). *Traité de droit administratif [Treaty of Administrative law]*. *International Comparative Law Review*, 43(4), 941.
- De Maria, F., Franco, C., & Solferino, N. (2015). *Corruption and innovation: the mediating role of trade* (Working Paper No. 139-2015). Associazione Italiana per la Cultura della Cooperazione e del Non-Profit.
- De Waldemar, F. S. (2012). New Products and Corruption: Evidence from Indian Firms: New Products and Corruption. *The Developing Economies*, 50(3), 268–284. doi:10.1111/j.1746-1049.2012.00171.x
- De Wijk, R. (2014). *The Art of Military Coercion: Why the West's Military Superiority Scarcely Matters*. Amsterdam University Press.
- de Zwart, M., Humphreys, S., & Van Dissel, B. (2014). Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK. *The University of New South Wales Law Journal*, 37(2), 713.
- Deb, R. (2018). Financial audit or forensic audit? Government sector panorama. *Indian Journal of Corporate Governance*, 11(2), 135–158.
- Debski, J., Jetter, M., Mösele, S., & Stadelmann, D. (2018). Gender and corruption: The neglected role of culture. *European Journal of Political Economy*, 55, 526–537. doi:10.1016/j.ejpoleco.2018.05.002
- Dee, C. C., & Durtschi, C. (2010). Return of the Tallahassee BeanCounters: A Case in Forensic Accounting. *Issues in Accounting Education*, 25(2), 279–321. doi:10.2308/iace.2010.25.2.279
- Degbaro, D., & Olofinsola, J. (2007). Forensic accountants and the litigation support engagement. *Nigerian Accountant*, 40(2), 49-52.
- Del Ponte, C., & Sudetic, C. (2009). *La traque, les criminels de guerre et moi: autobiographie [The hunt, the war criminals and me: autobiography]*. Éditions Héloïse d'Ormesson.
- Deloitte. (2015). *India Banking Fraud Survey-Edition II*. Deloitte. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/finance/in-fabanking-fraudsurvey-noexp.pdf>

## Compilation of References

- Demin, A. (2018). New model of tax administration: Change of paradigm. *Financial Law Review*, 10(2), 11–29. doi:10.4467/22996834FLR.18.008.9138
- Department for International Development. (2015). *Why corruption matters: understanding causes, effects and how to address them Evidence paper on corruption*. Retrieved from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/406346/corruption-evidence-paper-why-corruption-matters.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/406346/corruption-evidence-paper-why-corruption-matters.pdf)
- Department of the Treasury. (2016). *White Paper: Taxation Reform*. Australian Government Printer.
- Department of the Treasury. (2018). *Improving black economy enforcement and offences* (Consultation Paper). Retrieved from <https://treasury.gov.au/sites/default/files/2019-03/Consultation-Paper-Improving-black-economy-enforcement-and-offences.pdf>
- Desai, M. A., & Dharmapala, D. (2004). *Corporate Tax Avoidance and High Powered Incentives*. *Journal of Financial Economics*. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0304405X05001364>
- Desai, M. A., & Dharmapala, D. (2008). Tax and Corporate Governance: An Economic Approach. In W. Schoen (Ed.), *Tax and Corporate Governance* (Vol. 3, pp. 13–30). Springer - Verlag Berlin Heidelberg. doi:10.1007/978-3-540-77276-7\_3
- Desai, M. A. (2005). The degradation of reported corporate profits. *The Journal of Economic Perspectives*, 19(4), 171–192. doi:10.1257/089533005775196705
- DeVillis, R. F. (1991). *Scale development: Theory and applications*. Sage.
- Dey, P. K., & Rodriguez-Espindola, O. (2019, February 27). *Mexico is being held to ransom by oil thieves and systemic corruption*. Retrieved from <https://theconversation.com/mexico-is-being-held-to-ransom-by-oil-thieves-and-systemic-corruption-111118>
- DFID. (2015). *Why Corruption Matters: Understanding Causes Effects and How to Address Them* (DFID Evidence Paper on Corruption). London: Department for International Development. Retrieved from <https://www.gov.uk/government/publications/why-corruption-matters-understanding-causes-effects-and-how-to-address-them>
- Dhanalakshmi, S., & Subramanian, C. (2014). An analysis of data mining applications for fraud detection in securities market. *International Journal of Data Mining Techniques and Applications*, 3(1), 9–1. doi:10.20894/IJDMTA.102.003.001.003
- Dhar, P., & Sarkar, A. (2010). Forensic accounting. An accountants vision. *Vidysagar University Journal of Commerce*, 15(3), 93–104.
- DharK. (2012). SEBI and Collective Investment Schemes. *National Academy of Legal Studies and Research (NALSAR) University*. Available at SSRN 2014416. Retrieved from: doi:10.2139srn.2014416
- Diaz, D., Theodoulidis, B., & Sampaio, P. (2011). Analysis of stock market manipulations using knowledge discovery techniques applied to intraday trade prices. *Expert Systems with Applications*, 38(10), 12757–12771. doi:10.1016/j.eswa.2011.04.066
- Dickey, M. R. (2016, November 13). FriendFinder Networks Hack Reportedly Exposed Over 412 Million Accounts. *TechCrunch*. Retrieved from <https://techcrunch.com/2016/11/13/friendfinder-hack-412-million-accounts-breached/>
- DiGabriele, J. A. (2009). Implications of Regulatory Prescriptions and Audit Standards on The Evolution of Forensic Accounting in The Audit Process. *Journal of Applied Accounting Research*, 10(2), 109–121. doi:10.1108/09675420910984673
- Diih, S. S. (2005). *The infiltration of the New York's financial market by organised crime: pressures and control* [Unpublished Ph.D. Dissertation]. Cardiff University.

- Dimitrijevic, D., Jovkovic, B., & Milutinovic, S. (2020). (in press). The scope and limitations of external audit in detecting frauds in company's operations. *Journal of Financial Crime, ahead-of-print*(ahead-of-print). Advance online publication. doi:10.1108/JFC-11-2019-0155
- DiNapoli, P. P. (2002). Adolescent violent behavior and ego development. *The Journal of Adolescent Health, 31*(6), 446–448. doi:10.1016/S1054-139X(02)00450-0 PMID:12457576
- DiNapoli, T. P. (2010). *Red Flags for Fraud*. State of New York Office of the State Comptroller.
- Ding, S., & Wu, Z. (2014). Family ownership and corporate misconduct in U.S. small firms. *Journal of Business Ethics, 123*(2), 183–195. doi:10.1007/10551-013-1812-1
- Dixon, W. (2019, February 19). *Fighting cybercrime – what happens to the law when the law cannot be enforced?* Retrieved from <https://www.weforum.org/agenda/2019/02/fighting-cybercrime-what-happens-to-the-law-when-the-law-cannot-be-enforced/>
- Dobos, P., & Takacs-Gyorgy, K. (2018). The Factors Influencing the Emergence of Unethical Business Behaviour. *International Journal of Contemporary Management, 17*(3), 51–75. doi:10.4467/24498939IJCM.18.025.9621
- Dobos, P., & Takacs-Gyorgy, K. (2019). Possible Smart City Solutions in the Fight against Black Economy. *Interdisciplinary Description of Complex Systems, 17*(3, 3-A), 468–475. doi:10.7906/indec.17.3.5
- Doerrenberg, P., & Duncan, D. (2019). *How does firm tax evasion affect prices?* Universität Mannheim. Retrieved from <https://madoc.bib.uni-mannheim.de/47857/>
- Dohadwala, B. (2019, April 11). RBI issues directions to prevent market abuse. *Tax Guru*. Retrieved from <https://taxguru.in/rbi/rbi-issues-directions-prevent-market-abuse.html>
- Dombrowski v Pfister*, 380 US 479 (1965).
- Domingos, R. M. D. (2010). *A evolução da divulgação voluntária de informação nas empresas cotadas da Euronext Lisboa do ano 2006 a 2008*. ISCAL.
- Donaldson, T. (2012). Three ethical roots of the economic crisis. *Journal of Business Ethics, 106*(1), 5–8. doi:10.1007/10551-011-1054-z
- Dong, B., Dulleck, U., & Torgler, B. (2012). Conditional corruption. *Journal of Economic Psychology, 33*(3), 609–627. doi:10.1016/j.joep.2011.12.001
- Dorminey, J., Fleming, S., Kranacher, M., & Riley, R. (2010). Beyond the fraud triangle. *The CPA Journal, 80*(7), 17–23.
- Dorminey, J., Fleming, S., Kranacher, M., & Riley, R. Jr. (2012). The evolution of fraud theory. *Issues in Accounting Education, 27*(2), 555–579. doi:10.2308/iace-50131
- Dowling, G. R. (2013). The Curious Case of Corporate Tax Avoidance: Is it Socially Irresponsible? *Journal of Business Ethics, 1*–12. doi:10.1007/10551-013-1862-4
- Draca, M., & Machin, S. (2015). Crime and Economic Incentives. *Annual Review of Economics, 7*(1), 389–408. doi:10.1146/annurev-economics-080614-115808
- Dreisbach, T. (2020, August 14). Under Trump, SEC enforcement of insider trading dropped to lowest point in decades. *NPR*. Retrieved from <https://www.npr.org/2020/08/14/901862355/under-trump-sec-enforcement-of-insider-trading-dropped-to-lowest-point-in-decade>

## Compilation of References

- Drew, J. M., & Drew, M. E. (2010). *Ponzimonium: Madoff and the red flags of fraud* (Working Paper No. 2010, 07). Griffith Business School, University of Griffith Australia. Retrieved from <http://hdl.handle.net/10072/390466>
- DTCC. (2020). *The European Markets Infrastructure Regulation*. Retrieved from <https://www.dtcc.com/about>
- Duffie, D., & Stein, J. C. (2015). Reforming LIBOR and other financial market benchmarks. *The Journal of Economic Perspectives*, 29(2), 191–212. doi:10.1257/jep.29.2.191
- Duffield, G., & Grabosky, P. (2001). *The psychology of fraud Trends and Issues in Crime and Criminal Justice*. Australian Institute of Criminology.
- Duparc, P. A. (2010). La Suisse restitue au Liban les archives du fonds Dunand [Switzerland returns the archives of the Dunand collection to Lebanon]. *Le Monde*. Retrieved from [https://www.lemonde.fr/culture/article/2010/08/30/la-suisse-restitue-au-liban-les-archives-du-fonds-dunand\\_1404389\\_3246.html](https://www.lemonde.fr/culture/article/2010/08/30/la-suisse-restitue-au-liban-les-archives-du-fonds-dunand_1404389_3246.html)
- Dupuy, K., & Neset, S. (2018). *The cognitive psychology of corruption. Micro-level explanations for unethical behavior* (U4 Issue2018:2). Bergen: Chr. Michelsen Institute. Retrieved from <https://www.cmi.no/publications/6576-the-cognitive-psychology-of-corruption>
- Durkin, K., & Brinkman, R. (2009). 419 FRAUD: A Crime Without Borders in A Postmodern World. *International Review of Modern Sociology*, 35(2), 271–283.
- Dwenger, N., Kleven, H., Rasul, I., & Rincke, J. (2016). Extrinsic and intrinsic motivations for tax compliance: Evidence from a field experiment in Germany. *American Economic Journal. Economic Policy*, 8(3), 203–232. doi:10.1257/pol.20150083
- Dyreg, S. D., Hanlon, M., & Maydew, E. L. (2018). When does tax avoidance result in tax uncertainty? *The Accounting Review*, 94(2), 179–203. doi:10.2308/accr-52198
- Dyrud, M. A. (2005). I Brought You Good News: An Analysis of Nigerian 419 Letters. *Proceedings of the 2005 Association for Business Communication Annual Convention*.
- Dzamba, A. (2004). 36 Red Flags to Look for When Reviewing Financial Reporting Controls. *Financial Analysis. Planning & Reporting*, 4(8), 1–12.
- Easttom, W. C. (2018). *Network Defense and Countermeasures: Principles and Practices*. Pearson.
- EBA. (2019). *Report with advice for the European Commission on crypto-assets*. EBA. Retrieved from <https://eba.europa.eu>
- EC. (2013). *Evaluating and improving existing laws*. Brussels: European Commission. Retrieved from [https://ec.europa.eu/smart-regulation/evaluation/docs/syn\\_pub\\_rf\\_mode\\_en.pdf](https://ec.europa.eu/smart-regulation/evaluation/docs/syn_pub_rf_mode_en.pdf)
- EC. (2020a). *The European Market Infrastructure Regulation*. European Commission. [https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/post-trade-services/derivatives-emir\\_en](https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/post-trade-services/derivatives-emir_en)
- EC. (2020b). *Market Abuse Regulation*. European Commission. [https://ec.europa.eu/info/publications/market-abuse-regulation-mar\\_en](https://ec.europa.eu/info/publications/market-abuse-regulation-mar_en)
- Eckel, C. C., & Grossman, P. J. (2008). Men, women and risk aversion: Experimental evidence. *Handbook of Experimental Economics Results*, 1, 1061–1073.
- EFRAG. (2011). *Discussion Paper*. European Financial Reporting Advisory Group (EFRAG). Retrieved from [http://www.efrag.org/files/ProjectDocuments/Proactive - Income Taxes/120127\\_Income\\_tax\\_DP\\_final.pdf](http://www.efrag.org/files/ProjectDocuments/Proactive%20Income%20Taxes/120127_Income_tax_DP_final.pdf)

- Ekpo, C. E., Chime, J., & Enor, J. N. (2016). The irony of Nigeria's fight against corruption: An appraisal of president Muhammadu Buhari's first eight months in office. *International Journal of History and Philosophical Research*, 4(1), 61–73.
- El Hashem, B. (1990). *It was Kissinger who destroyed the nation of Lebanon*. EIR Feature.
- Elbahnasawy, N. G., & Revier, C. F. (2012). The determinants of corruption: Cross-country-panel-data analysis. *The Developing Economies*, 50(4), 311–333. doi:10.1111/j.1746-1049.2012.00177.x
- Electronic Communications Privacy Act of 1986, Pub. L. 99-508 (1986). Retrieved from <https://www.congress.gov/bill/99th-congress/house-bill/4952>
- Elias, A. I. (2014). The Use of Forensic in Fraud Detection and Control. *International Journal of Research in Management*, 4(5), 61–71.
- Elliott, T. L., Marquis, L. M., & Neal, C. S. (2013). Business ethics perspectives: Faculty plagiarism and fraud. *Journal of Business Ethics*, 112(1), 91–99. doi:10.1007/10551-012-1234-5
- Ellis, J., Smith, J., & White, R. (2020). Corruption and Corporate Innovation. *Journal of Financial and Quantitative Analysis*, 55(7), 2124–2149. doi:10.1017/S0022109019000735
- Eme, E. J. (2013). *An exploration of forensic accounting education and practice for fraud prevention and detection in Nigeria* (Unpublished PhD Thesis). University De Montfort, Leicester, UK.
- Enofe, A. O., Omagbon, P., & Ehigiator, F. I. (2015). Forensic audit and corporate fraud. *International Journal of Economics and Business Management*, 1(7), 1–10.
- Enofe, A. O., Omagbon, P., & Ehigiator, F. I. (2015). Forensic Audit and Corporate Fraud. *IIARD International Journal of Economics and Business Management*, 1(8), 55–64.
- Enste, D., & Heldman, C. (2017). *Causes and Consequences of Corruption: An Overview of Empirical Results* (IW-Report No. 2/2017). Cologne: Institut der deutschen Wirtschaft. Retrieved from <https://www.econstor.eu/handle/10419/157204>
- Eoyang, M., Peters, A., Mehta, I., & Gaskew, B. (2018, October 29). *To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors*. Retrieved from <https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors>
- Ernst & Young. (2017). *Reducing the Shadow Economy through Electronic Payments* (Report for Mastercard, 2017). Retrieved from [https://www.ey.com/Publication/vwLUAssets/Report\\_Shadow\\_Economy/\\$FILE/REPORT\\_ShadowEconomy\\_FINAL\\_17.pdf](https://www.ey.com/Publication/vwLUAssets/Report_Shadow_Economy/$FILE/REPORT_ShadowEconomy_FINAL_17.pdf)
- Esarey, J., & Schwindt-Bayer, L. A. (2019). Estimating causal relationships between women's representation in government and corruption. *Comparative Political Studies*, 52(11), 1713–1741. doi:10.1177/0010414019830744
- Esen, M. F., Bilgic, E., & Badas, U. (2019). How to detect illegal corporate insider trading? A data mining approach for detecting suspicious insider transactions. *Intelligent Systems in Accounting, Finance & Management*, 26(2), 60–70. doi:10.1002/isaf.1446
- ESMA. (2020). *Markets in Financial Instruments Directive*. European Securities and Market Authority Retrieved from <https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir>
- Etienne, J. (2013). Ambiguity and Relational Signals in Regulator-Regulatee Relationships. *Regulation & Governance*, 7(1), 35. doi:10.1111/j.1748-5991.2012.01160.x

## Compilation of References

- EU. (2014). *Regulation (EU) No 910/2014 of the European Parliament and of the Council - on electronic identification and trust services for electronic transactions in the internal market and repealing Directive. 1999/93/EC*. Brussels: Council of European Union. Retrieved from [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG)
- EUIPO. (2019). *Online Copyright Infringement in the European Union: Music, Films and TV (2017-2018), trends and drivers*. EUIPO.
- EurasiaNet. (2016a). *Uzbekistan: Officials Fired Over Pyramid Scheme*. EurasiaNet.Org. Retrieved from <https://eurasianet.org/uzbekistan-officials-fired-over-pyramid-scheme>
- EurasiaNet. (2016b). *Uzbekistan Arrests Its Own Bernie Madoff*. EurasiaNet.Org. Retrieved from <https://eurasianet.org/uzbekistan-arrests-its-own-bernie-madoff>
- EurasiaNet. (2018). *Kyrgyzstan: The Ponzi that Broke a Village* | Eurasianet. EurasiaNet.Org. Retrieved from <https://eurasianet.org/kyrgyzstan-the-ponzi-that-broke-a-village>
- Eurojust. (2019). *Common challenges in combating cybercrime*. Europol and Eurojust Public Information.
- Europa. (2019, June 26). *The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification*. Retrieved from <https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity>
- European Commission. (2014). *State aid: Commission investigates transfer pricing arrangements on corporate taxation of Apple (Ireland) Starbucks (Netherlands) and Fiat Finance and Trade (Luxembourg)*. Retrieved April 11, 2016, from [https://europa.eu/rapid/press-release\\_IP-14-663\\_en.htm](https://europa.eu/rapid/press-release_IP-14-663_en.htm)
- European Commission. (2015a). *Combating corporate tax avoidance : Commission presents Tax Transparency Package*. Retrieved June 7, 2016, from [https://europa.eu/rapid/press-release\\_IP-15-4610\\_en.htm](https://europa.eu/rapid/press-release_IP-15-4610_en.htm)
- European Commission. (2015b). *Commission decides selective tax advantages for Fiat in Luxembourg and Starbucks in the Netherlands are illegal under EU state aid rules*. Retrieved April 11, 2015, from [https://europa.eu/rapid/press-release\\_IP-15-5880\\_en.htm](https://europa.eu/rapid/press-release_IP-15-5880_en.htm)
- European Commission. (2016). *State aid: Commission concludes Belgian “Excess Profit” tax scheme illegal; around €700 million to be recovered from 35 multinational companies*. Retrieved April 11, 2016, from [https://europa.eu/rapid/press-release\\_IP-16-42\\_en.htm](https://europa.eu/rapid/press-release_IP-16-42_en.htm)
- European Commission. (2018). *Operational Guidance for the EU’s international cooperation on cyber capacity building*. European Commission.
- Europex. (2020a). *European Market Infrastructure Regulation (EMIR) (EU) No 648/2012*. Association of European Energy Exchanges. Retrieved from <https://www.europex.org/eu-legislation/emir/>
- Europex. (2020b). *Market Abuse Regulation (MAR) and Market Abuse Directive (CS MAD)*. Association of European Energy Exchanges. Retrieved from <https://www.europex.org/eu-legislation/mar-and-cs-mad-2/>
- Europol. (2018, March 26). *Mastermind Behind Eur 1 Billion Cyber Bank Robbery Arrested in Spain*. Retrieved from <https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>
- Evans, O. N. (2017). Forensic accounting and the combating of economic and financial crimes in Ghana. *European Scientific Journal*, 13(31), 379–393. doi:10.19044/esj.2017.v13n31p379



- Eyisi, A. S., & Ezuwore, C. N. (2014). The impact of forensic auditors in corporate governance. *Research Journal of Finance and Accounting*, 5(8), 31–39.
- Eze, E., & Okoye, E. (2019). Forensic accounting and fraud detection and prevention in Imo State Public Sector. *Accounting and Taxation Review*, 3(1), 12–26.
- Faizan, M., & Khan, R. A. (2019). Exploring and analyzing the dark Web: A new alchemy. *First Monday*, 24(5). Advance online publication. doi:10.5210/fm.v24i5.9473
- Falk, C. F., & Blaylock, B. K. (2012). The H Factor: A Behavioral Explanation of Leadership Failures in the 2007-2009 Financial System Meltdown. *Journal of Leadership, Accountability and Ethics*, 9(2), 68–82.
- Farhoomand, A., & Lentini, D. (2008). *e-Business Transformation in the Banking Industry: The Case of Citibank*. Asia Case Research Centre. The University of Hong Kong. Retrieved from [http://www.acrc.hku.hk/case/case\\_showdetails.asp?ct=newly&c=944&cp=1949&pt=1](http://www.acrc.hku.hk/case/case_showdetails.asp?ct=newly&c=944&cp=1949&pt=1)
- Farhoomand, A. (2004). *Managing (e) business transformation*. Palgrave Macmillan. doi:10.1007/978-1-137-08380-7
- Farooqui, A., & Nisa, S. (2017). Corporate Frauds and Its Impact: An Analysis of Select Cases. *Asian Journal of Management Applications and Research*, 8(1), 82–95.
- Farrar, J., Kaplan, S. E., & Thorne, L. (2019). The effect of interactional fairness and detection on taxpayers' compliance intentions. *Journal of Business Ethics*, 154(1), 167–180. doi:10.1007/10551-017-3458-x
- Farrar, J., Massey, D. W., Osecki, E., & Thorne, L. (2018). Tax fairness: Conceptual foundations and empirical measurement. *Journal of Business Ethics*, 162(3), 487–503. doi:10.1007/10551-018-4001-4
- FASB. (2011). *Accounting Standards Codification 740 Income Taxes*. Financial Accounting Standards Board. Retrieved from <https://law.resource.org/pub/us/code/bean/fasb.html/fasb.740.2011.html>
- FATF. (2020). *Virtual Currencies Key Definitions and Potential AML/CFT Risks*. Financial Action Task Force. Retrieved from: <https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
- Fathi, W. N. W., Ghani, E. K., Said, J., & Puspitasari, E. (2017). Potential employee fraud Scape in Islamic banks: The fraud triangle perspective. *Global Journal of Al-Thaqafah*, 7(2), 79–93. doi:10.7187/GJAT122017-3
- Faulkner, N., Borg, K., Bragge, P., Curtis, J., Ghafoori, E., Goodwin, D., Jorgensen, B. S., Jungbluth, L., Kneebone, S., Smith, L., Wright, B., & Wright, P. (2018). The INSPIRE Framework: How Public Administrators Can Increase Compliance with Written Requests Using Behavioral Techniques. *Public Administration Review*, 79(1), 125–135. doi:10.1111/puar.13004
- Fazekas, M., & Wachs, J. (2020). Corruption and the network structure of public contracting markets across government change. *Politics and Governance*, 8(2), 153–166. doi:10.17645/pag.v8i2.2707
- FBI. (2020). *What We Investigate, Cyber Crime*. Federal Bureau of Investigation. Retrieved from <https://www.fbi.gov/investigate/cyber>
- Fedeli, S., & Forte, F. (2012). A Game Theoretic Approach to Cross-Border VAT Evasion within EU Member States and its Relationship with the Black Economy. *Economic Analysis and Policy*, 42(2), 209–220. doi:10.1016/S0313-5926(12)50021-4
- Federal Trade Commission Act. 15 U.S.C. §§ 41-58, et. seq. (1914).

## Compilation of References

- Federal Trade Commission. (2019a). *What You Need to Know About Romance Scams*. Federal Trade Commission. Retrieved from <https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams>
- Federal Trade Commission. (2019b, February 12). *Romance Scams Rank Number One On Total Reported Losses*. Federal Trade Commission. Retrieved from <https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses>
- Federal Trade Commission. (2019c, February 12). *Romance Scams Will Cost You*. Federal Trade Commission. Retrieved from <https://www.consumer.ftc.gov/blog/2019/02/romance-scams-will-cost-you>
- Federal Trade Commission. (2020a). *Policy*. Federal Trade Commission. Retrieved from <https://www.ftc.gov/policy>
- Federal Trade Commission. (2020b, January). *Equifax Data Breach Settlement*. Federal Trade Commission. Retrieved from <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>
- Federal Trade Commission. (n.d.). *Report Identity Theft and Get a Recovery Plan*. Federal Trade Commission. Retrieved from <https://www.identitytheft.gov/>
- Fei, L., Shi, H., Sun, X., Liu, J., Shi, H., & Zhu, Y. (2020). The Profile of Ponzi Scheme Victims in China and the Characteristics of Their Decision-making Process. *Deviant Behavior*, 00(00), 1–14. doi:10.1080/01639625.2020.1768639
- Feld, L. P., Heckemeyer, J. H., & Overesch, M. (2013). Capital structure choice and company taxation: A meta-study. *Journal of Banking & Finance*, 37(8), 2850–2866. doi:10.1016/j.jbankfin.2013.03.017
- Fenaroli, G. C. (2016). *Financial Warfare: Money as an Instrument of Conflict and Tension in the International Arena* (Senior Projects). Bard College. Retrieved from [https://digitalcommons.bard.edu/senproj\\_s2016/136/](https://digitalcommons.bard.edu/senproj_s2016/136/)
- Ferdousi, Z., & Maeda, A. (2006). Unsupervised outlier detection in time series data. In *22nd International Conference on Data Engineering Workshops (ICDEW'06)* (pp. 51–56). IEEE. 10.1109/ICDEW.2006.157
- Ferguson, R. H. (2017). Offline ‘stranger’ and online lurker: Methods for an ethnography of illicit transactions on the darknet. *Qualitative Research*, 17(6), 683–698. doi:10.1177/1468794117718894
- Fernandes, P. O., Monte, A. P., & Afonso, S. (2013a). *Corporate Social Responsibility For The Psi 20 Portuguese Companies. Responsibility and Sustainability. Socioeconomic, political and legal issues* (Vol. 1). Research Group on Marketing and Operative Research & Faculty on Economics and Business Sciences, University of León. Retrieved from <https://bibliotecadigital.ipb.pt/handle/10198/11087>
- Fernandes, P. O., Monte, A. P., & Afonso, S. C. (2013b). Corporate Social Responsibility for the PSI 20 Portuguese companies. *Responsability and Sustainability*, 1, 7–15. Retrieved from [https://bibliotecadigital.ipb.pt/bitstream/10198/11087/1/RS-1\\_2\\_2-Fernandes-et-al.pdf](https://bibliotecadigital.ipb.pt/bitstream/10198/11087/1/RS-1_2_2-Fernandes-et-al.pdf)
- Fernandes, N., & Ferreira, M. A. (2009). Insider trading laws and stock price informativeness. *Review of Financial Studies*, 22(5), 1845–1887. doi:10.1093/rfs/hhn066
- Fernandez, R., McGauran, K., & Frederik, J. (2013). *Avoiding Tax in Times of Austerity. Energias de Portugal (EDP) and the Role of the Netherlands in Tax Avoidance in Europe*. Retrieved from [https://www.somo.nl/publications-en/Publication\\_3987](https://www.somo.nl/publications-en/Publication_3987)
- Ferreira, H. A. L. (2014). *Impostos diferidos: uma análise à sua contabilização mediante a dimensão das empresas*. ISCAL.
- Filippova, T. V., Kashapova, E. R., & Nikitina, S. S. (2016). Financial literacy as a key factor for an individual’s social and economic well-being. *EDP Sciences*, 28, 5. Retrieved from <http://earchive.tpu.ru/handle/11683/33078>

- Finance, U. K. (2018). *Fraud the Facts 2019: The definitive overview of payment industry fraud*. UK Finance. Retrieved from <https://www.ukfinance.org.uk/>
- Fischel, D. R., & Ross, D. J. (1991). Should the Law Prohibit 'Manipulation' in Financial Markets? *Harvard Law Review*, 105(2), 503–553. doi:10.2307/1341697
- Fisher, J. M. (2014). Fairer Shores: Tax Havens, Tax Avoidance, and Corporate Social Responsibility. *Boston University Law Review*. Boston University. School of Law, 94, 337–365. <http://ezproxy.concytec.gob.pe:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=94865540&lang=es&site=eds-live>
- Fitsanakis, J. (2016, January 25). Switzerland made secret deal with PLO in the 1970s, new book alleges. *Intelnews*. Retrieved from <https://intelnews.org/2016/01/25/01-1849/>
- Fitzgibbon, W., & Starkman, D. (2017). *The 'Paradise Papers' and the Long Twilight Struggle Against Offshore Secrecy*. Retrieved from <https://www.icij.org/investigations/paradise-papers/paradise-papers-long-twilight-struggle-offshore-secrecy>
- Fletcher, E. (2019, February 12). *Romance scams rank number one on total reported losses*. Retrieved from <https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses>
- Fligstein, N., & Roehrkasse, A. F. (2016). The causes of fraud in the financial crisis of 2007 to 2009: Evidence from the mortgage-backed securities industry. *American Sociological Review*, 81(4), 617–643. doi:10.1177/0003122416645594
- Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed Through Cryptocurrencies? *Review of Financial Studies*, 32(5), 1798–1853. doi:10.1093/rfs/hhz015
- Fonseca, A. (2011). *O impacto do reconhecimento de impostos diferidos nas demonstrações financeiras de empresas não cotadas: estudo de caso de 10 empresas do gabinete de contabilidade - Audifirb, Lda*. ISCAL. Retrieved from [http://repositorio.ipl.pt/bitstream/10400.21/3515/1/Trabalho Final.pdf](http://repositorio.ipl.pt/bitstream/10400.21/3515/1/Trabalho%20Final.pdf)
- Fontaine, A. S. (2016). Prime Minister Resigns. *The Reykjavik Grapevine*. Retrieved from <https://grapevine.is/news/2016/04/05/prime-minister-resigns/>
- Forester, T., & Morrison, P. (1994). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press.
- Francis, B. B., Hasan, I., Wu, Q., & Yan, M. (2014). Are female CFOs less tax aggressive? Evidence from tax aggressiveness. *The Journal of the American Taxation Association*, 36(2), 171–202. doi:10.2308/atax-50819
- Frankel, T. (2012). *The Ponzi scheme puzzle: a history and analysis of con artists and victims*. Oxford University Press. doi:10.1093/acprof:osobl/9780199926619.001.0001
- Fraud.net. (2020). *Fraud definitions*. Retrieved from: <https://fraud.net/d/fraud-definition/>
- Fraud.org. (2020). *Scams of the Heart: Sweetheart Swindles*. Fraud.org. Retrieved from <https://fraud.org/sweetheart-swindles/>
- Free, C., & Murphy, P. R. (2015). The ties that bind: The decision to co-offend in fraud. *Contemporary Accounting Research*, 32(1), 18–54. doi:10.1111/1911-3846.12063
- Frelberger, P. (1981). Micro Crime Macro Problem. *InfoWorld*, 38–39.
- Freud, S. (1923). The Ego and the Id. *The Standard Edition of the Complete Psychological Works of Sigmund Freud, Volume XIX (1923-1925): The Ego and the Id and Other Works*, 1 – 66.
- Frey, B. S. (2018). Countering Terrorism: Deterrence vs More Effective Alternatives. *Open Economics*, 1(1), 30–35. doi:10.1515/openec-2017-0002

## Compilation of References

- Friedrichs, D. (2004). Enron Et Al.: Paradigmatic White Collar Crime Cases for the New Century. *Critical Criminology*, 12(2), 113–132. doi:10.1023/B:CRIT.0000040258.21821.39
- Fruhlinger, J. (2020, February 12). Marriott Data Breach FAQ: How Did It Happen and What Was the Impact? CSO. Retrieved from <https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html>
- FSA. (2011). *David Massey v Financial Services Authority: UKUT 49 (TCC)*. Retrieved from [https://www.fca.org.uk/publication/final-notice/david\\_massey\\_fn.pdf](https://www.fca.org.uk/publication/final-notice/david_massey_fn.pdf)
- Fullerton, R. (2000). Political leaders must be held accountable for corruption. *Crossroads*, 6(4), 5–6.
- Funk, W. F., & Richard, H. S. (2005). *Administrative Law. Examples and Explanations*. Aspen Publishers.
- Furnell, S. (2001b). *Cybercrime: Vandalizing the Information Society*. Addison Wesley.
- Furnell, S. M. (2001a). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, 1(2), 35–44.
- Fu, Zh., & Mitnight, E. (2015). *Critical Success Factors for Continually Monitoring, Evaluating and Assessing Management of Enterprise IT*. ISACA.
- Fyneface, N. A., & Sunday, O. O. (2017). Forensic accounting and fraudulent practices in the public sector. *International Journal of Arts and Humanities*, 6(2), 171–181.
- Gao, J., Greenberg, R., & Wong-On-Wing, B. (2015). Whistleblowing intentions of lower-level employees: The effect of reporting channel, bystanders, and wrongdoer power status. *Journal of Business Ethics*, 126(1), 85–99. doi:10.1007/10551-013-2008-4
- Gao, Y., Sun, J., & Zhou, Q. (2017). Forward looking vs backward looking: An empirical study on the effectiveness of credit evaluation system in China's online P2P lending market. *China Finance Review International*, 7(2), 228–248. doi:10.1108/CFRI-07-2016-0089
- Garcia, D. A., & Parraga, M. (2019, January 12). *Explainer: Mexico's fuel woes rooted in chronic theft, troubled refineries*. Retrieved from <https://www.reuters.com/article/us-mexico-fuel-explainer-idUSKCN1P52BC>
- Garfinkel, J. A., & Nimalendran, M. (2003). Market structure and trader anonymity: An analysis of insider trading. *Journal of Financial and Quantitative Analysis*, 38(3), 591–610. doi:10.2307/4126733
- Garriga, E., & Melé, D. (2004). Corporate Social Responsibility Theories : Mapping the Territory Social Responsibility Corporate Theories : Mapping the Territory. *Journal of Business Ethics*, 53(1/2), 51–71. doi:10.1023/B:BUSI.0000039399.90587.34
- Gastwirth, J. L. (1977). A probability model of a pyramid scheme. *The American Statistician*, 31(2), 79–82.
- Gatsi, J. G., Gadzo, S. G., & Kportorgbi, H. K. (2013). The effect of corporate income tax on financial performance of listed manufacturing firms in Ghana. *Research Journal of Finance and Accounting*, 4(15), 118–124.
- Gaviria, A. (2002). Assessing the effects of corruption and crime on firm performance: Evidence from Latin America. *Emerging Markets Review*, 3(3), 245–268. doi:10.1016/S1566-0141(02)00024-9
- Gbegi, D. O., & Adebisi, J. F. (2014). Forensic accounting skills and techniques in fraud investigation in the Nigerian public sector. *Mediterranean Journal of Social Sciences*, 5(3), 248–252. doi:10.5901/mjss.2014.v5n3p243

- Gbegi, O. O., & Adebisi, J. F. (2013). The new fraud diamond model: How can it help forensic accountants in fraud investigation in Nigeria public sector? *Mediterranean Journal of Social Sciences*, 5(3), 243–252.
- Gediz Oral, B. (2011). Mali yolsuzlukla mücadele stratejileri: Türk vergi sistemi [Anti-financial corruption strategies: Turkish tax system]. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(3), 403–431.
- Gee, J., & Button, M. (2019). *The financial cost of fraud*. Retrieved from <http://www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf>
- Geis, G. (2011). *White-collar and corporate crime: a documentary and reference guide*. ABC-CLIO.
- Gentles, S. J., Charles, C., Ploeg, J., & McKibbin, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report*, 20(11), 1772–1789.
- Ghaniy, N., & Hastiadi, F. F. (2017). Political, social and economic determinants of corruption. *International Journal of Economics and Financial Issues*, 7(4), 144–149.
- Ghazali, M. Z., Rahim, M. S., Ali, A., & Abidin, S. (2014). A Preliminary Study on Fraud Prevention and Detection at the State and Local Government Entities in Malaysia. *Procedia: Social and Behavioral Sciences*, 164(1), 437–444. doi:10.1016/j.sbspro.2014.11.100
- Gibson, O., & Gayle, D. (2015, May 27). *Fifa officials arrested on corruption charges as World Cup inquiry launched*. Retrieved from <https://www.theguardian.com/football/2015/may/27/several-top-fifa-officials-arrested>
- Gilbert, E. (2019). Military geoeconomics: money, finance and war. In R. Woodward (Ed.), *A Research Agenda for Military Geographies* (pp. 100–114). Edward Edgar Publishing. doi:10.4337/9781786438874.00014
- Gill, M. (2011a). Fraud and recessions: Views from fraudsters and fraud managers. *International Journal of Law, Crime and Justice*, 39(3), 204–214. doi:10.1016/j.ijlcj.2011.05.008
- Gill, M. (2011b). Learning from fraudsters' accounts of their offending. *Prison Service Journal*, 194, 27–32.
- Gilsinan, J. F., Millar, J., Seitz, N., Fisher, J., Harshman, E., Islam, M., & Yeager, F. (2008). The role of private sector organizations in the control and policing of serious financial crime and abuse. *Journal of Financial Crime*, 15(2), 111–123. doi:10.1108/13590790810866854
- GIR. (2009). *Global Integrity Report: 2009-Key Findings*. Retrieved from <http://www.globalintegrity.org>
- Global Reporting Initiative. (2013a). *G4 Sustainability Reporting Guidelines*. Retrieved August 24, 2015, from <https://www.globalreporting.org/resource/library/GRIG4-Part1-Reporting-Principles-and-Standard-Disclosures.pdf>
- Global Reporting Initiative. (2013b). *G4 Sustainability Reporting Guidelines. Implementation Manual Governo de Portugal. Plano Estratégico. Combate à Fraude e Evasão Fiscais e Aduaneiras, 2015-2017 (2015)*. Retrieved from [https://info.portaldasfinancas.gov.pt/nr/rdonlyres/e245bdae-d856-4186-a950-f0be649869df/0/plano\\_estrategico\\_combate\\_fraude\\_fiscal\\_aduaneira\\_2015\\_2017.pdf](https://info.portaldasfinancas.gov.pt/nr/rdonlyres/e245bdae-d856-4186-a950-f0be649869df/0/plano_estrategico_combate_fraude_fiscal_aduaneira_2015_2017.pdf)
- Gogan, M. (2018, April 4). Man-in-the-Middle (MITM) Attacks: What They Are And How To Prevent Them? *Equities*. Retrieved from <https://www.equities.com/news/man-in-the-middle-mitm-attacks-what-they-are-and-how-to-prevent-them>
- Goldsmith, J. (2011, March 9). Cybersecurity Treaties A Skeptical View. *Future challenges in national security and law*, 6. Retrieved from <https://perma.cc/F5LD-27C4>
- Golmohammadi, K., & Zaiane, O. R. (2012). Data mining applications for fraud detection in securities market. *2012 European Intelligence and Security Informatics Conference*, 107-114. 10.1109/EISIC.2012.51

## Compilation of References

- Golmohammadi, K., & Zaiane, O. R. (2015). Time series contextual anomaly detection for detecting market manipulation in stock market. *IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 1-10. 10.1109/DSAA.2015.7344856
- Golmohammadi, K., Zaiane, O. R., & Díaz, D. (2014). Detecting stock market manipulation using supervised learning algorithms. *International Conference on Data Science and Advanced Analytics (DSAA)*, 435-441. 10.1109/DSAA.2014.7058109
- Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, 35(1), 220-265. doi:10.1080/07421222.2018.1440766
- Goodman, M. (1997). Why the Police Don't Care About Computer Crime. *Harvard Journal of Law & Technology*, 10, 466-494.
- Gorham, M. (2019). *2019 Internet Crime Report*. FIB.
- Gottschalk, P. (2018). Fraud Examiners in Private Investigations of White-Collar Crime. In *Fraud and Corruption* (pp. 213-235). Springer. doi:10.1007/978-3-319-92333-8\_11
- Gouda, M., & Park, S. M. (2015). Religious Loyalty and Acceptance of Corruption. *Journal of Economics and Statistics*, 235(2), 184-206.
- Grabosky, P. (2001). Virtual Criminality: Old Wine in New Bottles? *Social & Legal Studies*, 10(2), 243-249. doi:10.1177/a017405
- Graham, R., & Pitman, B. (2020). Freedom in the wilderness: A study of a Darknet space. *Convergence (London)*, 26(3), 593-619. doi:10.1177/1354856518806636
- Grant Thornton. (2016). *Financial and corporate frauds*. New Delhi: India. Retrieved from <https://www.grantthornton.in/globalassets/1.-member-firms/india/assets/pdfs/financialand-corporate-frauds.pdf>
- Gray, O. R., & Mousalli, S. D. (2006). Forensic accounting and auditing united again: A historical perspective. *Journal of Business Issues*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1642100](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1642100)
- Gray, C. W., & Kaufmann, D. (1998). Corruption and development. *Finance & Development*, 35(1), 7-10.
- Gray, D. (2008). Forensic accounting and auditing: Compared and contrasted to traditional accounting and auditing. *American Journal of Business Education*, 1(2), 116-126. doi:10.19030/ajbe.v1i2.4630
- Gray, G. L., & Debreceeny, R. S. (2014). A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. *International Journal of Accounting Information Systems*, 15(4), 357-380. doi:10.1016/j.accinf.2014.05.006
- Gray, P. (1997). *Artificial legal intelligence*. Dartmouth Publishing Co.
- Gredler, C. (2016, September 9). *The Real Cost of Identity Theft*. Retrieved from <https://www.csid.com/2016/09/real-cost-identity-theft/>
- Grewal-Carr, V., & Marshall, S. (2016). *Block-chain Enigma. Paradox. Opportunity*. London: Deloitte LLP. Retrieved from <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf>
- Gribnau, H. (2015). Corporate social responsibility and tax planning: Not by rules alone. *Social & Legal Studies*, 24(2), 225-250. doi:10.1177/0964663915575053

- Grinberg, I. (2018). International Taxation in an Era of Digital Disruption: Analyzing the Current Debate. *Taxes*, 3, 85-118. Retrieved from <https://scholarship.law.georgetown.edu/facpub/2145>
- Grippio, F. J., & Ibex, J. W. T. (2003). *Introduction to Forensic Accounting*. National Public Accountant.
- Grippio, F. J., & Ibex, T. (2003). Introduction to forensic accounting. *National Public Accountant*, 4, 4-8.
- Grohmann, A., Klühs, T., & Menkhoff, L. (2018). Does financial literacy improve financial inclusion? Cross country evidence. *World Development*, 111, 84-96. doi:10.1016/j.worlddev.2018.06.020
- Gugerty, M. K. (2007). You can't save alone: Commitment in rotating savings and credit associations in Kenya. *Economic Development and Cultural Change*, 55(2), 251-282. doi:10.1086/508716
- Gui, Z., Huang, Y., & Zhao, X. (2020). *Financial Fraud and Investor Awareness* (Working Paper). doi:10.2139/ssrn.3025400
- Gullkvist, B., & Jokipii, A. (2013). Perceived importance of red flags across fraud types. *Critical Perspectives on Accounting*, 24(1), 44-61. doi:10.1016/j.cpa.2012.01.004
- Gunasegaran, M., Quaddus, M., & Evans, R. (2010). Behavioral Intention to Use Forensic Accounting Services: A Critical Review of Theories and an Integrative Model. *Business Review (Federal Reserve Bank of Philadelphia)*, 15, 42-48.
- Gunningham, N. (2015). Regulation: From Traditional to Cooperative. In *The Oxford Handbook of White-Collar Crime*. New York: Oxford University Press.
- Guofeng, D. (2017). Legal Regulation of Alienation Operation of P2P Net Loan Platforms. *Journal of Shanghai University of Finance and Economics*, 19(4), 105-117.
- Gupta, P. P., Weirich, T. R., & Turner, L. E. (2013). Sarbanes-Oxley and public reporting on internal control: Hasty reaction or delayed action? *Accounting Horizons*, 27(2), 371-408. doi:10.2308/acch-50425
- Gupta, R. (2008). Tax evasion and financial repression. *Journal of Economics and Business*, 60(6), 517-535. doi:10.1016/j.jeconbus.2007.10.002
- Gupta, R. P., & Biswas, B. (2021). Banking Scams in India: A Case Based Analysis. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Gupta, S., Mills, L. F., & Towery, E. M. (2014). The Effect of Mandatory Financial Statement Disclosures of Tax Uncertainty on Tax Reporting and Collections. *The Journal of the American Taxation Association*, 36(2), 203-229. doi:10.2308/atax-50766
- Güredin, E. (2007). *Denetim ve Güvence Hizmetleri: SMMM ve YMM'lere Yönelik İlkeler ve Teknikler*. İstanbul: 11. Baskı, Arıkan Yay.
- Hacquebord, F., & Pernet, C. (2017). *Drilling Deep*. Retrieved from <http://www.a51.nl/sites/default/files/pdf/wp-drilling-deep-a-look-at-cyberattacks-on-the-oil-and-gas-industry.pdf>
- Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. John Wiley & Sons.
- Hadnagy, C. (2018). *Social Engineering* (2nd ed.). Wiley. doi:10.1002/9781119433729
- Hagan, J., Hewitt, J. D., & Alwin, D. F. (1979). Ceremonial justice: Crime and punishment in a loosely coupled system. *Social Forces*, 58(2), 506-527. doi:10.2307/2577603
- Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The Use of Partial Least Squares Structural Equation Modelling in Strategic Management Research: A Review of Past Practices and Recommendations for Future Applications. *Long Range Planning*, 45(5-6), 320-340. doi:10.1016/j.lrp.2012.09.008

## Compilation of References

- Hair, J., Anderson, R. E., Tatham, R. L., & Black, W. (1984). *Multivariate data analysis*. Petroleum Publishing.
- Hakmeh, J. (2017, June 6). *Building a Stronger International Legal Framework on Cybercrime*. Retrieved from <https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime>
- Halder, D., & Jaishankar, K. (2011). *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations*. IGI Global.
- Hamel, I. (2003). Victoire à l'arraché d'un trafiquant d'armes [Victory in the snatch of an arms dealer]. *Swissinfo*. Retrieved October 2019, from <https://www.Swissinfo.ch/fre/victoire-%C3%A0-l-arrach%C3%A9-d-un-trafiquant-d-armes/3212952>
- Handoko, B. L., & Selly (2020). The effect of fraud diamond on detection of financial statement fraud. *International Journal of Advanced Science and Technology*, 29(3), 467–475.
- Han, J., Kamber, M., & Pei, J. (2012). *Data Mining: Concepts and Techniques*. Morgan Kaufmann Publishers.
- Hansen, L. L., & Movahedi, S. (2010). Wall Street Scandals: The Myth of Individual Greed. *Sociological Forum*, 25(2), 367–374. doi:10.1111/j.1573-7861.2010.01182.x
- Hansen, L. P. (2021). *White Collar and Corporate Crime: A Case Study Analysis Approach*. Wolters Kluwer.
- Hao, X. (2010). Analysis of the Necessity to Develop the Forensic Accounting in China. *International Journal of Business and Management*, 5(5), 185–187. doi:10.5539/ijbm.v5n5p185
- Haray, J. W., Hillebrecht, J. M., Saleski, C. G., Masella, J. A., & King, J. D. (2016, December 7). *What is a personal benefit? US Supreme Court issues major insider trading decision – key takeaways*. White Collar Alert, DLA Piper Publications. Retrieved from <https://www.dlapiper.com/en/us/insights/publications/2016/12/what-is-a-personal-benefit/>
- Hardeck, I., Inger, K., Moore, R., & Schneider, J. (2019). *Cross-Cultural Evidence on Tax Disclosures in CSR Reports—A Textual Analysis Approach*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3308467](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3308467)
- Hardeck, I., & Hertl, R. (2013). Consumer Reactions to Corporate Tax Strategies: Effects on Corporate Reputation and Purchasing Behavior. *Journal of Business Ethics*, 123(2), 309–326. doi:10.1007/10551-013-1843-7
- Harris, C. K., & Brown, A. M. (2000). The Qualities of a Forensic Accountant. *Pennsylvania CPA Journal*, 71(1), 2–3.
- Hasan, I., Hoi, C. K. S., Wu, Q., & Zhang, H. (2014). Beauty is in the eye of the beholder: The effect of corporate tax avoidance on the cost of bank loans. *Journal of Financial Economics*, 113(1), 109–130. doi:10.1016/j.jfineco.2014.03.004
- Hasler, A., & Lusardi, A. (2017). The gender gap in financial literacy: A global perspective. Global Financial Literacy Excellence Center, The George Washington University School of Business.
- Hassan, R., & Noor, F. M. (2020). Islamic Good Governance for Waqf Institutions: A Proposed Framework. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 424–439). IGI Global. doi:10.4018/978-1-7998-0218-1.ch023
- Hatfield, M. (2015). Taxation and Surveillance: An Agenda. *Yale Journal of Law & Technology*, 17, 340–349.
- Hayes, R., Wallage, P., & Gortemaker, H. (2014). *Principles of auditing: an introduction to international standards on auditing*. Pearson.
- Helenne Doody and Technical Information Service. (2009). *Corporate Fraud - Topic Gateway* (Series No. 57). London: CIMA. Retrieved from [https://www.cimaglobal.com/Documents/ImportedDocuments/cid\\_tg\\_corporate](https://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_corporate)
- Henriksen, L. F., & Ponte, S. (2018). Public orchestration, social networks, and transnational environmental governance: Lessons from the aviation industry. *Regulation & Governance*, 12(1), 23–45. doi:10.1111/rego.12151



- Henseler, J., Ringle, C. M., & Sarstedt, M. (2014). A new criterion for assessing discriminant validity in variance-based structural equation modelling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. doi:10.1007/11747-014-0403-8
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). Testing Measurement Invariance of Composites Using Partial Least Squares. *International Marketing Review*, 33(3), 405–431. doi:10.1108/IMR-09-2014-0304
- Heo, Y., Hou, F., & Park, S. G. (2021). Does corruption grease or sand the wheels of investment or innovation? Different effects in advanced and emerging economies. *Applied Economics*, 53(1), 35–60. doi:10.1080/00036846.2020.1791313
- Hess, S., & Soltes, E. (2018). *MMM and bitcoin: Russian Ponzi mastermind Sergei Mavrodi is dead, but his legacy lives on in crypto* — Quartz. Quartz. Retrieved from <https://qz.com/1259524/mmm-and-bitcoin-russian-ponzi-mastermind-sergei-mavrodi-is-dead-but-his-legacy-lives-on-in-crypto/>
- Hess, P. (2002). *Cyberterrorism and Information War*. Anmol Publications.
- Hodge, A., Shankar, S., Rao, D. S. P., & Duhs, A. (2011). Exploring the Links Between Corruption and Growth: Corruption and Growth. *Review of Development Economics*, 15(3), 474–490. doi:10.1111/j.1467-9361.2011.00621.x
- Hogan, C. E., Rezaee, Z., Riley, R. A. Jr, & Velury, U. K. (2008). Financial statement fraud: Insights from the academic literature. *Auditing*, 27(2), 231–252. doi:10.2308/aud.2008.27.2.231
- Hoi, C. K., Wu, Q., & Zhang, H. (2013). Is corporate social responsibility (CSR) associated with tax avoidance? Evidence from irresponsible CSR activities. *The Accounting Review*, 88(6), 2025–2059. doi:10.2308/accr-50544
- Hoinaru, R., Buda, D., Borlea, S. N., Văidean, V. L., & Achim, M. V. (2020). The Impact of Corruption and Shadow Economy on the Economic and Sustainable Development. Do They “Sand the Wheels” or “Grease the Wheels”? *Sustainability*, 12(2), 481. doi:10.3390/s12020481
- Holland, K., Lindop, S., & Zainudin, F. (2016). Tax avoidance: A threat to corporate legitimacy? An examination of companies’ financial and CSR reports. *British Tax Review*, (3).
- Hollow, M. (2014). Money, morals and motives: An exploratory study into why bank managers and employees commit fraud at work. *Journal of Financial Crime*, 21(2), 174–190. doi:10.1108/JFC-02-2013-0010
- Holtfreter, K. (2015). General theory, gender-specific theory, and white-collar crime. *Journal of Financial Crime*, 22(4), 422–431. doi:10.1108/JFC-12-2014-0062
- Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Support Systems*, 46(4), 853–864. doi:10.1016/j.dss.2008.11.013
- Hoopes, J., Robinson, L., & Slemrod, J. (2018). Public Tax-Return Disclosure. *Journal of Accounting and Economics*, 66(1), 142–162. doi:10.1016/j.jacceco.2018.04.001
- Hope, O. K., Ma, M. S., & Thomas, W. B. (2013). Tax avoidance and geographic earnings disclosure. *Journal of Accounting and Economics*, 56(2-3), 170–189. doi:10.1016/j.jacceco.2013.06.001
- Hopwood, W. S., Leiner, J. J., & Young, G. R. (2008). *Forensic Accounting*. McGraw Hill/Irwin.
- Horton, J., Macve, R., & Struyven, G. (2004). Qualitative research: experiences in using semi structured interviews. In C. Humphrey & B. Lee (Eds.), *The real life guide to accounting research: A behind-the-scenes view of Using qualitative research methods* (pp. 339–357). Elsevier. doi:10.1016/B978-008043972-3/50022-0
- Hoseini, M., Gerayli, M. S., & Valiyan, H. (2019). Demographic characteristics of the board of directors’ structure and tax avoidance. *International Journal of Social Economics*, 46(2), 199–212. doi:10.1108/IJSE-11-2017-0507

## Compilation of References

- Houck, M. M., Kranacher, M. J., Morris, B., Riley, R. A., Robeitson, J. J., & Wells, J. T. (2006). Forensic Accounting as an Investigative Tool: Developing a Model Curriculum for Fraud and Forensic Accounting. *The CPA Journal*, 76(8), 68–70.
- Howard, S., & Sheetz, M. (2007). *Forensic accounting and fraud investigation for no experts*. Wiley.
- Howe, M. A., & Malgwi, C. A. (2006). Playing the ponies: A \$ 5 million embezzlement case. *Journal of Education for Business*, 82(1), 27–33. doi:10.3200/JOEB.82.1.27-33
- Huang, Q., & Yuan, T. (2019). Does Political Corruption Impede Firm Innovation? Evidence from the United States. *Journal of Financial and Quantitative Analysis*, 1–36. doi:10.1017/S0022109019000966
- Huang, Z., Deng, J., Xiong, M., Ren, Y., & Qiao, Y. (2014). Comparisons of P2P Regulatory Systems between USA, UK and China's P2P Regulatory Policies. *Financial Regulation Research*, 10, 4.
- Huddart, S., Ke, B., & Shi, C. (2007). Jeopardy, non-public information, and insider trading around SEC 10-K and 10-Q filings. *Journal of Accounting and Economics*, 43(1), 3–36. doi:10.1016/j.jacceco.2006.06.003
- Hudori, R., & Mustikasari, E. (2020). The Strength of Audits, Reporting Standards and Corruption, on Tax Evasion: A Cross-Country Study. *International Journal of Economics & Business Administration*, 8(2), 554–567. doi:10.35808/ijeba/481
- Huffman, M. L., Cohen, P. N., & Pearlman, J. (2010). Engendering change: Organizational dynamics and workplace gender desegregation, 1975–2005. *Administrative Science Quarterly*, 55(2), 255–277. doi:10.2189/asqu.2010.55.2.255
- Hughes, S. (2012). US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program. *Canadian Journal of Law and Society*, 27(3), 399–425. doi:10.1017/S0829320100010577
- Human Rights Watch and others v Secretary of State for the Foreign and Commonwealth Office and others* [2016] UKIPTrib 15\_165-CH.
- Humke, J. (1997). Comment, The Misappropriation Theory of Insider Trading: Outside the Lines of Section 10(b). *Marquette Law Review*, 80(3), 819–852.
- Huntington, S. P. (1968). *Political order in changing societies*. Yale University Press.
- Huseynov, F., & Klammer, B. K. (2012). Tax avoidance, tax management and corporate social responsibility. *Journal of Corporate Finance*, 18(4), 804–827. doi:10.1016/j.jcorpfin.2012.06.005
- Hussain, M. M., Kennedy, P., & Kierstead, V. (2010). Can audit prevent fraudulent financial reporting practices? Study of some motivational factors in two Atlantic Canadian entities. *Issues in Social and Environmental Accounting*, 4(1), 65–73. doi:10.22164/isea.v4i1.47
- Hussain, M., Nadeem, M. W., Iqbal, S., Mehrban, S., Fatima, S. N., Hakeem, O., & Mustafa, G. (2019). Security and Privacy in FinTech: A Policy Enforcement Framework. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 81–97). IGI Global. doi:10.4018/978-1-5225-7805-5.ch005
- Hussen, M. S., & Çokgezen, M. (2020). The impact of regional institutional quality on firm innovation: evidence from Africa. *Innovation and Development*, 1–22. doi:10.1080/2157930X.2020.1750143
- IASB. (2009). *Income Tax: Basis for Conclusions. Exposure Draft ED/2009/2*. International Accounting Standards Board. Retrieved from <https://www.ifrs.org/Current-Projects/IASB-Projects/Income-Taxes/ED-march-09/Documents/EDIncomeTaxesBC.pdf>

- Ibemere, I. D. (2020). Next Level: 2021 budget serviced by Debt! *Dataphyte*. Retrieved from <https://www.dataphyte.com/economy/next-level-2021-budget-serviced-by-debt/>
- IBM. (2020). *Blockchain*. Retrieved from <https://www.IBM.com/blockchain/what-is-blockchain>
- Ibrahim, U., Rose, S. S., & Mudzamir, M. B. (2016). Adoption of forensic accounting in fraud detection process by anti-corruption agency. *A Conceptual Frame Work*, 6(2), 139 – 148.
- Ibrahim. (2018). Adoption of forensic accounting in fraud detection process by Anti-corruption Agency: A conceptual framework. *International Journal of Management Research & Review*, 6(8), 139-148.
- Ibrahim, A. R. (2021). Religio-Spiritual Implications of Corruption and Money Laundering: The Case of Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- ICIJ. (2017). *The Panama Papers*. The International Consortium of Investigative Journalists. Retrieved from <https://panamapapers.icij.org/>
- IFRS. (2015). *IAS 12 Income Taxes. Impact of uncertainty when an entity recognises and measures a current tax liability or asset—Proposed draft IFRIC Interpretation (2015)*. London: International Financial Reporting Standards. Retrieved from <http://www.ifrs.org/Meetings/MeetingDocs/Interpretations Committee/2015/January/AP02A - IAS 12 Unceratin tax position - Draft interpretation.pdf>
- IFRS. (2017). *IFRS Standards*. Retrieved from <http://www.IFRS.org/Pages/default.aspx>
- IGT. (2018). *The Future of the Tax Profession*. Inspector-General of Taxation. Australian Government Printer.
- Imam, A. (2013). *Forensic accounting model for Fraud prevention and detection in Nigeria public sector* (Unpublished PhD Thesis). Usman Danfodio University, Accounting, Sokoto, Nigeria.
- Imam, A., Kumshe, A. M., & Jajere, M. S. (2015). Applicability of forensic accounting services for financial fraud detection and prevention in the public sector of Nigeria. *International Journal of Information Technology and Business Management*, 4(1), 136–152.
- IMF. (2009). *IMF Survey: IMF Advice Helps Fight Financial Fraud as Schemes Multiply. Pyramid, ponzi schemes*. International Monetary Fund. Retrieved from <https://www.imf.org/en/News/Articles/2015/09/28/04/53/sopol021209a>
- Imoniana, J. O., Antunes, M. T. P., & Formigoni, H. (2013). The forensic accounting and corporate fraud. *JISTEM-Journal of Information Systems and Technology Management*, 10(1), 119-144.
- In'airat, M. (2015). The role of corporate governance in fraud reduction-A perception study in the Saudi Arabia business environment. *Journal of Accounting & Finance*, 15(2), 119- 128.
- Insurance Information Institute. (2020). *Facts + Statistics: Identity theft and cybercrime*. Retrieved from: <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>
- Intel Security. (2014). *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II*. Intel Security. Retrieved from [https://www.csis.org/files/attachments/140609\\_McAfee\\_PDF.pdf](https://www.csis.org/files/attachments/140609_McAfee_PDF.pdf)
- International Monetary Fund. (2009). *Switzerland: Financial Sector Assessment Program - Detailed Assessment of Observance of Financial Sector Standards and Codes*. International Monetary Fund.
- Inyada, S. J., Olopade, D. O., & John, U. (2019). Effect of forensic audit on bank fraud in Nigeria. *American International Journal of Contemporary Research*, 9(2), 40- 45.

## Compilation of References

- IOSCO. (2000). *Investigating and prosecuting market manipulation. International Organization of Securities Commissions Report*. Retrieved from <https://www.iosco.org/>
- Iqbal, S., Hussain, M., Munir, M. U., Hussain, Z., Mehrban, S., Ashraf, A., & Ayubi, S. (2019). Crypto-Currency: Future of FinTech. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 1–13). IGI Global. doi:10.4018/978-1-5225-7805-5.ch001
- Irianto, B. S., Sudibyo, Y. A., & Wafirli, A. (2017). The Influence of Profitability, Leverage, Firm Size and Capital Intensity Towards Tax Avoidance. *International Journal of Accounting and Taxation*, 5(2), 33–41. doi:10.15640/ijat.v5n2a3
- Ishida, C., Chang, W., & Taylor, S. (2016). Moral intensity, moral awareness and ethical predispositions: The case of insurance fraud. *Journal of Financial Services Marketing*, 21(1), 4–18. doi:10.1057/fsm.2015.26
- Islam, M. J., Rahman, M. H., & Hossan, M. T. (2011). Forensic accounting as a tool for detecting fraud and corruption: An empirical study in Bangladesh. *ASA University Review*, 5(2), 77–85.
- Islam, S. R. (2018). *A Deep Learning Based Illegal Insider-Trading Detection and Prediction Technique in Stock Market*. Retrieved from <https://www.semanticscholar.org/paper/A-Deep-Learning-Based-Illegal-Insider-Trading-and-Islam/ffb4bf38805fdf58bcd3aba7829b379996f24059>
- Islam, A., Rashid, M. H. U., Hossain, S. Z., & Hashmi, R. (2020). Public policies and tax evasion: Evidence from SAARC countries. *Heliyon (London)*, 6(11). Advance online publication. doi:10.1016/j.heliyon.2020.e05449
- İşler, K., & Kutluay Tutar, F. (2019). Yolsuzluk ve ekonomik etkileri: Türkiye örneği [Corruption and economic impacts: In Turkey]. *Atlas International Refereed Journal on Social Sciences*, 5(17), 32–59.
- Iwata, E. (2003). Accounting Detectives in Demand. *USA Today*.
- Izedomin, F. I., & Mgbame, C. O. (2011). Curbing financial frauds in Nigeria, a case for forensic accounting. *African Journal of Humanities and Society*, 1(12), 52–56.
- Izzo, S. (2019). *Karl-Heinz Hoffmann's Secret History Links Neo-Nazis With Palestinian Terror*. Tablet Magazine. Retrieved from <https://www.tabletmag.com/jewish-arts-and-culture/culture-news/286220/karl-heinz-hoffmann-far-right> 1/11
- Jackson, K. M., Hruska, J., & Parker, D. (1992). *Computer Security References Book*. CRC Press.
- Jain, A. K. (2001). *The Political Economy of Corruption*. Routledge. doi:10.4324/9780203468388
- Javelin. (2020). *Javelin Strategy & Research*. Retrieved from <https://www.javelinstrategy.com/>
- Jayasekara, S. F. S. D. (2021). Risk-based AML/CFT Regulations for Effective Supervision. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Jenkins, R. & Newell, P. (2013). CSR, Tax and Development. *Third World Quarterly*, 34(March), 378–396. doi:10.1080/01436597.2013.784596
- Jenkins, J. G., & Sawyers, R. B. (2002). Financial Statement Disclosure of Corporate Tax Shelters. *The CPA Journal*, 72(6), 50–54.
- Jetter, M., Agudelo, A. M., & Hassan, A. R. (2015). The Effect of Democracy on Corruption: Income is Key. *World Development*, 74, 286–304. doi:10.1016/j.worlddev.2015.05.016
- Ji, Z. (2019). The Role of Information: Analysis of organizers' and Investors' Behavior in Ponzi scheme. *9th International Conference on Education and Social Science (ICESS 2019)*. 10.25236/icess.2019.141

- JMKR. (2020). *Электронная база данных юридических лиц, филиалов (представительств)*. Justice Ministry of Kyrgyz Republic. Retrieved from <https://register.minjust.gov.kg/register/Public.seam?publicId=445887>
- Johansson, E., & Carey, P. (2016). Detecting Fraud: The Role of the Anonymous Reporting Channel. *Journal of Business Ethics*, 139(2), 391–409. doi:10.1007/10551-015-2673-6
- Johnson, S. (1983). Francois Genoud: Terrorist controller for Swiss banks. *Executive Intelligence Review*.
- Johnson, S., Kaufmann, D., McMillan, J., & Woodruff, C. (2000). Why do firms hide? Bribes and unofficial activity after communism. *Journal of Public Economics*, 76(3), 495–520. doi:10.1016/S0047-2727(99)00094-8
- Johnston, M. (2009). *Poverty and Corruption*. Forbes. Retrieved from [https://www.forbes.com/2009/01/22/corruption-poverty-development-biz-corruption09-cx\\_mj\\_0122johnston.html?sh=3f24c2111a56](https://www.forbes.com/2009/01/22/corruption-poverty-development-biz-corruption09-cx_mj_0122johnston.html?sh=3f24c2111a56)
- Jones, M. J. (2012). *Creative Accounting, Fraud and International Accounting Scandals*. Wiley. doi:10.1002/9781119208907
- Jonkers, H., Band, I., & Quartel, D. (2012). ArchiSurance Case Study. *The Open Group*. Retrieved from <https://publications.opengroup.org/y163>
- Joosten, E., Bogers, M., Beeres, R., & Bertrand, R. (2019). Predictors for compliance with anti-terrorist financing standards. *Journal of Money Laundering Control*, 22(2), 257–269. doi:10.1108/JMLC-02-2018-0011
- Joseph, F. A., Okike, B. M., & Yoko, V. E. (2016). The Impact of Forensic Accounting in Fraud Detection and Prevention: Evidence from Nigerian Public Sector. *International Journal of Business Marketing and Management*, 1(5), 4–41.
- Joseph, F. A., Okike, B. M., & Yoko, V. E. (2016). The Impact of forensic accounting in fraud detection and prevention: Evidence from Nigerian public sector. *International Journal of Business Marketing and Management*, 1(55), 34–41.
- Jusoh, W. N. H. W. (2020). Corporate Social Responsibility: Conventional and Islamic Perspectives. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 129–149). IGI Global. doi:10.4018/978-1-7998-0218-1.ch007
- Justesen, M. K., & Bjørnskov, C. (2014). Exploiting the poor: Bureaucratic corruption and poverty in Africa. *World Development*, 58, 106–115. doi:10.1016/j.worlddev.2014.01.002
- Kabzeva, A., Niemann, M., Müller, P., & Steinmetz, P. (2010). Applying TOGAF to Define and Govern a Service-oriented Architecture in a Large-scale research & development (R&D). *Proceedings of the Sixteenth Americas Conference on Information Systems*.
- Kalenborn, C., & Lessmann, C. (2013). The impact of democracy and press freedom on corruption: Conditionality matters. *Journal of Policy Modeling*, 35(6), 857–886. doi:10.1016/j.jpolmod.2013.02.009
- Kanter, R. M. (2010). Powerlessness Corrupts. *Harvard Business Review*, 2010(July-August). <https://www.hbs.edu/faculty/Pages/item.aspx?num=38070> PMID:20607962
- Kapardis, M. K. (2016). *Corporate Fraud and Corruption*. Palgrave MacMillian. doi:10.1057/9781137406439
- Kapardis, M. K., & Papastergiou, K. (2016). Fraud victimization in Greece: Room for improvement in prevention and detection. *Journal of Financial Crime*, 23(2), 481–500. doi:10.1108/JFC-02-2015-0010
- Kapoor, M. (2018, September 26). *4 reasons why MGNREGA is not benefitting workers*. Retrieved from <https://www.businesstoday.in/top-story/4-reasons-why-mgnrega-is-not-benefitting-workers/story/282891.html>
- Karpoff, J. M. (2020). The future of financial fraud. *Journal of Corporate Finance*, 101694. doi:10.1016/j.jcorpfin.2020.101694

## Compilation of References

- Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Science*, 3(3), 191.
- Kasum, A. S. (2009). The Relevance of Forensic Accounting to Financial Crimes in Private and Public Sectors of Third World Economies: A Study from Nigeria. *The 1st International Conference on Governance Fraud Ethics and Social Responsibility*, 1-12.
- Kasum, A. S. (2009). The relevance of forensic accounting to financial crimes in private and public sectors of the third world economies: A study from Nigeria. *Journal of Accountancy*, 2(1), 23–40. doi:10.2139srn.1384242
- Katz, D. J. (2017). Waging Financial Warfare: Why and How. *Parameters*, 47(2), 41–49.
- Kaur, P., Krishan, K., Sharma, S. K., & Kanchan, T. (2018). ATM Card Cloning and Ethical Considerations. *Science and Engineering Ethics*, 25(5), 1311–1320. doi:10.1007/11948-018-0049-x PMID:29717470
- Kay, M. M. C., & King, M. C. (November 2019). *Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm*. Paper presented at the 2019 IEEE International Symposium on Technology and Society (ISTAS), Medford, MA. Retrieved from <https://ieeexplore.ieee.org/abstract/document/8938009> doi:10.1109/ISTAS48451.2019.8938009
- Kaya, U. (2005). Muhasebe Mesleğinde Adli Muhasebe Uzmanlığı ve Türkiye Açısından Gerekliği. *Muhasebe Bilim Dünyası Dergisi*, 7(1), 49–64.
- Keatinge, T., & Danner, K. (2018). Assessing Innovation in Terrorist Financing. *Studies in Conflict and Terrorism*, 1–18. doi:10.1080/1057610X.2018.1559516
- Keene, S. D. (2014). *Operationalizing Counter Threat Finance Strategies*. The Letort papers. Strategic Studies Institute. Retrieved from <https://apps.dtic.mil/dtic/tr/fulltext/u2/a612777.pdf>
- Kefela, G. T. (2010). Promoting access to finance by empowering consumers-Financial literacy in developing countries. *Educational Research Review*, 5(5), 205–212. <http://www.academicjournals.org/ERR>
- Kelton, S. (2020). *The deficit myth. Modern monetary theory and how to build a better economy*. John Murray.
- Kemp, S., Miro-Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, 26(3), 293–312. doi:10.1007/10610-020-09439-2
- Kenthineni, S., & Cao, Y. (2020). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review*, 30(3), 325–344. doi:10.1177/1057567719827051
- Kenyon, W., & Tilton, P. D. (2006). Potential Red Flags and Fraud Detection Techniques. In *A Guide to Forensic Accounting Investigation*. John Wiley & Sons.
- Kenyon, T. (2008). Tax Evasion, Disclosure, and Participation in Financial Markets: Evidence from Brazilian Firms. *World Development*, 36(11), 2512–2525. doi:10.1016/j.worlddev.2007.11.010
- Kesari, A. (2020a). The Effect of State Data Breach Notification Laws on Medical Identity Theft. University of California, Berkeley - D-Lab (Data-Intensive Social Science Lab); Yale Law School. doi:10.2139srn.3700248
- Kesari, A. (2020b). Predicting Cybersecurity Incidents Through Mandatory Disclosure Regulation. University of California, Berkeley - D-Lab (Data-Intensive Social Science Lab); Yale Law School. doi:10.2139srn.3700243
- Khan, M. M. (1999). Political and administrative corruption: Concepts, comparative experiences, and Bangladesh case. A Paper Prepared for Transparency International: Bangladesh Chapter, Dhaka.

- Khan, M. T., & Kanich, C. (2017). Old is Still Gold: A Comparison of Cyber and Traditional Consumer Fraud in The United States. *IEEE*. Retrieved from <https://www.ieee-security.org/TC/SPW2017/ConPro/papers/khan-conpro17.pdf>
- Khan, F. A., Asif, M., Ahmad, A., Alharbi, M., & Aljuaid, H. (2020). Blockchain technology improvement suggestions, security challenges on smart girl and its application in healthcare for sustainable development. *Sustainable Cities and Society*, 55, 102018. doi:10.1016/j.scs.2020.102018
- Khan, N., Rafay, A., & Shakeel, A. (2020). Attributes of Internal Audit and Prevention, Detection and Assessment of Fraud in Pakistan. *Lahore Journal of Business*, 9(1), 33–58. doi:10.35536/ljb.2020.v9.i1.a2
- Khiaonarong, T., & Humphrey, D. (2019). *Cash Use Across Countries and the Demand for Central Bank Digital Currency* (IMF Working Paper WP/19/46). International Monetary Fund.
- Khlif, H., & Guidara, A. (2018). Quality of management schools, strength of auditing and reporting standards and tax evasion. *EuroMed Journal of Business*, 13(2), 149–162. doi:10.1108/EMJB-05-2017-0017
- Kiehlborn, T. (2007). Risk management-challenge and opportunity. *Management International Review*, 47(4), 621–624.
- Kiley, D. (2018, August 23). Wanna Buy a Lamborghini Quickly? You Can Use Cryptocurrency at the Big Auctions Now. *Forbes*. Retrieved from: <https://www.forbes.com/sites/davidkiley5/2018/08/23/wanna-buy-a-lamborghini-quickly-you-can-use-crypto-currency-at-the-bonham-auction/?sh=4957d77c4ed>
- Kim, J., & Im, C. (2017). Study on corporate social responsibility (CSR): Focus on tax avoidance and financial ratio analysis. *Sustainability*, 9(10), 1710. doi:10.3390/u9101710
- Kim, Y., & Kogan, A. (2014). Development of an anomaly detection model for a bank's transitory account system. *Journal of Information Systems*, 28(1), 145–165. doi:10.2308/isys-50699
- Kirschner, J. (1995). *Currency and coercion: the political economy of international monetary power*. Princeton University Press.
- Kirschner, J. (2006). Currency and coercion in the Twenty-First Century. In D. A. Andrews (Ed.), *International monetary power* (pp. 139–161). Cornell University Press.
- Klaft, M. (2008a). Online peer-to-peer lending: A lenders' perspective. In H. R. Arabnia, & A. Bahrami (Eds.), *Proceedings of the International Conference on E-Learning, E-Business, Enterprise Information Systems, and E-Government* (pp. 371–375). London: CSREA Press
- Klein, R. (2015). How to avoid or minimize fraud exposures. *The CPA Journal*, 85(3), 6.
- Knack, S., & Kisunko, G. (2011). *Trends in corruption and regulatory burden in Eastern Europe and Central Asia* (Working Paper No. 59465). The World Bank.
- Koh, A. N., Arokiasamy, L., & Suat, C. L. A. (2009). Forensic accounting: Public acceptance towards occurrence of fraud detection. *International Journal of Business and Management*, 4(11), 145–149. doi:10.5539/ijbm.v4n11p145
- Kolhatkar, S. (2018). *Black Edge: Inside Information, Dirty Money, and the Quest to Bring Down the Most Wanted Man on Wall Street*. Random House.
- Kollias, C. (2008). A preliminary investigation of the burden sharing aspects of a European Union common defence policy. *Defence and Peace Economics*, 19(4), 253–263. doi:10.1080/10242690802164777
- Komisar, L. (2003). Offshore banking: The secret threat to America. *Dissent*, 50(2), 45–45.

## Compilation of References

- Kou, Y., Lu, C., Sirwongwattana, S., & Huang, Y. (2004). Survey of fraud detection techniques. *IEEE International Conference on Networking, Sensing & Control*, 749–754.
- Kowall, J., & Fletcher, C. (2013). *Modernize Your Monitoring Strategy by Combining Unified Monitoring and Log Analytics Tools*. Gartner Inc.
- Kozachenko, I. Y., Gubareva, A., & Kovalenko, K. (2017). International popularization of financial pyramids: Theoretical and practical aspects. *Universidad y Sociedad*, 9(2), 261–264. <https://rus.ucf.edu.cu/index.php/rus>
- KPMG. (2010). *Fraud and Misconduct Survey 2010*. Retrieved from: <http://www.kpmg.com>
- KPMG. (2013). *KPMG Malaysia Fraud, Bribery and Corruption survey 2013*. Retrieved from: <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/fraud-survey-report.pdf>
- KPMG. (2016). *Global profiles of the fraudster: Technology enables and weak controls fuel the fraud*. Retrieved, from <https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf>
- Krammer, S. M. S. (2013). Greasing the wheels of change: the impact of corruption on firms' innovation in transition economies (Working Paper). *35th DRUID Celebration Conference*, 17–19.
- Kranacher, M. J. (2010). Bringing the world together on one standard. *The CPA Journal*, 80(10), 17.
- Kranacher, M. J., Riley, R., & Wells, J. T. (2010). *Forensic accounting and fraud examination*. John Wiley & Sons.
- Kruglikov, K., & Coalson, R. (2020). *Building A Fortune On Misfortune: Pyramid Schemes Still A Bane In Russian Hinterland*. RFE/RL's Russian Service. Retrieved from <https://www.rferl.org/a/russia-pyramid-schemes-veliky-ustyug-putin/30436190.html>
- Kshetri, N. (2006). The Simple Economics of Cybercrime. *IEEE Security and Privacy*, 4(1), 33–39. doi:10.1109/MSP.2006.27
- Kumar, B. S., & Ravi, V. (2016). A survey of the applications of text mining in financial domain. *Knowledge-Based Systems*, 114, 128–147. doi:10.1016/j.knosys.2016.10.003
- Kumshe, A. M., Umar, I., & Imam, A. (2018). Prospects of Forensic Accounting Education in Nigeria: A Review. *Journal of Resources & Economic Development*, 1(1), 74–84.
- Kundu, S., & Rao, N. (2014). Reasons of Banking Fraud-A Case of Indian Public Sector Banks. *International Journal of Information Systems Management Research and Development*, 4(1), 11–24.
- Kunz, D. B. (1991). *The economic diplomacy of the Suez crisis*. University of North Carolina Press.
- KYC360. (2018, December 6). *EU group approves new-look ID cards to combat €2 billion identity theft*. Retrieved from <https://www.riskscreen.com/kyc360/news/new-look-eu-id-cards-to-help-combat-e2-billion-identity-theft-approved/>
- Kyle, A. S., & Viswanathan, S. (2008). How to define illegal price manipulation. *The American Economic Review*, 98(2), 274–279. doi:10.1257/aer.98.2.274
- Kyte, A. (2010). *Nine Critical Success Factors for Business Value -Through Application Overhaul*. Gartner Inc.
- La Porta, R., Lopez-de-Silanes, F., Shleifer, A., & Vishny, R. (1999). The quality of government. *Journal of Law Economics and Organization*, 15(1), 222–279. doi:10.1093/jleo/15.1.222
- Labs, T. (2020). *Fraud Guides 101*. Retrieved from <https://terbiumlabs.com/>



- Laguir, I., Staglianò, R., & Elbaz, J. (2015). Does corporate social responsibility affect corporate tax aggressiveness? *Journal of Cleaner Production*, 107, 662–675. Advance online publication. doi:10.1016/j.jclepro.2015.05.059
- Laleh, N., & Azgomi, M. A. (2009, March). A taxonomy of frauds and fraud detection techniques. In *International Conference on Information Systems, Technology and Management* (pp. 256-267). Berlin: Springer. 10.1007/978-3-642-00405-6\_28
- Lanis, R., & Richardson, G. (2012). Corporate social responsibility and tax aggressiveness: An empirical analysis. *Journal of Accounting and Public Policy*, 31(1), 86–108. doi:10.1016/j.jaccpubpol.2011.10.006
- Larson, S. (2017, October 4). *Every single Yahoo account was hacked - 3 billion in all*. Retrieved from <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html>
- Lawder, D. (2016). *IMF: Global corruption costs trillions in bribes, lost growth*. Reuters.com. Retrieved from <https://www.reuters.com/article/us-imf-corruption-idUSKCN0Y22B7>
- Lawton, T. C., Rosenau, J. N., & Verdun, A. C. (Eds.). (2018). *Strange Power: Shaping the Parameters of International Relations and International Political Economy*. Routledge.
- Le Monde. (2019). Le Prix Nobel d'économie Angus Deaton: Quand l'Etat produit une élite prédatrice [Nobel Lauréate in Economics Angus Deaton: "When the state produces a predatory elite]. *Le Monde*. Retrieved from [https://www.lemonde.fr/idees/article/2019/12/27/angus-deaton-quand-l-etat-produit-une-elite-predatrice\\_6024205\\_3232.html](https://www.lemonde.fr/idees/article/2019/12/27/angus-deaton-quand-l-etat-produit-une-elite-predatrice_6024205_3232.html)
- Le News. (2015). Swiss People's Party (UDC) leaders found guilty of racism. *Le News*. Retrieved from <https://lenews.ch/2015/04/30/two-swiss-peoples-party-udc-leaders-found-guilty-of-racism/>
- Le News. (2017). Racism sentence upheld against former Swiss People's Party secretary general. *Le News*. Retrieved from <https://lenews.ch/2017/04/13/racism-sentence-upheld-against-former-swiss-peoples-party-secretary-general/>
- Le Nguyen, Ch. (2020). National criminal jurisdiction over transnational financial crimes. *Journal of Financial Crime*, 27(4), 1361–1377. doi:10.1108/JFC-09-2019-0117
- Lee, W., & Stolfo, S. (1998). Data mining approaches for intrusion detection. *Proceedings of the 7th USENIX Security Symposium*. Retrieved from [https://www.usenix.org/legacy/publications/library/proceedings/sec98/full\\_papers/lee/lee.pdf](https://www.usenix.org/legacy/publications/library/proceedings/sec98/full_papers/lee/lee.pdf)
- Lee, C., Wang, C., & Ho, S. (2020). Country governance, corruption, and the likelihood of firms' innovation. *Economic Modelling*, 92, 326–338. doi:10.1016/j.econmod.2020.01.013
- Lee, W. S., & Guven, C. (2013). Engaging in corruption: The influence of cultural values and contagion effects at the micro level. *Journal of Economic Psychology*, 39, 287–300. doi:10.1016/j.joep.2013.09.006
- Leff, N. H. (1970). Economic Development through bureaucratic development. In *Political Corruption: Readings in Comparative Analysis*. Transaction Books.
- Leff, N. H. (1964). Economic Development Through Bureaucratic Corruption. *The American Behavioral Scientist*, 8(3), 8–14. doi:10.1177/000276426400800303
- Leistedt, S. J., & Linkowski, P. (2016). Fraud, individuals, and networks: A biopsychosocial model of scientific frauds. *Science & Justice*, 56(2), 109–112. doi:10.1016/j.scijus.2016.01.002 PMID:26976469
- Lendemen, R. (2003). *Implications for Investigations and Forensic Auditor*. Boston Beacon Press.
- Lenter, D., Slemrod, J., & Shackelford, D. (2003). Public Disclosure of Corporate Tax Return Information: Accounting, Economics, and Legal Perspectives. *National Tax Journal*, 56(4), 803–830. doi:10.17310/ntj.2003.4.06

## Compilation of References

- Lenz, R. (2016). Peer-to-Peer Lending: Opportunities and Risks. *European Journal of Risk Regulation*, 7(4), 688–700. doi:10.1017/S1867299X00010126
- Levenson, M. (2019, December 11). 5 Charged in New Jersey in \$722 Million Cryptocurrency Ponzi Scheme. *The New York Times*. Retrieved from <https://www.nytimes.com/2019/12/11/us/cryptocurrency-ponzi-scheme-nj.html>
- Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology & Criminal Justice*, 8(4), 389–419. doi:10.1177/1748895808096470
- Levi, M. (2009). White-Collar Crimes and the Fear of Crime: A Review. In S. S. Simpson & D. Weisburd (Eds.), *The criminology of white-collar crime* (pp. 79–109). Springer. doi:10.1007/978-0-387-09502-8\_5
- Levy, K. (2017). Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law. *Emerging Science. Technology in Society*, 3, 1–15.
- Lewis, J. (2018, February). *Economic Impact of Cybercrime—No Slowing Down*. Retrieved from [https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm\\_source=Press&utm\\_campaign=bb9303ae70-EMAIL\\_CAMPAIGN\\_2018\\_02\\_21&utm\\_medium=email](https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email)
- Lewis, L. J., Park, J. K., & Berkowitz, D. (2013). The Second Circuit holds the short-swing profit rule inapplicable to insider's purchase and sale of different types of stock in the same company. *Insights: The Corporate and Securities Law Advisor*, 27(2), 37–39.
- Lewis, M. K. (2015). *Understanding Ponzi schemes: can better financial regulation prevent investors from being defrauded?* Edward Elgar Publishing Ltd., doi:10.4337/9781782549109
- Leys, C. (1965). What is The Problem About Corruption? *The Journal of Modern African Studies*, 3(2), 215–230. doi:10.1017/S0022278X00023636
- Lightfoot, G., & Wisniewski, T. (2014). Information Asymmetry and Power in a Surveillance Society. *Information and Organization*, 24(4), 214–235. doi:10.1016/j.infoandorg.2014.09.001
- Lin, T. C. W. (2015). Financial Weapons of War. *Minnesota Law Review*, 100, 1377–1440.
- Lin, Y., Canhua, K., & Long, W. (2015). Study on Internet Financial Supervision Game: A Case Study of the P2P Net Loan Mode. *Nankai Economic Studies*, 2015(5), 126–139.
- Lisowsky, P., Robinson, L., & Schmidt, A. (2013). Do Publicly Disclosed Tax Reserves Tell Us About Privately Disclosed Tax Shelter Activity? *Journal of Accounting Research*, 51(3), 583–629. doi:10.1111/joar.12003
- Littlejohn Shinder, D. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress Shinderbooks.
- Liu, Y., & Feng, H. (2014). *Tax structure and corruption: Cross-country evidence* (Working Paper 14-27). International Center for Public Policy.
- Liu, C., & Mikesell, J. L. (2018). Corruption and tax structure in American States. *American Review of Public Administration*, 49(5), 585–600. doi:10.1177/0275074018783067
- Liu, L., & Miller, S. L. (2019). Intersectional Approach to Top Executive White-Collar Offenders' Discourses: A Case Study of the Martha Stewart and Sam Waksal Insider Trading Scandal. *Sociological Inquiry*, 89(4), 600–623. doi:10.1111/oin.12265
- Lo Prete, A. (2013). Economic literacy, inequality, and financial development. *Economics Letters*, 118(1), 74–76. doi:10.1016/j.econlet.2012.09.029

- Loebbecke, J. K., Eining, M. M., & Willingham, J. J. (1989). Auditors' experience with material irregularities: Frequency, nature, and detectability. *Auditing*, 9(1), 1–28.
- Lokanan, M., & Chopra, G. (2021). Money Laundering in Real Estate (RE): The Case of Canada. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Lopes, I. T. (2014). The information compliance indexes: the illustrative case of income taxes. *Contaduría Y Administración: Revista Internacional*, 59(4), 11–37. Retrieved from [https://repositorio.iscte-iul.pt/bitstream/10071/8190/1/publisher\\_version\\_CA2014.pdf](https://repositorio.iscte-iul.pt/bitstream/10071/8190/1/publisher_version_CA2014.pdf)
- Lopes, I. C. R. (2015). *Divulgação de informação voluntária: análise empírica às empresas do PSI-20*. ISCAL.
- Loukas, G., Patrikakis, C. Z., & Wilbanks, L. R. (2020). Digital Deception: Cyber Fraud and Online Misinformation. *IT Professional*, 22(2), 19–20. doi:10.1109/MITP.2020.2980090
- Lou, Y. I., & Wang, M. L. (2009). Fraud risk factor of the fraud triangle assessing the likelihood of fraudulent financial reporting. *Journal of Business & Economics Research*, 7(2), 61–78.
- Løvseth, T. (2001). *Corruption and Alienation*. Paper presented at ECPR Joint Sessions April 2001, Grenoble, Panel 16: “Corruption, Scandal and the Contestation of Governance in Europe”. Retrieved from <https://ecpr.eu/Events/Event/PaperDetails/5494>
- Lu, J. (2019, August). *Assessing the Cost, Legal Fallout of Capital One Data Breach*. Retrieved from [https://www.researchgate.net/publication/335210159\\_Assessing\\_The\\_Cost\\_Legal\\_FalloutOf\\_Capital\\_One\\_Data\\_Breach](https://www.researchgate.net/publication/335210159_Assessing_The_Cost_Legal_FalloutOf_Capital_One_Data_Breach)
- Lufax. (2014). *White paper: P2P Lending Market in China*. Retrieved from <http://blog.lendit.com/wp-content/uploads/2015/04/Lufax-white-paper-Chinese-P2P-Market.pdf>
- Lukes, S. (1974). *Power: A Radical View*. Palgrave Macmillan. doi:10.1007/978-1-349-02248-9
- Luo, Y., Shen, J., & Liu, X. (2016). *New policy of P2P lending guides healthy development of the industry: A detailed review and research on P2P interim measures*. Beijing: Huatai Securities. Retrieved from <https://www.htsc.com.cn>
- Lusardi, A., Mitchell, O. S., & Curto, V. (2010). Financial literacy among the young. *The Journal of Consumer Affairs*, 44(2), 358–380. doi:10.1111/j.1745-6606.2010.01173.x
- Ma, B., Zhou, Z., & Hu, F. (2017). Pricing mechanisms in the online Peer-to-Peer lending market. *Electronic Commerce Research and Applications*, 26(6), 119–130. doi:10.1016/j.elerap.2017.10.006
- MacGregor, J., & Stuebs, M. (2014). The silent Samaritan syndrome: Why the whistle remains unblown. *Journal of Business Ethics*, 120(2), 149–164. doi:10.1007/10551-013-1639-9
- MacKenzie, B., Coe Tsee, D., Njikizana, T., Chamboko, R., & Colyvas, B. (2011). *Income Taxes. In 2011 Interpretation and Application of International Financial Reporting Standards*. John Wiley & Sons, Inc.
- Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital ‘Demimonde’. *Information Communication and Society*, 19(1), 111–126. doi:10.1080/1369118X.2015.1093531
- Magee, J. R. (2011). *Peer-to-Peer Lending in the United States: Surviving after Dodd-Frank* (Working Paper No. 9). North Carolina Banking Institute. Retrieved from <https://go.gale.com/ps/anonymouse?id=GALE%7CA254244467&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=10967249&p=AONE&sw=w>
- Maghaireh, A. (2005). Combating Cyberterrorism: The Response from Australia and New Zealand. In *International Terrorism: New Zealand Perspectives papers from a seminar held in Wellington* (pp. 81-92). Institute of Policy Studies.

## Compilation of References

- Magumba, M. (2019). Tax administration reforms: Lessons from Georgia and Uganda (ICTD African Tax Administration Paper 5). Institute of Development Studies.
- Mahagaonkar, P. (2008). *Corruption and innovation: a grease or sand relationship?* (Working No. 017). Jena economic research papers.
- Malinowski, C. (2005). The Digital Investigative Unit: Staffing. In A. Thomas (Ed.), *Training, and Issues, Forensic Computer Crime Investigation*. CRC Press. doi:10.1201/9781420028379.ch2
- Mandell, L. (2009). The Impact of Financial Education in High School and College On Financial Literacy and Subsequent Financial Decision Making. *The American Economic Association Meetings*, 1–38. Retrieved from <https://www.aeaweb.org/conference/2009/retrieve.php?pdfid=507>
- Mandell, L., & Klein, L. S. (2009). The impact of financial literacy education on subsequent financial behavior. - Psyc-NET. *Financial Counseling and Planning*, 20(1), 15–24. <https://psycnet.apa.org/record/2009-19876-001>
- Manning, G. A. (2005). *Financial Investigation and Forensic Accounting*. Taylor and Francis.
- Manning, P. (2018). Madoff's Ponzi investment fraud: A social capital analysis. *Journal of Financial Crime*, 25(2), 320–336. doi:10.1108/JFC-06-2017-0057
- Manurung, D. T., & Hardika, A. L. (2015). *Analysis of factors that influence financial statement fraud in the perspective fraud diamond: Empirical study on banking companies listed on the Indonesia Stock Exchange year 2012 to 2014*. Paper presented at International Conference on Accounting Studies. Retrieved from <http://repo.uum.edu.my/17583/>
- Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, 59(3), 257–266. doi:10.1016/j.bushor.2016.01.002
- Marchini, K., & Pascual, A. (2019, March 6). *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*. Retrieved from <https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt>
- Marden, R., & Edwards, R. (2005). Internal controls for the small business: Skimming and the fraud triangle. *Internal Auditing*, 20(1), 3–10.
- Margulies, P. (2014). Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden. *The Hastings Law Journal*, 66, 1–13.
- Margulies, P. (2016). Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights. *Florida Law Review*, 68(4), 1045–1117.
- Markham, J. (2014). *Law Enforcement and the History of Financial Market Manipulation*. Routledge.
- Markin, R. J. (1979). The role of rationalization in consumer decision processes: A revisionist approach to consumer behavior. *Journal of the Academy of Marketing Science*, 7(4), 316–334. doi:10.1007/BF02729682
- Markman, M. S., Bucrek, J. E., Levko, A., Lechner, S. P., Haller, M. W., Dennis, R. W., Clayton, M. M., Dineen, J. C., & Schaffer, G. (2006). Other Dimensions of Forensic Accounting. In *A Guide to Forensic Accounting Investigation*. John Wiley & Sons.
- Marks, A., Bowling, B., & Keenan, C. (2017). Automatic Justice? Technology, Crime, and Social Control. In R. Brown-sword, E. Scotford, & K. Yeung (Eds.), *The Oxford Handbook of Law, Regulation and Technology*. Oxford University Press.
- Marria, V. (2019, February 4). *How Cryptocurrencies Are Empowering Cybercriminals*. Retrieved from <https://www.forbes.com/sites/vishalmarria/2019/02/04/how-cryptocurrencies-are-empowering-cybercriminals/#7be42bc237c5>

- Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in IS research. *Journal of Computer Information Systems*, 54(1), 11–22. doi:10.1080/08874417.2013.11645667
- Martínez, F. G. (2019a). *Special Problems in Information Security: From Privacy to Emerging Technologies for Hyper-connected Systems* (Master's thesis). Madrid: Universidad Politécnica de Madrid.
- Martínez, F. G. (2019b). Analysis of the US Privacy Model: Implications of the GDPR in the US. *International Journal of Hyperconnectivity and the Internet of Things*, 3(1), 43–52. doi:10.4018/IJHIoT.2019010103
- Martinez, F. G., & Dawson, M. (2019). Unprotected Data: Review of Internet Enabled Psychological and Information Warfare. *Land Forces Academy Review*, 24(3), 187–198. doi:10.2478/raft-2019-0022
- MAS. (2020). *Wash Trades*. Singapore: Monetary Authority of Singapore. Retrieved from <https://www.mas.gov.sg/>
- Masood, S. (2017). *Nawaz Sharif, Pakistan's Prime Minister, Is Toppled by Corruption Case*. *New York Times*. Retrieved from <https://www.nytimes.com/2017/07/28/world/asia/pakistan-prime-minister-nawaz-sharif-removed.html>
- Mathieu, A. (2020). Power and Currency: Did the Euro Improve the French State's Monetary Power? *International Journal of Political Economy*, 49(1), 62–82. doi:10.1080/08911916.2019.1693163
- Mathur, N. (2010). Shopping malls, credit cards and global brands: Consumer culture and lifestyle of India's new middle class. *South Asia Research*, 30(3), 211–231. doi:10.1177/026272801003000301
- Maurisse, M. (2016). L'enfer des expatriés français en Suisse: une «enquête». [The hell of French expatriates in Switzerland: an “investigation”]. *Le Temps*. Retrieved from <https://www.letemps.ch/opinions/lenfer-expatries-francais-suisse-une-enquete>
- Mauro, P. (1995). Corruption and Growth. *The Quarterly Journal of Economics*, 110(3), 681–712. doi:10.2307/2946696
- Mawanza, W. (2014). An analysis of the main forces of workplace fraud in Zimbabwean organisations: The fraud triangle perspective. *International Journal of Management Sciences and Business Research*, 3(2), 86–94. doi:10.2139/ssrn.2463235
- Mayer, A. H., da Costa, C. A., & Righi, R. D. R. (2020). Electronic health records in a blockchain: A systematic review. *Health Informatics Journal*, 26(2), 1273–1288. doi:10.1177/1460458219866350 PMID:31566472
- McConnell International LLC. (2000, December). *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*. Retrieved from <http://www.iwar.org.uk/law/resources/cybercrime/mcconnell/CyberCrime.pdf>
- McDaniel, D. (2019). *Data Breaches: Who is Behind Them, Why They Do It, and How to Protect Your Data*. Infosecwriters. Retrieved from [http://www.infosecwriters.com/Papers/dmcdaniel\\_databreaches.pdf](http://www.infosecwriters.com/Papers/dmcdaniel_databreaches.pdf)
- McDonough, M. (2010, February 25). Bad Check Schemes Targeting Lawyers are Increasingly Sophisticated. *ABA Journal*. Retrieved from [https://www.abajournal.com/news/article/bad\\_check\\_schemes\\_targeting\\_lawyers\\_are\\_increasingly\\_sophisticated/](https://www.abajournal.com/news/article/bad_check_schemes_targeting_lawyers_are_increasingly_sophisticated/)
- McGee, R. W., & Preobragenskaya, G. G. (2006). The ethics of tax evasion: A survey of Romanian business students and faculty. *Accounting and Financial Systems Reform in Eastern Europe and Asia*, 299–334.
- McGeever, J. (2017). *Timeline - The global FX rigging scandal*. Retrieved from <https://www.reuters.com/article/global-currencies-scandal/timeline-the-global-fx-rigging-scandal-idUSL5N1F14VV>
- McKinley, J., & Owsley, J. (2013). Transfer Pricing and Its Effect on Financial Reporting. *Journal of Accountancy*. Retrieved from <http://www.redi-bw.de/db/ebSCO.php/search.ebSCOhost.com/login.aspx?direct=true&db=buh&AN=92022767&site=ehost-live>

## Compilation of References

- McMillan, E. (2019, July 25). Cybercrime is going up across Canada, and most cases remain unsolved. *CBC News*. Retrieved from <https://www.CBC.ca/news/canada/nova-scotia/cyber-crime-rising-across-canada-1.5221330>
- McMullan, M. (1961). A theory of corruption. *The Sociological Review*, 9(2), 181–201. doi:10.1111/j.1467-954X.1961.tb01093.x
- Memdani, L., Kademi, T. T., & Rafay, A. (2021). Effect of Terrorism Financing on selected Global Indices: The Case of 2015 Paris Attacks. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Memon, N., & Lorenz, C. (2016). Does selecting a taxpayer for audit violate civil rights—a critical analysis of the Pakistani High Court's decision? *eJournal of Tax Research*, 14(3), 766–785.
- Méon, P., & Sekkat, K. (2005). Does corruption grease or sand the wheels of growth? *Public Choice*, 122(1-2), 69–97. doi:10.1007/11127-005-3988-0
- Meyer, G. (2000). Hacker, Phreakers, and Pirates: The Semantics of the Computer Underground. In G. M. Godwin (Ed.), *Criminal Psychology and Forensic Technology: A Collaborative Approach to Effective Profiling*. CRC Press.
- Millane, E., & Stewart, M. (2019). Behavioural insights in tax collection: getting the legal settings right. *eJournal of Tax Research*, 16(3), 500–535.
- Miller, J. (2017). Swiss high court rules anti-immigration SVP ad broke racism laws. *Reuters*. Retrieved from <https://www.reuters.com/article/us-swiss-racism-svp-idUSKBN17FIUT>
- Mills, L. F., Robinson, L., & Sansing, R. C. (2010). FIN 48 and tax compliance. *The Accounting Review*, 85(5), 1721–1742. doi:10.2308/accr.2010.85.5.1721
- Minarchiste, P. L. (2015). Quelles sont les causes de la crise de 2008? [What are the causes of the 2008 crisis?] *Contrepoints*. Retrieved from <https://www.Contrepoints.org/2015/03/14/201111-queelles-sont-les-causes-de-la-crise-de-2008>
- Ministério das Finanças. (2015). *Portaria n.º 220/2015 de 24 de julho (2015)*. PORTUGAL: Diário da República, 1.ª série — N.º 143 — 24 de julho de 2015. Retrieved from [http://www.cnc.min-financas.pt/pdf/SNC/2016/Portaria\\_220\\_2015\\_24Jul\\_DF.pdf](http://www.cnc.min-financas.pt/pdf/SNC/2016/Portaria_220_2015_24Jul_DF.pdf)
- Ministry of Foreign Affairs of Denmark. (2020). *Denmark is the least corrupt country in the World*. Retrieved from <https://studyindenmark.dk/news/denmark-is-the-least-corrupt-country-in-the-world>
- Minniti, R. K. (2011). *Introduction to Forensic Accounting*. Retrieved from <http://www.imavalleyofthesun.org>
- Mishra, S., & Singh, G. (2017). Forensic accounting: An emerging approach to deal with corporate frauds in India. *Global Journal of Enterprise Information System*, 9(2), 104–109. doi:10.18311/gjeis/2017/15922
- Mitra, S. (2017). To tax or not to tax? When does it matter for informality? *Economic Modelling*, 64, 117–127. doi:10.1016/j.econmod.2017.02.024
- Mock, T. J., Srivastava, R. P., & Wright, A. M. (2017). Fraud risk assessment using the fraud risk model as a decision aid. *Journal of Emerging Technologies in Accounting*, 14(1), 37–56. doi:10.2308/jeta-51724
- Modugu, K. P., & Anyaduba, J. O. (2013). Forensic accounting and financial fraud in Nigeria: An empirical approach. *International Journal of Business and Social Science*, 4(7), 281–289.
- Mohd, S. I., & Mazni, A. (2007). An Overview of Forensic Accounting in Malaysia. *International Conference on Business and Information*.

- Mongkolnavin, J., & Tirapat, S. (2009). Marking the close analysis in the Thai bond market surveillance using association rules. *Expert Systems with Applications*, 36(4), 8523–8527. doi:10.1016/j.eswa.2008.10.073
- Mo, P. H. (2001). Corruption and Economic Growth. *Journal of Comparative Economics*, 29(1), 66–79. doi:10.1006/jcec.2000.1703
- Morais, A. I., & Lourenço, I. C. (2013). Informação a divulgar. In IFRS: Demonstrações financeiras. Um guia para executivos (pp. 76–149). Coimbra: Edições Almedina, S.A.
- Morales, J., Gendron, Y., & Guénin-Paracini, H. (2014). The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. *Accounting, Organizations and Society*, 39(3), 170–194. doi:10.1016/j.aos.2014.01.006
- Morgan, A. R., & Burnside, C. (2014). Olympus corporation financial statement fraud case study: The role that national culture plays on detecting and deterring fraud. *Journal of Business Case Studies*, 10(2), 175–184. doi:10.19030/jbcs.v10i2.8506
- Mouré, K. (2020). Money in wars. In S. Battilossi, Y. Cassis, & K. Yago (Eds.), *Handbook of the History of Money and Currency* (pp. 995–1020). Springer., doi:10.1007/978-981-13-0596-2\_39
- Mulligan, S. (2018). *Cross-Border Data Sharing Under the CLOUD Act*. Congressional Research Service.
- Mundial, B. (1997). *Helping countries combat corruption: the role of the World Bank. Poverty Reduction and Economic Management*. The World Bank Group.
- Munshi, N. (2020, December 10). Nigerian economy at risk of ‘unravelling’, warns World Bank. *Financial Times*. Retrieved from <https://www.ft.com/content/14f600e9-2a7b-4a59-be67-f6485b256e99>
- Murdock, H. (2008). The three dimensions of fraud: Auditors should understand the needs, opportunities, and justifications that lead individuals to commit fraudulent acts. *The Internal Auditor*, 65(4), 81–83.
- Murphy, K. (2019). Moving towards a more effective model of regulatory enforcement in the Australian Taxation Office. Centre for Tax System Integrity (CTSI). Canberra: ANU Press.
- Murphy, R. (2014). *In the Shade: Research on the UK’s missing economy*. University of London. Retrieved from <https://openaccess.city.ac.uk/16563/>
- Mustafa, D., Baita, A. J., & Adhama, H. D. (2020). Quantitative economic evaluation of zakah-poverty nexus in Kano state, Nigeria. *International Journal of Islamic Economics and Finance*, 3(1), 21–50. doi:10.18196/ijief.2120
- Muthusamy, G. (2011). *Behavioral intention to use forensic accounting services for the detection and prevention of fraud by large Malaysian companies* (Doctoral dissertation). Curtin University, Australia.
- Muthusamy, G., Quaddus, M., & Evans, R. (2010, June). Organizational intention to use forensic accounting services for fraud detection and prevention by large Malaysian companies. *Proceedings of the 2010 Oxford Business & Economic Conference (OBEC)*.
- Myers, B. A., Pane, J. F., & Ko, A. (2004). Natural programming languages and environments. *Communications of the ACM*, 47(9), 47–52. doi:10.1145/1015864.1015888
- NAACP v Alabama*, 357 US 449, 462 (1958).
- Nabais, J. C. (1998). *O dever fundamental de pagar impostos*. Almedina.
- Nafti, O., Kateb, I., & Masghouni, O. (2020). Tax evasion, firm’s value and governance: Evidence from Tunisian Stock Exchange. *Journal of Financial Crime*, 27(3), 781–799. doi:10.1108/JFC-02-2020-0023

## Compilation of References

- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.
- Narayan, D. (2000). Poverty is powerlessness and voicelessness. *Finance & Development*, 37(4), 18.
- National Consumers League. (2011, February 7). *Scams, Shams, and Predators: Online Dating in a Digital Age*. National Consumers League. Retrieved from [https://www.nclnet.org/scams\\_shams\\_and\\_predators\\_online\\_dating\\_in\\_a\\_digital\\_age](https://www.nclnet.org/scams_shams_and_predators_online_dating_in_a_digital_age)
- National Crime Agency. (n.d.). *Sextortion (Webcam Blackmail)*. National Crime Agency. Retrieved from <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/kidnap-and-extortion/sextortion-webcam-blackmail>
- Nawaz, F. (2010). *Exploring the relationships between corruption and tax revenue* (U4 Expert Answer No. 228). Transparency International. Retrieved from <https://www.u4.no/publications/exploring-the-relationships-between-corruption-and-tax-revenue/>
- Newman, L. H. (2019, October 9). Never Trust a Platform to Put Privacy Ahead of Profit. *Wired*. Retrieved from <https://www.wired.com/story/twitter-two-factor-advertising/>
- News, A. B. C. (2019, August 24). *Dozens of Nigerian nationals arrested in California over alleged \$68m love scam*. Retrieved from <https://www.abc.net.au/news/2019-08-24/fbi-take-down-alleged-nigerian-love-scammers-in-46-million-case/11445500>
- Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569. doi:10.1016/j.dss.2010.08.006
- Nia, E. H., & Said, J. (2015). Assessing fraud risk factors of assets misappropriation: Evidences from Iranian banks. *Procedia Economics and Finance*, 31, 919–924. doi:10.1016/S2212-5671(15)01194-6
- Nicholson, L. (2014, February 4). 'We all told her not to go': Lonely WA grandmother Jette Jacobs' search for love ended in death. Retrieved from <https://www.watoday.com.au/national/western-australia/we-all-told-her-not-to-go-lonely-wa-grandmother-jette-jacobs-search-for-love-ended-in-death-20140204-31ywq.html>
- Nightingale, E. (2015). *A critical analysis of the relationship between democracy and corruption*. University of Sussex.
- Nikolova, M. (2017). *A new financial pyramid emerges in Russia every 48 hours*. FinanceFeeds. Retrieved from <https://financefeeds.com/new-financial-pyramid-emerges-russia-every-48-hours/>
- Nikolov, N. (2011). General characteristics of civil forfeiture. *Journal of Money Laundering Control*, 14(1), 16–31. doi:10.1108/13685201111098851
- Nisbet, R., Miner, G., & Yale, K. (2018). Advanced Algorithms for Data Mining. *Handbook of Statistical Analysis and Data Mining Applications*, 149–167. doi:10.1016/B978-0-12-416632-5.00008-6
- Njanike, K., Dube, T., & Mashayanye, E. (2009). The effectiveness of forensic auditing in detecting, investigating, and preventing bank frauds. *Journal of Sustainable Development in Africa*, 10(4), 405–425.
- Nobes, C. W. (1998). Toward a general model of reasons for international differences in financial reporting. *Abacus*, 34(2), 495–519. doi:10.1111/1467-6281.00028
- Nor, S. M., & Hashim, N. A. (2015). CSR and sustainability of Islamic banking: The bankers view. *Jurnal Pengurusan*, 45, 73–81. doi:10.17576/pengurusan-2015-45-07



- North Carolina Computer Trespass Act N.C.G.S. §14-458. (2016).
- Norton. (2020, March 10). *What is a Data Breach?* Norton. Retrieved from <https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html>
- Nosheen, S., Sadiq, R., & Rafay, A. (2016, September). The primacy of innovation in strategic financial management- understanding the impact of innovation and performance on capital structure. In *2016 IEEE International Conference on Management of Innovation and Technology (ICMIT)* (pp. 280-285). IEEE. 10.1109/ICMIT.2016.7605048
- Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. doi:10.1177/1609406917733847
- Nunnally, J. C. (1994). *Psychometric theory* (3<sup>rd</sup> ed.). Tata McGraw-Hill Education.
- Nur-tegin, K. D. (2008). Determinants of business tax compliance. *The B.E. Journal of Economic Analysis & Policy*, 8(1), 1–26. doi:10.2202/1935-1682.1683
- Nwaeze, C. (2008). Quality and internal control challenges in contemporary Nigeria banking. *Zenith Economic Quarterly*, 3(2), 23– 28.
- Nwosu, M.E., (2015). Forensic auditing and financial accounting in Nigeria: An assessment. *International Journal of Economics and Management Studies*, 2(7), 6– 11.
- NZLC. (2010). *Invasion of Privacy: Penalties and Remedies Report* (Report No. 113). New Zealand Law Commission.
- O’Fallon, M. J., & Butterfield, K. D. (2013). A review of the empirical ethical decision-making literature: 1996–2003. In *Citation Classics from the Journal of Business Ethics* (pp. 213–263). Springer. doi:10.1007/978-94-007-4126-3\_11
- O’Reilly, T. (2013). Open Data and Algorithmic Regulation. In B. Goldstein & L. Dyson (Eds.), *Beyond Transparency: Open Data and the Future of Civic Innovation* (pp. 289–300). Code for America Press.
- OECD. (1976). *Declaration by the Governments of OECD Member Countries and Decisions of the OECD Council on Guidelines for Multinational Enterprises*. Paris: Organisation for Economic Co-operation and Development (OECD) Publications. Retrieved from <http://www.oecd.org/daf/inv/mne/50024800.pdf>
- OECD. (2011). *OECD Guidelines for Multinational Enterprises*. Paris: Organisation for Economic Co-operation and Development (OECD) Publications. doi:10.1787/9789264115415-en
- OECD. (2011). *Putting an end to offshore tax evasion*. Global Forum on Transparency and Exchange of Information for Tax Purposes, Switzerland. Retrieved from <http://www.oecd.org/tax/transparency/>
- OECD. (2013, July 20). *Closing the tax gap*. Remarks by Angel Gurría, Secretary-General of the OECD, G20/OECD Action Plan on Base Erosion and Profit Shifting (BEPS) Moscow. Retrieved from <http://www.oecd.org/about/secretary-general/closing-the-tax-gap.htm>
- OECD. (2014). *Development Co-operation Report*. The Organisation for Economic Co-operation and Development. Retrieved from <https://www.oecd.org/dac/development-cooperation-report/>
- OECD. (2014). *Illicit Financial Flows from Developing Countries: Measuring OECD Responses*. Paris: Organisation for Economic Cooperation and Development. Retrieved from <https://www.oecd.org/corruption-integrity/>
- OECD. (2016). *Public Procurement Toolbox*. OECD.

## Compilation of References

- OECD. (2017). *The Changing Tax Compliance Environment and the Role of Audit*. Organisation for Economic Cooperation and Development. Retrieved from <https://www.oecd.org/ctp/the-changing-tax-compliance-environment-and-the-role-of-audit-9789264282186-en.htm>
- OECD. (2018). *Levels of Financial Literacy in Eurasia*. Organisation for Economic Co-operation and Development. Retrieved from <https://www.oecd.org/education/financial-education-cis.htm>
- OECD. (2020). *Anti-Corruption*. Paris: Organisation for Economic Cooperation and Development. Retrieved from <https://www.oecd.org/g20/topics/anti-corruption>
- Ogiriki, T., & Appah, E. (2018). Forensic accounting & auditing techniques on public sector fraud in Nigeria. *International Journal of African and Asian Studies*, 47, 7–16.
- Ogiriki, T., & Appah, E. (2018). Forensic accounting & auditing techniques on public sector fraud in Nigeria. *International Journal of African and Asian Studies*, 47, 7–18.
- Ogundana, O., Okere, W., Ogunleye, O., & Oladapo, I. (2018). Forensic accounting and fraud prevention and detection in Nigerian banking industry. *COJ Reviews & Research*, 1(1), 1-8. doi:10.31031/COJRR.2018.01.000504
- Öğüt, H., Doganay, M., & Aktas, R. (2009). Detecting stock-price manipulation in an emerging market: The case of Turkey. *Expert Systems with Applications*, 36(9), 11944–11949. doi:10.1016/j.eswa.2009.03.065
- Okoye, E. I., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and prevention in the public sector. (A study of selected ministries in Kogi state). *International Journal of Academic Research in Business and Social Sciences*, 3(3), 1–19.
- Okoye, E., & Ndah, E. N. (2019). Forensic accounting and fraud prevention in manufacturing companies in Nigeria. *International Journal of Innovative Finance and Economics Research*, 7(1), 107–116.
- Okoye, E. I., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and Prevention in the Public Sector. (A Study of Selected Ministries in Kogi State). *International Journal of Academic Research in Business & Social Sciences*, 3(3), 1–19.
- Okoye, E., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and prevention in the public sector. A study of selected ministries in Kogi State. *International Journal of Academic Research in Business & Social Sciences*, 3(1), 1–1.
- Okoye, E., & Ndah, E. N. (2019). Forensic accounting and fraud prevention in manufacturing companies in Nigeria. *International Journal of Innovative Finance and Economics Research*, 7(1), 107–116.
- Okoye, E., & Ndah, E. N. (2019). Forensic Accounting and Fraud Prevention in Manufacturing Companies in Nigeria. *International Journal of Innovative Finance and Economics Research*, 7(1), 107–116.
- Okunbor, J. A., & Obaretin, O. (2010). Effectiveness of the Application of Forensic Accounting Services in Nigerian Corporate Organisations. *AAU Journal of Management Sciences*, 1(1), 171–184.
- Okunbor, J. A., & Obratin, O. (2010). Effectiveness of the application of forensic accounting services in Nigerian organizations. *Journal of Management Sciences*, 1(1), 171–184.
- Olaniyi, T. A., Saad, T., Abiola, W. O., & Adebayo, S. A. (2013). Employee motivation and public sector fraud: Evidence from kwara state, Nigeria. *Journal of Humanities. Social Sciences and Creative Arts*, 8(1), 13–24.
- Olaoye, C. O., & Olanipekun, C. T. (2018). Impact of forensic accounting and investigation on corporate governance in Ekiti State. *Journal of Accounting. Business and Finance Research*, 4(1), 28–36. doi:10.20448/2002.41.28.36

- Olukayode, S. A. (2018). Forensic accounting investigation techniques and successful prosecution of corruption cases in Nigeria. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 8(3), 37–44.
- Ones, D., & Viswesvaran, C. (2001). Integrity tests and other criterion-focused occupational personality scales (COPS) used in personnel selection. *International Journal of Selection and Assessment*, 9(1/2), 31–39. doi:10.1111/1468-2389.00161
- Onwubiko, C. (2020). Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. *Computers & Security*, 96, 101838. doi:10.1016/j.cose.2020.101900
- Opukri, C., & Imomotimi Ebienfa, K. (2013). International Terrorism and Global Response: An Appraisal. *American Journal of Humanities and Social Sciences*, 1(3), 109–115. doi:10.11634/232907811301373
- Oraegbunam, I. K. (2015). Jurisdictional challenges in fighting cybercrimes: Any panacea from international law? *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 6, 57–65.
- Orucu, A. I., Aysu, A., & Bakırtaş, D. (2012). Yolsuzluğun kurumlar vergisi gelirleri üzerine etkisi: OECD ülkeleri analizi [The impact of corruption on corporate tax revenues: Analysis of OECD countries]. *Maliye Dergisi*, 163, 539–556.
- Othman, R., Aris, N. A., Mardziah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector: Accountants' and internal auditors' perceptions. *Procedia Economics and Finance*, 28, 59–67.
- Othman, R., Aris, N. A., Mardziah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector: Accountants' and internal auditors' perceptions. *Procedia Economics and Finance*, 28, 59–67. doi:10.1016/S2212-5671(15)01082-5
- Otutua-Amoah, N. (2017). Statistically Speaking: The Numbers Behind Cybercrimes. *Child. Legal Rts. J.*, 37, 174–179.
- Owen, G., & Savage, N. (2015, September). *The Tor Dark Net* (Paper Series: No. 20). The Centre for International Governance Innovation and Chatham House. Retrieved from <https://www.cigionline.org/publications/tor-dark-net>
- Owojori, A. A., & Asaolu, T. O. (2009). The role of forensic accounting in solving the vexed problem of corporate world. *European Journal of Scientific Research*, 29(2), 183–187.
- Oyedokun, G. E. (2013). *Emergence of forensic accounting and the role in Nigeria economy*. In a lecture delivered at the Annual NUASA Week, 2012.
- Özbek, Ç. (2003). İç Denetimde Yeni Uygulamalar. 7. *Türkiye İç Denetim Sempozyumu*.
- Özkul, F. U., & Pamukçu, A. (2012). Fraud detection and forensic accounting. In *Emerging fraud* (pp. 19–41). Springer. doi:10.1007/978-3-642-20826-3\_2
- Özkul, F. U., & Pektekin, P. (2009). Muhasebe Yolsuzluklarını Tespitinde Adli Muhasebecinin Rolü ve Veri Madenciliği Tekniklerinin Kullanılması. *Muhasebe ve Bilim Dünyası Dergisi*, 11(4), 57–87.
- Palmer, A. (2017). *Countering economic crime: a comparative analysis*. Routledge. doi:10.4324/9781315227122
- Pamungkas, I. D., Ghazali, I., & Achmad, T. (2018). A pilot Study of Corporate Governance and Accounting Fraud: The fraud Diamond Model. *The Journal of Business and Retail Management Research*, 12(2), 253–261. doi:10.24052/JBRMR/V12IS02/APSOCGAAFTFDM
- Papava, V. (2013). Reforming of the Post-Soviet Georgia's Economy in 1991-2011. *SSRN Electronic Journal*, 1–152. doi:10.2139/ssrn.2291142
- Paranjape, M., & Sheeth, R. (2011). A study of creative accounting and forensic accounting as interlinked trends in accounting. *International Journal For Business. Strategy and Management*, 1(1), 1–8.

## Compilation of References

- Paravicini, G. (2018). Millions flow from Gaddafi's 'frozen funds' to unknown beneficiaries. *Politico*. Retrieved from <https://www.politico.eu/article/muammar-gaddafi-frozen-funds-belgium-unknown-beneficiaries/>
- Parker, D. (1976a). Computer abuse perpetrators and vulnerabilities of computer systems. In *National Computer Conference* (pp. 65-73). AFIPS. Retrieved from <https://dl.acm.org/doi/10.1145/1499799.1499810>
- Parker, C., & Nielsen, V. L. (2017). Compliance: 14 questions. In P. Drahos (Ed.), *Regulatory theory: Foundations and applications* (pp. 217–232). ANU Press.
- Parker, D. (1976b). *Crime by Computer*. Charles Scribner's Sons.
- Parker, S. (2016). *The demise of secret bank accounts – Switzerland's private banks. face a new era of transparency*. Wolters Kluwer Financial Services, Inc.
- Patsuria, N. (2012, December 12). Center Point Group's Vast Ponzi Scheme. *Georgian Journal*. Retrieved from <https://www.georgianjournal.ge/business/21413-center-point-groups-vast-ponzi-scheme.html>
- Pauch, D. (2018). Gray Economy as Part of Tax Gap. *European Journal of Service Management*, 27(1), 197–210.
- Paunov, C. (2016). Corruption's asymmetric impacts on firm innovation. *Journal of Development Economics*, 118, 216–231. doi:10.1016/j.jdeveco.2015.07.006
- Payne, J. E., & Saunoris, J. W. (2020). Corruption and Firm Tax Evasion in Transition Economies: Results from Censored Quantile Instrumental Variables Estimation. *Atlantic Economic Journal*, 48(2), 195–206. doi:10.1007/11293-020-09666-2
- Pedneault, S., Silverstone, H., Rudewicz, F., & Sheetz, M. (2012). *Forensic accounting and fraud investigation for non-experts*. John Wiley & Sons.
- Pedro, C. (2013, September 9). Estudo ilustra com o caso da EDP como as empresas portuguesas pagam menos impostos ao deslocarem lucros para a Holanda. *Journal Dos Negócios*. Retrieved from [https://www.jornaldenegocios.pt/empresas/detalhe/caso\\_da\\_edp\\_mostra\\_que\\_empresas\\_lusas\\_sedeadas\\_na\\_holanda\\_pagam\\_menos\\_impostos\\_em\\_portugal.html](https://www.jornaldenegocios.pt/empresas/detalhe/caso_da_edp_mostra_que_empresas_lusas_sedeadas_na_holanda_pagam_menos_impostos_em_portugal.html)
- Pereira, E. J. dos R. (2013). *O reconhecimento e a divulgação dos impostos diferidos em Portugal: Análise às entidades cotadas no PSI geral durante os anos de 2009 a 2011*. ISCAL. Retrieved from [http://repositorio.ipl.pt/bitstream/10400.21/3494/1/Disserta%C3%A7%C3%A3o - Vers%C3%A3o Final %20Protegido%20.pdf](http://repositorio.ipl.pt/bitstream/10400.21/3494/1/Disserta%C3%A7%C3%A3o%20-%20Vers%C3%A3o%20Final%20Protegido%20.pdf)
- Perez, E. (2020, July 12). *How the US and Europe Are Regulating Crypto in 2020*. Retrieved from <https://cointelegraph.com/news/how-the-us-and-europe-are-regulating-crypto-in-2020>
- Peter, Z., Masoyi, A. D., Ernest, E. I., & Gabriel, A. O. (2014). Application of forensic auditing in reducing fraud cases in Nigeria money deposit banks. *Global Journal of Management and Business Research*, 14(3), 14–22.
- Peterson, A. (2016, November 14). Adult FriendFinder Hit With One of the Biggest Data Breaches Ever, Report Says. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2016/11/14/adult-friendfinder-hit-with-one-of-the-biggest-data-breaches-ever-report-says/>
- Petraşcu, D., & Tieanu, A. (2014). The role of internal audit in fraud prevention and detection. *Procedia Economics and Finance*, 16, 489–497. doi:10.1016/S2212-5671(14)00829-6
- Pi, H., & Xu, Z. (2016). *Summary report of Financial product for the year ended December 2015*. Karachi: Fortune Securities. Retrieved from <https://www.fortunesecurities.com/>
- Pintarich v Deputy Commissioner of Taxation* [2018] FCAFC 79.
- Pinto, L. C. de A. (2014). *Ética e responsabilidade social das empresas cotadas da Euronext Lisboa*. ISCAL.

- Pires, R. C. (2011). Ética e imposto: Reflexão de uma preocupação com a valorização da Sociologia e da Psicologia Fiscais. In *Ética fiscal* (pp. 33–58). Liabo: Universidade Lusíada Editora
- Pocar, F. (2004). New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research*, 10(1), 27–37. doi:10.1023/B:CRIM.0000037565.32355.10
- Poço, M. de L. C., Lopes, C. M. da M., & Silva, A. M. F. G. da. (2015). Percepção da evasão e fraude fiscal em Portugal: um estudo sociológico - Parte I. *Revista de Finanças Públicas E Direito Fiscal*, 7(3), 131–153.
- Pogarsky, G., Roche, S. P., & Pickett, J. T. (2018). Offender Decision-making in Criminology: Contributions from Behavioral Economics. *Annual Review of Criminology*, 1, 379–400.
- Polychroniou, C. J. (2020, April 10). Chomsky and Pollin: To heal from COVID-19, we must imagine a different world. *Truthout*. Retrieved from <https://truthout.org/articles/chomsky-and-pollin-to-heal-from-covid-19-we-must-imagine-a-different-world/>
- Potter, K. (2018). *Increased use of two-factor authentication force new social engineering tactics*. (Publication No. 10789454) [Master's thesis, Utica College]. ProQuest Dissertations Publishing.
- Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*. Que Corporation.
- Prabowo, H. Y. (2014). To be corrupt or not to be corrupt. *Journal of Money Laundering Control*, 17(3), 306–326. doi:10.1108/JMLC-11-2013-0045
- Pradhan, S. (2000). *Anticorruption in transition: A contribution to the policy debate*. The World Bank.
- Pratiwi, N., Shalihatulhayah, A., & Mayasari, D. (n.d.). The Influence of Political Factors on IFRS Adoption. *The 3rd Uzbekistan-Indonesia International Joint Conference on Economic Development and Nation Character Building to Meet the Global Economic Challenges*.
- Prebble, R., & Prebble, J. (2010). Does the Use of General Anti-Avoidance Rules to Combat Tax Avoidance Breach Principles of the Rule of Law? A Comparative Study. *Saint Louis University Law Journal*, 55(1), 21–46.
- Preuss, L. (2010). Tax avoidance and corporate social responsibility: You can't do both, or can you? *Corporate Governance: International Journal of Business in Society*, 10(4), 365–374. doi:10.1108/14720701011069605
- Preuss, L. (2012). Responsibility in Paradise? The Adoption of CSR Tools by Companies Domiciled in Tax Havens. *Journal of Business Ethics*, 110(1), 1–14. doi:10.1007/10551-012-1456-6
- PriceWaterhouseCoopers. (2008). Taxation. In B. Johnson & P. Holgate (Eds.), *IFRS Manual of Accounting - 2009. Global Guide to International Financial Reporting Standards* (pp. 13001–14001). CCH.
- PriceWaterhouseCoopers. (2014). *Financial statement presentation: 2014*. Retrieved August 31, 2015, from [http://www.pwc.com/en\\_US/us/cfodirect/assets/pdf/accounting-guides/pwc-financial-statement-presentation-second-edition-2015.pdf](http://www.pwc.com/en_US/us/cfodirect/assets/pdf/accounting-guides/pwc-financial-statement-presentation-second-edition-2015.pdf)
- Pringle, R. (2019). Money as a Tool of the State. In *The Power of Money* (pp. 151–156). Palgrave Macmillan. doi:10.1007/978-3-030-25894-8\_14
- Punch, M. (2000). Suite violence: Why managers murder and corporations kill. *Crime, Law, and Social Change*, 33(3), 243–280. doi:10.1023/A:1008306819319
- Purohit, M. C. (2007). Corruption in tax administration, performance accountability and combating Corruption. In A. Shah (Ed.), *World Bank Public Sector Governance and Accountability Series*. Academic Press.

## Compilation of References

- PWC. (2014). *Economic crime: A threat to business globally*. Retrieved from <https://www.pwc.com/gx/en/economic-crime-survey/pdf/pwc-latin-america-economic-crime-survey.pdf>
- PwC. (2020). *Global economic and fraud survey of 2020*. Retrieved from <https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf>
- Qiu, J., Lin, Z., & Luo, B. (2012). Effects of borrower-defined conditions in the online peer-to-peer lending market. In M. J. Shaw, D. Zhang, & W. T. Yue (Eds.), *E-life: web-enabled convergence of commerce, work, and social life* (pp. 167–179). Springer. doi:10.1007/978-3-642-29873-8\_16
- Quisenberry, W. L. (2017). Ponzi of all Ponzis: Critical analysis of the Bernie Madoff scheme. *International Journal of Econometrics and Financial Management*, 5(1), 1–6.
- Rab, H. (2020). Money and Monetary Issues in Islamic Finance. In A. Rafay (Ed.), *Handbook of Research on Theory and Practice of Global Islamic Finance* (pp. 38–60). IGI Global. doi:10.4018/978-1-7998-0218-1.ch003
- Rae, K., Subramaniam, N., & Sands, J. (2008). Risk management and ethical environment: Effects on internal audit and accounting control procedures. *Journal of Applied Management Accounting Research*, 6(1), 11–30.
- Rafay, A. (Ed.). (2019). *FinTech as a Disruptive Technology for Financial Institutions*. IGI Global. doi:10.4018/978-1-5225-7805-5
- Rafay, A. (Ed.). (2021). *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Rafay, A., & Ajmal, M. M. (2014). Earnings Management through Deferred Taxes Recognized under IAS 12: Evidence from Pakistan. *Lahore Journal of Business*, 3(1), 1–19. doi:10.35536/ljb.2014.v3.i1.a1
- Rafay, A., Ajmal, M., & Khalid, Z. (2016). Self-Sustainability of SME Banks - A Myth or Reality? Evidence from Selected Developing Economies across Asia. *SMEDA Research Journal*, 3(1), 64–74.
- Rafay, A., & Farid, S. (2017). Financial Integration in Money Markets: Evidence from SAARC Region. *DLSU Business and Economics Review*, 26(2), 87–114.
- Rafay, A., & Farid, S. (2018). Shariah Supervisory Board Report (SSBR) in Islamic Banks: An experimental study of Investors' perception and behaviour. *International Journal of Islamic and Middle Eastern Finance and Management*, 11(2), 274–296. doi:10.1108/IMEFM-07-2017-0180
- Rafay, A., Farid, S., Yasser, F., & Safdar, S. (2020). Social Collateral and Repayment Performance: Evidence from Islamic Micro Finance. *Iranian Economic Review*, 24(1), 41–74.
- Rafay, A., Sadiq, R., & Ajmal, M. M. (2016). The Effect of IAS-24 Disclosures on Governance Mechanisms and Ownership Structures in Pakistan. *Lahore Journal of Business*, 5(1), 15–36. doi:10.35536/ljb.2016.v5.i1.a2
- Rafay, A., Sadiq, R., & Mohsan, T. (2016). X-Efficiency in Banking Industry – Evidence from South Asian Economy. *Global Management Journal for Academic & Corporate Studies*, 6(1), 25–36.
- Rafay, A., Yasser, F., & Khalid, Z. (2019). Revaluation of Non-Current Assets under IAS-16: Possibility of any Managerial inducement - Evidence from a South Asian Economy. *DLSU Business and Economics Review*, 29(1), 93–105.
- Rahman, A. (2009). *Tackling corruption through tax administration reform* (Note Series No. 48312). Investment Climate Department, World Bank Group.
- Rahman, N. A. A., Zizi, N. A., Sairi, I. H., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology (IJIET)*, 10(5), 378–382. doi:10.18178/ijiet.2020.10.5.1393

- Rahn, W. M., Krosnick, J. A., & Breuning, M. (1994). Rationalization and derivation processes in survey studies of political candidate evaluation. *American Journal of Political Science*, 38(3), 582–600. doi:10.2307/2111598
- Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. *Issues in Accounting Education*, 23(4), 521–233. doi:10.2308/iace.2008.23.4.521
- Ramaswamy, V. (2005). Corporate Governance and the Forensic Accountant. *The CPA Journal*, 70(3), 68–70.
- Ramaswamy, V. (2007). New frontiers: Training forensic accountants within the accounting Program. *Journal of College Teaching and Learning*, 4(9), 3–38. doi:10.19030/tlc.v4i9.1545
- Ramos, M. (2003). Auditors' Responsibility for Fraud Detection. *Journal of Accountancy*, 95(1), 28–36.
- Ramzan, M., Ahmad, I., & Rafay, A. (2020). Is Auditor independence influenced by Non-audit services? A stakeholder's viewpoint. *Pakistan Journal of Commerce and Social Sciences*, 14(1), 388–408.
- Ranallo, L. F. (2006). *Forensic Investigations and Financial Audits: Compare and Contrast. In A Guide to Forensic Accounting Investigation*. John Wiley & Sons.
- Rangarajan, L. N. (Ed.). (1987). *Kautilya: The Arthashastra*. Penguin Classics.
- Raphaeli, N. (2003). Financing of terrorism: Sources, methods, and channels. *Terrorism and Political Violence*, 15(4), 59–82. doi:10.1080/09546550390449881
- Rashid, M. H. U. (2020). Taxpayer's Attitude Towards Tax Evasion in a Developing Country: Do the Demographic Characteristics Matter? *International Journal of Applied Behavioral Economics*, 9(2), 1–19. doi:10.4018/IJABE.2020040101
- Ravanetti, A. (2016). Switzerland Bank on Fintech with Lighter Regulations. *Crowd Valley*. Retrieved from <https://news.crowdvalley.com/news/switzerland-bank-on-fintech-with-lighter-regulations>
- Rayes, J., & Mani, P. (2019). Exploring Insider Trading Within Hypernetworks. In P. Haber, T. Lampoltshammer, & M. Mayr (Eds.), *Data Science – Analytics and Applications*. Springer. doi:10.1007/978-3-658-27495-5\_1
- Reddy, E., & Minnaar, A. (2018). Cryptocurrency: A Tool and Target for Cybercrime. *Acta Criminologica: Southern African Journal of Criminology*, 31(3), 71–92.
- Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, 3(2), 494–412.
- Reinstein, A., & McMillan, J. J. (2004). The Enron Debacle: More Than A Perfect Storm. *Critical Perspectives on Accounting*, 15(6-7), 955–970. doi:10.1016/j.cpa.2003.08.006
- Reurink, A. (2018). *Financial Fraud: A Literature Review*. Max Planck Institute for the Study of Societies.
- Reuters. (2012). *UK, Germany push for multinationals to pay "fair share" of taxes*. Retrieved from <https://www.reuters.com/article/2012/11/05/us-g20-tax-idUSBRE8A413D20121105>
- Reuters. (2019). Swiss group files criminal complaint against Credit Suisse over Mozambique loans. *Reuters*. <https://www.Reuters.com/article/us-mozambique-creidtsuisse/swiss-group-files-criminal-complaint-against-credit-suisse-over-mozambique-loans-idUSKCN1S5174>
- Reuters. (2020, July 17). Twitter says about 130 accounts were targeted in cyberattack this week. *CBC News*. Retrieved from <https://www.cbc.ca/news/technology/twitter-accounts-hacked-1.5653200>
- Rezaee, Z., & Lander, G. H. (1996). Integrating Forensic Accounting into the Accounting Curriculum. *Accounting Education*, 1(2), 147–163.

## Compilation of References

- Rezaee, Z., Lander, G. H., & Reinstein, A. (1992, August 20–25). Forensic Accounting: Challenges and Opportunities. *The Ohio CPA Journal*.
- Rezaee, Z., & Riley, R. (2012). *Financial Statement Fraud: Prevention and Detection*. Wiley. doi:10.1002/9781119198307
- Rezaee, Z., & Wang, J. (2019). Relevance of Big Data to Forensic Accounting Practice and Education. *Managerial Auditing Journal*, 34(3), 268–288. doi:10.1108/MAJ-08-2017-1633
- RFE/RL's Uzbek Service. (2018). *Uzbek Financier Jailed For Pyramid Scheme*. Radio Free Europe / Radio Liberty' Uzbek Service. Retrieved from <https://www.rferl.org/a/uzbekistan-pyramid-schemer-jailed/29056501.html>
- Rhodes, K. (2012). The counterfeiting weapons. *Region Focus*, 16(1), 34–37.
- Rho, J. (2007). Blackbeard of the Twentieth Century: Holding Cybercriminals Liable under the Alien Torts Statute. *Chicago Journal of International Law*, 7, 695–718.
- Richards, N. M. (2012). The dangers of surveillance. *Harvard Law Review*, 126, 1935.
- Rickards, J. (2012). *Currency Wars*. Penguin.
- Rickman, G. J. (1999). *Swiss Banks and Jewish Souls*. Transaction Publishers.
- Riemer, S. H. (1941). Embezzlement: Pathological basis. *The Journal of Criminal Law and Criminology*, 32(4), 411–423. doi:10.2307/1136639
- Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's Comments: A Critical Look at the Use of PLS-SEM. *Management Information Systems Quarterly*, 36(1), iii–xiv. doi:10.2307/41410402
- Rodrigues, J. (2012). *Sistema de normalização contabilística. SNC explicado*. Porto Editora.
- Rolland, J. (2004). *Lebanon: Current Issues and Background*. Nova Science Publishers Inc.
- Romanosky, S., Telang, R., & Acquisti, A. (2011). Do Data Breach Disclosure Laws Reduce Identity Theft? *Journal of Policy Analysis and Management*, 30(2), 256–286. doi:10.1002/pam.20567
- Roque, I. A. M. (2012). *Contabilidade Ambiental: estudo sobre a sua aplicabilidade numa amostra de empresas do PSI-20*. Escola Superior de Ciências Empresariais de Setúbal. Retrieved from [http://comum.rcaap.pt/bitstream/123456789/3996/1/Tese Contabilidade Ambiental - Iolanda Roque.pdf](http://comum.rcaap.pt/bitstream/123456789/3996/1/Tese%20Contabilidade%20Ambiental%20-%20Iolanda%20Roque.pdf)
- Rose-Ackerman, S. (2007). Measuring private sector corruption (U4 Brief, 2007(5)). Bergen: Michelsen Institute.
- Rose-Ackerman, S., & Palifka, B. J. (2016). *Corruption and Government: Causes, Consequences, and Reform*. Cambridge University Press. doi:10.1017/CBO9781139962933
- Rose, P. S., & Marquis, M. H. (2006). *Money and Capital Markets: Financial Institutions and Instruments in a Global Marketplace*. McGraw-Hill.
- Ross, S. (2020, March 4). Can you invest in hedge funds? *Investopedia*. Retrieved from <https://www.investopedia.com/ask/answers/011915/can-you-invest-hedge-funds.asp>
- Ross, E. A. (1907). *Sin and society: An analysis of latter-day iniquity*. Houghton Mifflin.
- Rukmi, A. M., & Soetrisno, W. A. (2019). Role of clustering based on density to detect patterns of stock trading deviation. *Journal of Physics: Conference Series*, 1218(1).



- Rutledge, S. L. (2010). *Consumer Protection and Financial Literacy: Lessons from Nine Country Studies* (No. 5326; Policy Research Working Paper, Issue June). <http://econ.worldbank.org>
- Saeed, S., Mubarik, F., & Zulfiqar, S. (2021). Money Laundering: A Thought-Provoking Crime. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Saha, C. A. (2014). A multidimensional approach to investigating frauds and scams: A study in the global and Indian context. *The Management Accountant India*, 49(9), 29–36.
- Salehi, M., & Azary, Z. (2008). Fraud detection and audit expectation gap: Empirical evidence from Iranian bankers. *International Journal of Business and Management*, 3(10), 65–77.
- Salihu, I. A., Annuar, H. A., & Obid, S. N. S. (2015). Foreign investors' interests and corporate tax avoidance: Evidence from an emerging economy. *Journal of Contemporary Accounting & Economics*, 11(2), 138–147. doi:10.1016/j.jcae.2015.03.001
- Sambo, U., & Sule, B. (2021). Financing as a Livewire for Terrorism: The Case of North-Eastern Nigeria. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Sampson, S. (2019). Citizen duty or Stasi society? Whistleblowing and disclosure regimes in organizations and communities. *Ephemera*, 19(4), 792–798.
- Sanches, J. L. S., Câmara, F. de S. da, & Gama, J. T. da. (Eds.). (2009). *Reestruturação de empresas e limites do planeamento fiscal*. Coimbra: Coimbra Editora.
- Sanches, J. L. S. (2006). *Os limites de planeamento fiscal*. Coimbra Editora.
- Sandler, T., & Forbes, J. F. (1980). Burden sharing, strategy, and the design of NATO. *Economic Inquiry*, 18(3), 425–444. doi:10.1111/j.1465-7295.1980.tb00588.x
- Sanger, D. E., Perlroth, N., Thrush, G., & Rappeport, A. (2018, December 11). Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing. *The New York Times*. Retrieved from <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>
- Sarker, S., Almukaynizi, M., Shakarian, J., & Shakarian, P. (2019). Mining user interaction patterns in the dark web to predict enterprise cyber incidents. *Social Network Analysis and Mining*, 9(1), 1–28. doi:10.1007/13278-019-0603-9
- Sarwar, A., & Afaf, G. (2016). A comparison between psychological and economic factors affecting individual investor's decision-making behavior. *Cogent Business & Management*, 3(1), 1–18. doi:10.1080/23311975.2016.1232907
- Sauka, A. (2008). Productive, Unproductive and Destructive Entrepreneurship: A Theoretical and Empirical Exploration. *SSRN Electronic Journal*. doi:10.2139/ssrn.1147811
- Sausgruber, R., & Tyran, J. R. (2005). Testing the Mill hypothesis of fiscal illusion. *Public Choice*, 122(1-2), 39–68. doi:10.1007/11127-005-3992-4
- Scamwatch. (2019, April 29). *Scams cost Australians half a billion dollars*. Retrieved from <https://www.scamwatch.gov.au/news-alerts/scams-cost-australians-half-a-billion-dollars>
- Scheiwiller, T., & Symons, S. (2014). Corporate responsibility and paying tax. *The OECD Observer. Organisation for Economic Co-Operation and Development*, 1. [http://www.oecdobserver.org/news/archivestory.php/aid/3132/Corporate\\_responsibility\\_and\\_paying\\_tax.html](http://www.oecdobserver.org/news/archivestory.php/aid/3132/Corporate_responsibility_and_paying_tax.html)
- Scheufele, D. A. (2000). Agenda-setting, priming, and framing revisited: Another look at cognitive effects of political communication. *Mass Communication & Society*, 3(2-3), 297–316. doi:10.1207/S15327825MCS0323\_07

## Compilation of References

- Schiappa, D. (2019, September 12). *The Big Business Of Cybercrime: The Dark Web*. Retrieved from <https://www.forbes.com/sites/forbestechcouncil/2019/09/12/the-big-business-of-cybercrime-the-dark-web/>
- Schiavo, V. (2019). FinTech: the top five legal issues to consider. *Dentons*. Retrieved from <https://www.dentons.com/en/insights/articles/2019/february/26/fintech-the-top-five-legal-issues-to-consider>
- Schmidt, D. (2007). Anti-Corruption: What Do We Know? Research on Preventing Corruption in the Post-Communist World. *Political Studies Review*, 5(2), 202–232. doi:10.1111/j.1478-9299.2007.00129.x
- Schnader, A. L., Bedard, J. C., & Cannon, N. (2015). The principal-agent dilemma: Reframing the auditor's role using stakeholder theory. *Accounting and the Public Interest*, 15(1), 22–26. doi:10.2308/apin-51234
- Schnatterly, K. (2003). Increasing firm value through detection and prevention of white-collar crime. *Strategic Management Journal*, 24(7), 587–614. doi:10.1002/mj.330
- Schneider, F., & Buehn, A. (2012). *Shadow economies in highly developed OECD countries: What are the driving forces?* Retrieved from <https://www.econstor.eu/bitstream/10419/67170/1/727543865.pdf>
- Schneider, F., Buehn, A., & Montenegro, C. E. (2010). *Shadow economies all over the world: New estimates for 162 countries from 1999 to 2007* (Working Paper No. 5356). Washington, DC: World Bank Group.
- Schneider, F., Raczkowski, K., & Mróz, B. (2015). Shadow economy and tax evasion in the EU. *Journal of Money Laundering Control*, 18(1), 34–51. doi:10.1108/JMLC-09-2014-0027
- Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. *Security Journal*, 29(2), 107–121. doi:10.1057/j.2013.1
- Schwarcz, D., & Zaring, D. (2017). Regulation by threat: Dodd-frank and the nonbank problem. *The University of Chicago Law Review*. *University of Chicago. Law School*, 84, 1813.
- SEC. (2000). Final Rule: Selective disclosure and insider trading. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/rules/final/33-7881.htm>
- SEC. (2003, June 4) SEC charges Martha Steward, Broker Peter Bacanovic with illegal insider trading. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/news/press/2003-69.htm>
- SEC. (2006). 2006 Performance and Accountability Report. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/about/secpar/secpar2006.pdf>
- SEC. (2013a). Ponzi schemes using virtual currencies. In *Investor Alert: Vol. N.153-7/13*. U.S. Securities Exchange Commission. Retrieved from [https://www.sec.gov/files/ia\\_virtualcurrencies.pdf](https://www.sec.gov/files/ia_virtualcurrencies.pdf)
- SEC. (2013b). *SEC Charges Texas Man with Running Bitcoin-Denominated Ponzi Scheme*. U.S. Securities Exchange Commission. Retrieved from <https://www.sec.gov/news/press-release/2013-132#.Ue6yZODmp-I>
- SEC. (2016, Nov 14). SEC announces settlement with former government official in insider trading case. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/litigation/litreleases/2016/lr23688.htm>
- SEC. (2018, April 30). SEC obtains final consent judgements against William Walters and Thomas Davis. Litigation Release No. 24125. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/litigation/litreleases/2018/lr24125.htm>
- SEC. (n.d.a) SEC Enforcement Actions: Insider Trading Cases. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/spotlight/insidertrading/cases.shtml>

- SEC. (n.d.b). Fast Answers: Form 10-Q. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/fast-answers/answersform10qhtm.html>
- SEC. (n.d.c). Fast Answers: Hedge Funds. *U.S. Securities and Exchange Commission*. Retrieved from <https://www.sec.gov/fast-answers/answershedgehtm.html>
- Secretário do Estado dos Assuntos Fiscais. Despacho n.º 260/2015 -XIX, Aviso n.º 8256/2015, Diário de República, 2.ª série — N.º 146 — 29 de julho de 2015. PORTUGAL. Retrieved from [http://www.cnc.min-financas.pt/pdf/SNC/2016/Aviso\\_8256\\_2015\\_29Jul\\_NCRF\\_RG.pdf](http://www.cnc.min-financas.pt/pdf/SNC/2016/Aviso_8256_2015_29Jul_NCRF_RG.pdf)
- Seddon, A. E., & Pass, A. D. (2009). *Forensic Sciences*. Salem Press.
- Seetharaman, A., Senthilvelmurugan, M., & Periyamayagam, R. (2004). Anatomy of Computer Accounting Frauds. *Managerial Auditing Journal*, 19(8), 1055–1072. doi:10.1108/02686900410557953
- Segal, M. (2015). Peer-to-Peer Lending: A Financing Alternative for Small Business. *Issue Brief*, 10, 1–14.
- Sekmen, T., & Hatipoglu, M. (2019). FinTech and Stock Market Behaviors: The Case of Borsa Istanbul. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 170–205). IGI Global. doi:10.4018/978-1-5225-7805-5.ch008
- Sennewald, C. A., & Tsukayama, J. K. (2006). *The Process of Investigation: Concepts and Strategies for Investigators in the Private Sector*. Butterworth-Heinemann Press.
- Serrano-Cinca, C., Gutiérrez-Nieto, B., & López-Palacios, L. (2015). Determinants of default in P2P lending. *PLoS One*, 10(10), 1–22. doi:10.1371/journal.pone.0139427 PMID:26425854
- Sethi, R. M., Ardener, S., & Burman, S. (1995). Women's ROSCAs in contemporary Indian society. In *Money-Go-Rounds: The Importance of Rotating Savings and Credit Associations for Women*. Berg.
- Shahrokhi, M. (2008). E-finance: Status, Innovations, Resources and Future Challenges. *Managerial Finance*, 34(6), 365–398. doi:10.1108/03074350810872787
- Shah, S. (2021). Compliance Monitoring and Testing Seismometer to Detect Compliquake. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Sharkey, N., & Fraser, J. (2017). Applying foreign anti-corruption law in the Chinese tax context: Conceptual difficulties and challenges. *eJournal of Tax Research*, 15(2), 312–332.
- Sharma, C., & Mitra, A. (2015). Corruption, governance and firm performance: Evidence from Indian enterprises. *Journal of Policy Modeling*, 37(5), 835–851. doi:10.1016/j.jpolmod.2015.05.001
- Sharma, M. (2008). *Management of financial institutions: with emphasis on bank and risk management*. PHI Learning Pvt. Ltd.
- Shen, J. (2017). *A review and comment on Guidelines for Fund Depository of Online Lending Information Intermediary Institutions*. Beijing: Huatai Securities. Retrieved from <https://www.htsc.com.cn>
- Sherman, L. (2000, July 15). Hedge fund investing 101. *Forbes*. Retrieved from <https://www.forbes.com/2000/07/15/feat.html#72a0f2e23994>
- Sidorov, J. (2015). Best practices for health outcomes public reporting. *Population Health Management*, 18(6), 399–401. doi:10.1089/pop.2015.0033 PMID:26091187

## Compilation of References

- Silva, M. de L. e. (2015). *A divulgação do risco nas demonstrações financeiras: uma análise ao anexo das sociedades não financeiras portuguesas*. ISCAL. Retrieved from <http://repositorio.ipl.pt/handle/10400.21/4619>
- Silva, A. R. M. (2014). *A divulgação da responsabilidade social empresarial nas empresas do PSI geral da Euronext Lisboa: Relatórios de sustentabilidade vs. divulgação online*. ISCAL.
- Silverstone, H., & Sheetz, M. (2007). *Forensic accounting and fraud investigation for Non-Experts*. John Wiley & Sons.
- Silverstone, H., Sheetz, M., Pedneault, S., & Rudewicz, F. (2004). *Forensic Accounting and Fraud Investigation for Non-experts*. Wiley.
- Simha, A., & Stachowicz-Stanusch, A. (2015). The effects of ethical climates on trust in supervisor and trust in organization in a Polish context. *Management Decision*, 53(1), 24–39. doi:10.1108/MD-08-2013-0409
- Simmel, G. (1990). *The Philosophy of Money*. Routledge.
- Simon, R. J. (1975). *The Contemporary Woman and Crime*. National Institute of Mental Health.
- Simser, J. (2014). Culpable insiders-the enemy within, the victim without. *Journal of Financial Crime*, 21(3), 310–320. doi:10.1108/JFC-11-2013-0068
- Singer, A. (2020, March 15). *French Court Moves the BTC Chess Piece — How Will Regulators Respond?* Retrieved from <https://cointelegraph.com/news/french-court-moves-the-btc-chess-piece-how-will-regulators-respond>
- Singh, D. B., & Panwar, S. (2017). Study of Effects of Demonetization on the Informal Economy of India. *International Journal of Engineering Technology, Management and Applied Sciences*, 5(5), 552–561.
- Singleton, T. W., Bologna, G. J., Lindquist, R. J., & Singleton, A. J. (2006). *Fraud Auditing and Forensic Accounting*. Wiley.
- Singleton, T. W., Singleton, A. J., Bologna, G. J., & Lindquist, R. J. (2006). *Fraud auditing and forensic accounting*. John Wiley & Sons.
- Singleton, T., & Flesher, D. L. (2003). A 25 years retrospective on the IIA's SAC project. *Managerial Auditing Journal*, 18(1), 39–53. doi:10.1108/02686900310454237
- Sinha, A. (2021). Fraud Risk Management in Banks: An Overview of Failures and Best Practices. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Sinha, S. (2017). Dark Web and Tor. In *Beginning Ethical Hacking with Python* (pp. 173–177). Apress. doi:10.1007/978-1-4842-2541-7\_26
- Skalak, S. L., Alas, M. A., & Sellitto, G. (2012). Fraud: an introduction. In T. W. Golden, S. L. Skalak, M. M. Clayton, & J. S. Pill (Eds.), *A guide to forensic accounting investigation* (pp. 1–23). John Wiley & Sons.
- Skousen, C. J., & Wright, C. J. (2008). Contemporaneous risk factors and the prediction of financial statement fraud. *SSRN Digital Library*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=938736](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=938736)
- Slemrod, J., Ur Rehman, O., & Waseem, M. (2019). *Pecuniary and Non-Pecuniary Motivations for Tax Compliance: Evidence from Pakistan* (Working Paper 19/08). Oxford: University of Oxford.
- Slemrod, J. (2007). Cheating ourselves: The economics of tax evasion. *The Journal of Economic Perspectives*, 21(1), 25–48. doi:10.1257/jep.21.1.25
- Sloane, W. (1994). Firm Offers Public Huge Returns, But Government Calls it Illegal. *The Christian Science Monitor*. Retrieved from <https://www.csmonitor.com/1994/0728/28091.html>

- Smith, G. S., & Crumbley, D. L. (2003). Defining a Forensic Audit. *The Journal of Digital Forensics, Security and Law*, 4(1), 61-80. Retrieved from <https://commons.erau.edu/jdfsl/vol4/iss1/3/>
- Smith, A. (1776). An Inquiry into the Nature and Causes of the Wealth of Nations. The Glasgow Edition of the Works and Correspondence of Adam Smith: Vol. 2. *An Inquiry into the Nature and Causes of the Wealth of Nations*. Oxford University Press. doi:10.1093/oseo/instance.00043218
- Smith, N., & Thomas, E. (2015). The Role of Foreign Direct Investment and State Capture in Shaping Innovation Outcome in Russia. *Europe-Asia Studies*, 67(5), 777–808. doi:10.1080/09668136.2015.1042430
- Smith, R. (2016). Of bad-seed, black-sheep and prodigal-sons. *International Journal of Entrepreneurial Behaviour & Research*, 22(1), 39–62. doi:10.1108/IJEBr-04-2014-0059
- Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber Criminals on trial*. Cambridge University Press. doi:10.1017/CBO9780511481604
- Snowden, E. (2015). Most Racist, Award Goes To ... Switzerland? *Skating on Stilts*. Retrieved from <https://www.skatingonstilts.com/skating-on-stilts/2015/03/and-the-edward-snowden-most-racist-award-goes-to-switzerland.html>
- Sodan, H. & Ziekow, J. (2005). *Grundkurs offentlichess Recht* [Basic course in public law]. Verlag C.H.Beck oHG.
- Soft Expert. (2018). Enterprise Asset Management. *Soft Expert*. Retrieved from <https://www.softexpert.com/solucao/enterprise-asset-management-eam/>
- Soltani, B. (2014). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals. *Journal of Business Ethics*, 120(2), 251–274. doi:10.1007/10551-013-1660-z
- Song, D. B., Lee, H. Y., & Cho, E. J. (2013). The association between earnings management and asset misappropriation. *Managerial Auditing Journal*, 28(6), 542–567. doi:10.1108/02686901311329919
- Song, Y., Cao, L., Wu, X., Wei, G., Ye, W., & Ding, W. (2012). Coupled behavior analysis for capturing coupling relationships in group-based market manipulations. *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, 976-984. 10.1145/2339530.2339683
- Spalevic, Z., & Ilic, M. (2017). The use of dark web for the purpose of illegal activity spreading. *Ekonomika, Journal for Economic Theory and Practice and Social Issues*, 63, 73-82.
- Spencer, E. (1977). White-collar criminals. *The Journal of Social Issues*, 33(4), 179–196. doi:10.1111/j.1540-4560.1977.tb02531.x
- Spencer, J. C. (1959). A study of incarcerated white-collar offenders. In G. Geis (Ed.), *White-collar Criminal: The Offender in Business and the Professions*. Atherton Press.
- Sriyalatha, M. A. K. (2019). The Impact of Corruption on Economic Growth: A Case Study of South Asian Countries. *Economic Research Journal*, 3(10), 35–47. doi:10.29226/TR1001.2020.161
- Stack, B. (2018, March 11). *Here's How Much Your Personal Information Is Selling for on the Dark Web*. Retrieved from <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>
- Stafford, P. (2017, September 15). What is MiFID II and how will it affect EU's financial industry? *Financial Times*. Retrieved from <https://www.ft.com/content/ae935520-96ff-11e7-b83c-9588e51488a0>
- Stanbury, J., & Paley-Menzies, C. (2010). Forensic futurama: Why forensic accounting is evolving. *AICPA Store*, 28.

## Compilation of References

- Stearns, L. B., & Allan, K. D. (1996). Economic behavior in institutional environments: The corporate merger wave of the 1980s. *American Sociological Review*, 61(4), 699–718. doi:10.2307/2096400
- Stempel, J. (2019). UBS must defend against U.S. lawsuit over ‘catastrophic’ mortgage losses. *Yahoo Finance*. Retrieved from <https://finance.yahoo.com/news/ubs-must-defend-against-u-214743943.html>
- Stewart, J. B. (1992). *Den of Thieves*. Simon and Schuster.
- Stewart, J., & Dawson, M. (2018). How the modification of personality traits leave one vulnerable to manipulation in social engineering. *International Journal of Information Privacy. Security and Integrity*, 3(3), 187–208.
- Stiglitz, J. E., & Weiss, A. (1981). Credit rationing in markets with imperfect information. *The American Economic Review*, 71(3), 393–410.
- Straney, L. L. (2011). *Securities Fraud: Detection, Prevention, and Control*. Wiley.
- Strauss, P. L. (2002). *Administrative justice in the United States*. Carolina Academic Press.
- Strumeyer, G., & Swammy, S. (2017). *The Capital Markets: Evolution of the Financial Ecosystem*. Wiley. doi:10.1002/9781119220589
- Stupples, B., Sazonov, A., & Woolley, S. (2019, July 26). UBS Whistle-Blower Hunts Trillions Hidden in Treasure Isles. *Bloomberg*. Retrieved from <https://www.bloomberg.com/news/articles/2019-07-26/ubs-whistle-blower-hunts-trillions-hidden-in-treasure-islands>
- Sujit, S. (2019). A Research on Cyber Security Awareness based on Big Data. *International Journal of Recent Technology and Engineering*, 8(2S8, 2SA), 1798–1802. doi:10.35940/ijrte.B1156.0882S819
- Sukhai, N. (2004). Hacking and Cybercrime. In *1st Annual Conference on Information Security Curriculum Development* (pp. 128–132). ACM Press. 10.1145/1059524.1059553
- Sumah, S. (2018). Corruption, causes and consequences, trade and global market. In *Trade and Global Market*. Retrieved from <https://www.intechopen.com/books/trade-and-global-market/corruption-causes-and-consequences>
- Sung, M. J., Awasthi, R., & Lee, H. C. (2017). Can Tax Incentives for Electronic Payments Curtail the Shadow Economy? Korea’s Attempt to Reduce Underreporting in Retail Businesses. *Korean Journal of Policy Studies*, 32(2), 85–134.
- Sun, Y., & Johnston, M. (2009). Does democracy check corruption? Insights from China and India. *Comparative Politics*, 42(1), 1–19. doi:10.5129/001041509X12911362972719
- Supreme Court of India. (2013, April 26). N. Narayanan versus Adjudicating Officer, Sebi, K.S. Radhakrishnan and Dipak Misra, JJ. Civil Appeal Nos. 4112–4113 of 2013 D.No. 201 of 2013.
- Suryanto, T., & Ridwansyah, R. (2016). The Shariah financial accounting standards: How they prevent fraud in Islamic banking. *European Research Studies*, XIX(4), 140–157. doi:10.35808/ersj/587
- Suryono, R. R., Purwandari, B., & Budi, I. (2019). Peer to Peer (P2P) Lending Problems and Potential Solutions: A Systematic Literature Review. *Procedia Computer Science*, 161(15), 204–214. doi:10.1016/j.procs.2019.11.116
- Sutherland, E. H. (1945). Is “white collar crime” crime? *American Sociological Review*, 10(2), 132–139.
- Sutherland, E. H. (1939). White-Collar Criminality. *American Sociological Review*, 5(1), 1–12. doi:10.2307/2083937
- Sutherland, E. H. (1983). *White collar crime: The uncut version*. Yale University Press.

- Swain, S., & Pani, L. K. (2016). Frauds in Indian banking: Aspects, reasons, trend-analysis and suggestive measures. *International Journal of Business and Management Invention*, 5(7), 1–9.
- Swamy, A., Knack, S., Lee, Y., & Azfar, O. (2001). Gender and corruption. *Journal of Development Economics*, 64(1), 25–55. doi:10.1016/S0304-3878(00)00123-1
- Swanepoel, B., & Meiring, J. (2017). Morality associated with fraud, corruption and tax evasion in South Africa. *eJournal of Tax Research*, 15(2), 333-358.
- Swierczynska, J. (2016). The Reduction of Barriers in Customs as One of the Measures Taken by the Customs Service in the Process of Ensuring Security and Safety of Trade. *Studia Ekonomiczne*, 266, 212–222.
- Swinhoe, D. (2020, April 17). The 15 biggest data breaches of the 21st century. *CSO Online*. Retrieved from <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>
- Swissinfo. (2019). Swiss launch committee on slavery reparations. *Swissinfo*. [https://www.swissinfo.ch/eng/history-\\_swiss-launch-committee-on-slavery-reparations-/45421506](https://www.swissinfo.ch/eng/history-_swiss-launch-committee-on-slavery-reparations-/45421506)
- Taboada, C. (2015). OECD Base Erosion and Profit Shifting Action 6: The General Anti-Abuse Rule. *Bulletin for International Taxation*, 69(10), 602–608.
- Tagliabue, J. (1986). The Swiss stop keeping secrets. *The New York Times*. Retrieved from <https://www.nytimes.com/1986/06/01/business/the-swiss-stop-keeping-secrets.html>
- Tahat, Y., Omran, M. A., & AbuGhazaleh, N. M. (2018). Factors affecting the development of accounting practices in Jordan: An institutional perspective. *Asian Review of Accounting*, 26(4), 464–486. doi:10.1108/ARA-01-2017-0010
- Tajpour, A., & Zamani, M. (2020). Identity Theft and Prevention. In *Information Security and Optimization* (pp. 25–42). Chapman and Hall/CRC. doi:10.1201/9781003045854-3
- Takim, R., Ismail, K., Nawawi, A. H., & Jaafar, A. (2009). The Malaysian private finance initiative and value for money. *Asian Social Science*, 5(3), 103–111. doi:10.5539/ass.v5n3p103
- Taleb, N. (2007). *The Black Swan-The Impact of the Highly Improbable*. The Random House.
- Tamersoy, A. (2016). *Graph-based algorithms and models for security, healthcare, and finance* [Unpublished Doctoral dissertation]. Georgia Institute of Technology.
- Tamersoy, A., Xie, B., Lenkey, S. L., Routledge, B. R., Chau, D. H., & Navathe, S. B. (2013). Inside insider trading: Patterns & discoveries from a large scale exploratory analysis. In *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (pp. 797-804). Retrieved from <https://ieeexplore.ieee.org/document/6785794>
- Tang, J., & Karim, K. E. (2018). Financial fraud detection and big data analytics – implications on auditors’ use of fraud brainstorming session. *Managerial Auditing Journal*, 34(3), 324–337. doi:10.1108/MAJ-01-2018-1767
- Tanzi, V. (1998). Corruption Around the World: Causes, Consequences, Scope and Cures (IMF WP/98/63). Washington, DC: International Monetary Fund.
- Tanzi, V. (1998). *Corruption Around the World: Causes, Consequences, Scope, and Cures* (IMF Working Papers, 98(63)). International Monetary Fund.
- Tanzi, V. (2017). Corruption, complexity and tax evasion. *eJournal of Tax Research*, 15(2), 144.

## Compilation of References

- Tanzi, V. (1998). *Corruption around the world: Causes, consequences, cope, and cures (WP/98/64s)*. International Monetary Fund.
- Tanzi, V., & Davoodi, H. (1998). *Corruption, Public Investment, and Growth. The Welfare State, Public Investment, and Growth*. Springer. doi:10.1007/978-4-431-67939-4\_4
- Tasca, P. (2015). *Digital Currencies: Principles, Trends, Opportunities, and Risks* (ECUREX Research Working Paper). Retrieved from [https://faculty.fuqua.duke.edu/~charvey/Teaching/898\\_2016/Readings/Tasca.pdf](https://faculty.fuqua.duke.edu/~charvey/Teaching/898_2016/Readings/Tasca.pdf)
- TaskinsoyJ. (2020). From Primitive Barter to Inflationary Dollar: A Warless Economic Weapon of Mass Destruction. doi:10.2139srn.3542145
- Tavani, H. T. (2000). Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace. *ACM SIGCAS Computers and Society*, 30(3), 3–9. doi:10.1145/572241.572242
- Tengvall, M., & Claesson, G. (2015). *Peer-to-peer lending: the effects of institutional involvement social lending* (Master's thesis, Jönköping University). Retrieved from <https://www.diva-portal.org/smash/get/diva2:812631/FULLTEXT01.pdf>
- Tennant, D. (2011). Why do people risk exposure to Ponzi schemes? Econometric evidence from Jamaica. *Journal of International Financial Markets, Institutions and Money*, 21(3), 328–346. doi:10.1016/j.intfin.2010.11.003
- Tennessee Bar Association. (2009). *Internet Scams Target Attorneys*. Retrieved from <http://www.tba2.org/tbatoday/2009/TBAtoday06-09-2009.htm>
- Teoh, T., Lim, W. T., & Nguwi, Y. Y. (2019). From Technical Analysis to Text Analytics: Stock and Index Prediction with GRU. In *IEEE International Conference on Cybernetics and Intelligent Systems and IEEE Conference on Robotics, Automation and Mechatronics*, (pp. 496-500). Bangkok: IEEE.
- Thaker, M. A. M. (2018). A qualitative inquiry into cash waqf model as a source of financing for micro enterprises. *ISRA International Journal of Islamic Finance*, 10(1), 19–35. doi:10.1108/IJIF-07-2017-0013
- The Local Government (Amendment) Act 2006
- The Local Government (Public Procurement and Disposal of Public Assets) Regulations, 2006
- The Local. (2017). SVP ad ruled racist by Swiss supreme court. *The Local*. <https://www.thelocal.ch/20170413/svp-ad-ruled-racist-by-swiss-supreme-court>
- The Open Group. (2011). *Architecture Development Method*. The Open Group. Retrieved from <https://pubs.opengroup.org/architecture/togaf9-doc/arch/chap05.html>
- The PPDA Amendment Bill 2019
- The Public Procurement and Disposal of Public Assets (Amendment) Act, 2011
- The Public Procurement and Disposal of Public Assets Act 2003
- The Public Procurement and Disposal of Public Assets Regulations, 2014
- The UN Practitioner's Handbook (2006)
- The Verge. (2020). Retrieved from <https://www.theverge.com/>
- The World Bank. (2020). *World Development Indicators*. DataBank. Retrieved from <https://databank.worldbank.org/source/world-development-indicators#>



- Thomas, B., Clergue, J., Schaad, A., & Dacier, M. (2004). *A comparison of conventional and online fraud*. SAP Research, Sophia Antipolis, France. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.194.1307&rep=rep1&type=pdf>
- Thompson, J. K., & Choi, S. M. (2001). *Governance systems for collective investment schemes in OECD countries* (Occasional paper No. 1). OECD. Retrieved from [http://www.energytoolbox.org/library/infra2007/references/environmental\\_issues+compliance/Governance\\_Systems\\_for\\_Collective\\_Investment\\_Schemes.pdf](http://www.energytoolbox.org/library/infra2007/references/environmental_issues+compliance/Governance_Systems_for_Collective_Investment_Schemes.pdf)
- Thomson Reuters. (2020). *Markets in Financial Instruments Directive*. Retrieved from <https://www.thomsonreuters.com/en.html>
- Thornton, G. (2014). *Alternative lending: a regulatory approach to peer-to-peer lending*. Academic Press.
- TI. (2012). *Center Point Group – Georgia’s Biggest Construction Scandal*. Transparency International.
- Timofeyev, Y. (2015). Analysis of predictors of organizational losses due to occupational corruption. *International Business Review*, 24(4), 630–641. doi:10.1016/j.ibusrev.2014.11.007
- Tinder. (n.d.). *What is Photo Verification?* Retrieved from <https://www.help.tinder.com/hc/en-us/articles/360034941812-What-is-Photo-Verification->
- Tiwari, R., Anjum, B., Chand, K., & Pathak, R. (2017). An exploratory study of unethical practices in financial services in India. *International Research Journal of Management and Commerce*, 4(7), 219–228.
- Toch, H. (1979). *The Psychology of Crime and Criminal Justice*. Holt, Rinehart and Winston.
- Tolstikova, N. (1999). *Mmm As a Phenomenon of the Russian Consumer Culture*. ACR European Advances, E-04. <https://www.acrwebsite.org/volumes/11384/volumes/e04/E-04/full>
- Tomohara, A., Lee, H. J., & Lee, S. (2012). Did FIN 48 increase companies’ tax payments? Trade-off between disclosure and tax burdens. *Applied Economics*, 44, 4239–4248. doi:10.1080/00036846.2011.587789
- Torgler, B., & Schneider, F. (2007). *Shadow economy, tax morale, governance and institutional quality: a panel analysis* (Working Paper, No. 1923). Center for Economic Studies and ifo Institute (CESifo), Munich. Retrieved from <https://www.econstor.eu/bitstream/10419/25968/1/538033703.PDF>
- Torgler, B., & Valev, N. T. (2010). Gender and public attitudes toward corruption and tax evasion. *Contemporary Economic Policy*, 28(4), 554–568. doi:10.1111/j.1465-7287.2009.00188.x
- Tosoni, L. (2018). Rethinking Privacy in the Council of Europe’s Convention on Cybercrime. *Computer Law & Security Review*, 34(6), 1197–1214. doi:10.1016/j.clsr.2018.08.004
- Trad, A., & Kalpić, D. (2018c). The Business Transformation Framework and Enterprise Architecture Framework for Managers in Business Innovation. The role of legacy processes in automated business environments. *The Proceedings of E-LEADER 2017 Berlin, 1*.
- Trad, A. (2019). The Business Transformation and Enterprise Architecture Framework Applied to Analyze the Historically Recent Rise and the 1975 Fall of the Lebanese Business Ecosystem. In E. A. Nyam & A. H. Tunde (Eds.), *Impacts of Violent Conflicts on Resource Control and Sustainability* (pp. 75–108). IGI Global. doi:10.4018/978-1-5225-5987-0.ch004
- Trad, A. (2019c). *Using Google analytics to determine the leading business transformation framework that are based on enterprise architecture*. IBISTM.
- Trad, A. (2020). *The Business Transformation Framework and Enterprise Architecture Framework-The Financial Control and Technology Concept (FCTC)*. IGI Global.

## Compilation of References

- Trad, A., & Kalpić, D. (2016). The Business Engineering Transformation Framework for (e)commerce Architecture-Modelling Projects. In I. Lee (Ed.), *Encyclopaedia of E-Commerce Development, Implementation, and Management*. IGI Global. doi:10.4018/978-1-4666-9787-4.ch052
- Trad, A., & Kalpić, D. (2018a). The Business Transformation and Enterprise Architecture Framework: The Financial Engineering Technology Concept. In B. Sergi, F. Fidanoski, M. Ziolo, & V. Naumovski (Eds.), *Regaining Global Stability After the Financial Crisis* (pp. 23–45). IGI Global. doi:10.4018/978-1-5225-4026-7.ch002
- Trad, A., & Kalpić, D. (2018b). The Business Transformation Framework and Enterprise Architecture Framework for Managers in Business Innovation: The Role of Cyber and Information Technology Security in Automated Business Environments. In B. Christiansen & A. Piekarz (Eds.), *Global Cyber Security Labor Shortage and International Business Risk* (pp. 19–37). IGI Global.
- Trad, A., & Kalpić, D. (2019). The Business Transformation Framework and its Business Engineering Law support for (e) transactions. In M. Khosrow-Pour (Ed.), *Advanced Methodologies and Technologies in Business Operations and Management* (pp. 230–246). IGI Global. doi:10.4018/978-1-5225-7362-3.ch017
- Trad, A., & Kalpić, D. (2020). *Using Applied Mathematical Models for Business Transformation*. IGI Global. doi:10.4018/978-1-7998-1009-4
- Trading Economics. (2017a). *Switzerland - GDP Annual Growth Rate*. Trading Economics. Retrieved from <http://www.tradingeconomics.com/>
- Trading Economics. (2017b). *Lebanon - GDP Annual Growth Rate*. Trading Economics. Retrieved from <http://www.tradingeconomics.com/>
- Trading Economics. (2017c). *Switzerland's currency evolution*. Trading Economics. Retrieved from <http://www.trading-economics.com/>
- Trading Economics. (2017d). *Lebanon's currency evolution*. Trading Economics. Retrieved from <http://www.trading-economics.com/>
- Trahan, A., Marquart, J. W., & Mullings, J. (2005). Fraud and the American dream: Toward an understanding of fraud victimization. *Deviant Behavior*, 26(6), 601–620. doi:10.1080/01639620500218294
- Treisman, D. (2000). The causes of corruption: A cross-national study. *Journal of Public Economics*, 76(3), 399–457. doi:10.1016/S0047-2727(99)00092-4
- Tribune de Genève. (2014, September 14). Pour Christian Levrat, l'UDC est sur la voie du fascisme [For Christian Levrat, the SVP is on the path to fascism]. *Tribune de Geneve*. Retrieved from <https://www.lematin.ch/story/pour-christian-levrat-l-udc-est-sur-la-voie-du-fascisme-345254850803>
- Trompeter, G., Carpenter, T., Desai, N., Jones, K., & Riley, D. Jr. (2013). A synthesis of fraud related research. *Auditing*, 32(1), 287–321. doi:10.2308/ajpt-50360
- Trompeter, G., Carpenter, T., Jones, K., & Riley, D. Jr. (2014). Insights for research and practice: What we learn about fraud from other disciplines. *Accounting Horizons*, 28(4), 769–804. doi:10.2308/acch-50816
- Trusov, M., Bucklin, R. E., & Pauwels, K. (2009). Effects of word-of-mouth versus traditional marketing: Findings from an internet social networking site. *Journal of Marketing*, 73(5), 90–102. doi:10.1509/jmkg.73.5.90
- Tsakatika, M. (2016). SYRIZA's electoral rise in Greece: Protest, trust and the art of political manipulation. *South European Society & Politics*, 21(4), 519–540.

- Tsakumis, G. T., Curatola, A. P., & Porcano, T. M. (2007). The relation between national cultural dimensions and tax evasion. *Journal of International Accounting, Auditing & Taxation*, 16(2), 131–147. doi:10.1016/j.intaccudtax.2007.06.004
- Tu, L. (2017). Commercial banks' involvement in P2P lending: present dilemma and response. *Financial Market*, 555, 56–59.
- U.S. Court of Appeals. Second Circuit. (2012). *Gibbons v. Malone*. Retrieved from [https://scholar.google.com/scholar\\_case?case=13272908530594532132&q=Gibbons+v.+Malone&hl=en&as\\_sdt=6,32&as\\_vis=1](https://scholar.google.com/scholar_case?case=13272908530594532132&q=Gibbons+v.+Malone&hl=en&as_sdt=6,32&as_vis=1)
- U.S. Office of the Press Secretary. (2020, April 6). Remarks by President Trump, Vice President Pence, and members of the Coronavirus Task Force in press briefing. *White House*. Retrieved from <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-vice-president-pence-members-coronavirus-task-force-press-briefing-21/>
- U4. (2020). *Review of the literature on the link between corruption, poverty and conflict, and evidence on the impact of corruption on donor interventions*. Oslo: U4 Anti-Corruption Resource Centre. Retrieved from <https://www.u4.no/publications>
- UK Metropolitan Police Authority. (2007, January 25). *Progress of MPS E-crime Strategy*. Retrieved from <http://policeauthority.org/metropolitan/committees/mpa/2007/070125/10/index.html>
- Umar, U. H., & Kurawa, J. M. (2019). Business succession from an Islamic accounting perspective. *ISRA International Journal of Islamic Finance*, 11(2), 267–281. <https://DOI.org/10.1108/IJIF-06-2018-0059>
- Umar, U. H., Ado, M. B., & Ayuba, H. (2019). Is religion (interest) an impediment to Nigeria's financial inclusion targets by the Year 2020? A qualitative inquiry. *Qualitative Research in Financial Markets*, 12(3), 283–300. <https://DOI.org/10.1108/QRFM-01-2019-0010>
- Umar, M. A., Derashid, C., Ibrahim, I., & Bidin, Z. (2019). Public governance quality and tax compliance behavior in developing countries: The mediating role of socioeconomic conditions. *International Journal of Social Economics*, 46(3), 338–351. doi:10.1108/IJSE-11-2016-0338
- Umar, U. H. (2017). The relevance of accounting profession in Islamic inheritance. *Bayero International Journal of Accounting Research*, 11(1), 414–430.
- Umar, U. H. (2019). Integrating family *waqf* into an inheritable going concern business: an instrument for the sustainable welfare of exempted heirs. In K. M. Ali, M. K. Hassan, & A. E. S. Ali (Eds.), *Revitalization of Waqf for Socio-Economic Development* (Vol. 2, pp. 87–87). Springer. doi:10.1007/978-3-030-18449-0\_4
- Umar, U. H. (2020). The business financial inclusion benefits from an Islamic point of view: A qualitative inquiry. *Islamic Economic Studies*, 28(1), 83–100. doi:10.1108/IES-09-2019-0030
- Umar, U. H., & Haron, M. H. (2021). (Accepted). The Islamic need for investing inherited wealth and accounting treatments. *The Journal of Muamalat and Islamic Finance Research*.
- Umar, U. H., Kademi, T. T., & Haron, M. H. (2020). Integrating waqf and business: Ensuring business sustainability for the welfare of heirs and non-heirs. *International Journal of Economic. Management and Accounting*, 28(1), 191–213.
- UN. (2018). *Global Cost of Corruption at Least 5 Per Cent of World Gross Domestic Product* (8346<sup>th</sup> meeting of Security Council). Retrieved from <https://www.un.org/press/en/2018/sc13493.doc.htm>
- UN. (2020). *Money-Laundering and Globalization*. United Nations. Retrieved from <https://www.unodc.org/unodc/en/money-laundering/globalization.html>

## Compilation of References

- UNDP. (2008). *Tackling Corruption, Transforming Lives – Accelerating Human Development in Asia and the Pacific* (Human Development Report, UNDP). Retrieved from <http://hdr.undp.org/en/content/tackling-corruption-transforming-lives>
- UNECE. (2003). Progress in Systemic Reforms in the CIS. In *Economic Survey of Europe* (pp. 123–154). United Nations Economic Commission for Europe.
- Ungureanu, D., & Dascalu, E.-D. (2015). Improving VAT Compliance in Romania by Implementing a New Tool – Tax Lottery Receipts. *Journal of Economic Development, Environment and People*, 4(4), 47–57.
- United States of America (For the Federal Trade Commission), v. Kohl's Department Stores, Inc., No. 2:20-cv-859.* (2020). E.D. Wisc.
- United States v. Cioni*, 649 F.3d 276, 282 (4th Cir. 2011)
- Universität St. Gallen. (2015). *EMBA in Financial engineering*. Executive School of Universität St. Gallen. Retrieved from <https://www.unisg.ch/>
- UNODC. (2017). *Corruption in Nigeria, Bribery: public experience and response*. United Nations Office on Drugs and Crime. Retrieved from [https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Nigeria/Corruption\\_Nigeria\\_2017\\_07\\_31\\_web.pdf](https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Nigeria/Corruption_Nigeria_2017_07_31_web.pdf)
- USA v. Robel*, 389 US 258 (1967).
- USDOJ. (2004). *Report from the Field: The USA Patriot Act at Work*. U.S. Department of Justice.
- USDOJ. (2016, September 23). *ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison*. U.S. Department of Justice. Récupéré sur Retrieved from <https://www.justice.gov/usao-edva/pr/isil-linked-hacker-sentenced-20-years-prison>
- USDOJ. (2018, August 1). *Three Members of Notorious International Cybercrime Group “Fin7” In Custody for Role in Attacking Over 100 U.S. companies*. U.S. Department of Justice. Retrieved from <https://perma.cc/KMS2-9UQT>
- US-SEC. (2014). *Administrative Proceedings File No. 3-16199*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/admin/2014/34-73369.pdf>
- US-SEC. (2018). *Administrative Proceedings File No. 3-18887*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/admin/2018/33-10572.pdf>
- US-SEC. (2020a). *Market Manipulation*. United States Securities and Exchange Commission. Retrieved from <https://www.investor.gov/>
- US-SEC. (2020b). *Administrative Proceeding File No. 3-16316*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/apdocuments/3-16316-event-6.pdf>
- US-SEC. (2020c). *Pump and Dump Schemes*. United States Securities and Exchange Commission. Retrieved from <https://www.investor.gov/protect-your-investments/fraud/types-fraud/pump-and-dump-schemes>
- US-SEC. (2020d). *Litigation Complaints*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/litigation/complaints/2020/comp24832.pdf>
- US-SEC. (2020e). *Insider Trading*. United States Securities and Exchange Commission. Retrieved from <https://www.sec.gov/>
- Utt, R. (2008). The Subprime Mortgage Market Collapse: A Primer on the Causes and Possible Solutions. *Heritage Foundation*. Retrieved from <https://www.heritage.org/report/the-subprime-mortgage-market-collapse-primer-the-causes-and-possible-solutions>

- Uyumez, M. E. (2016). Vergi mevzuatının karmaşıklığı ve uzlaşma yöntemi bağlamında vergi uyumunun değerlendirilmesi [Assessing tax compliance in the context of the complexity of tax legislation and method of settlement]. *Ekonomi Bilimleri Dergisi*, 8(1), 75–92.
- Van der Toorn, J., Feinberg, M., Jost, J. T., Kay, A. C., Tyler, T. R., Willer, R., & Wilmuth, C. (2015). A sense of powerlessness fosters system justification: Implications for the legitimization of authority, hierarchy, and government. *Political Psychology*, 36(1), 93–110. doi:10.1111/pops.12183
- Van Duren, E. C. G. J. (2010). Money is ammunition; don't put it in the wrong hands. A view on COIN contracting from Regional Command South. *Militaire Spectator*, 179(11), 564–578.
- Van Gelder, J. L., & De Vries, R. E. (2016). Traits and states at work: Lure, risk and personality as predictors of occupational crime. *Psychology, Crime & Law*, 22(7), 701–720. doi:10.1080/1068316X.2016.1174863
- van Wegberg, R., Oerleman, J.-J., & van Deventer, O. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 25(2), 419–435. doi:10.1108/JFC-11-2016-0067
- Vasquez, M. H. (2017). The Financial Crimes Management of Account Takeover Fraud. *The University of Texas*. Retrieved from <https://repositories.lib.utexas.edu/bitstream/handle/2152/63762/VASQUEZ-MASTERSREPORT-2017.pdf>
- Vatis, M. (2010). The Council of Europe Convention on Cybercrime. In *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy* (pp. 207–223). Washington, DC: The National Academies Press.
- Veit, A. (2019). Swimming upstream: leveraging data and analytics for taxpayer engagement – an Australian and international perspective. *eJournal of Tax Research*, 16(3), 478.
- Venâncio, R. (2012a, January 4). Mais empresas podem seguir Jerónimo Martins. *Diário Económico*. Retrieved from <http://economico.sapo.pt/noticias/nprint/135089>
- Venâncio, R. (2012b, January 4). Marca Pingo Doce pode sofrer danos de reputação. *Económico*. Retrieved from <http://economico.sapo.pt/noticias/nprint/135087>
- Venter, A. (2007). A procurement fraud risk management model. *Meditari Accountancy Research*, 15(2), 77–93. doi:10.1108/10222529200700012
- Verizon. (2020). *2020 Data Breach Investigations Report*. Retrieved from <https://enterprise.verizon.com/resources/reports/dbir/>
- Verstein, A. (2011). The Misregulation of Person-to-Person Lending. *University of California Davis Law Review*, 45(2), 445–530.
- Victor, B., & Cullen, J. B. (1988). The organizational bases of ethical work climates. *Administrative Science Quarterly*, 33(1), 101–125. doi:10.2307/2392857
- Vinten, G. (2004). The future of UK internal audit education: Secularisation and submergence? *Managerial Auditing Journal*, 19(5), 580–596. doi:10.1108/02686900410537810
- Vousinas, G. (2016). The critical role of Internal Auditing in addressing bank fraud: A conceptual framework. *International Journal of Case Studies*, 5(3), 67–81.
- Vousinas, G. (2017). Shadow economy and tax evasion: The Achilles heel of Greek economy. Determinants, effects and policy proposals. *Journal of Money Laundering Control*, 20(4), 386–404.

## Compilation of References

- Vousinas, G. L. (2019). Advancing theory of fraud: The SCORE model. *Journal of Financial Crime*, 26(1), 372–381. doi:10.1108/JFC-12-2017-0128
- Vrij, A., Hope, L., & Fisher, R. P. (2014). Eliciting reliable information in investigative interviews. *Policy Insights from the Behavioral and Brain Sciences*, 1(1), 129–136. doi:10.1177/2372732214548592
- Vu, T. T., Chang, S., Ha, Q. T., & Collier, N. (2012). An experiment in integrating sentiment features for tech stock prediction in twitter. *Workshop on Information extraction and entity analytics on social media data*, 23–38.
- Wachs, J., Yasseri, T., Lengyel, B., & Kertész, J. (2019). Social capital predicts corruption risk in towns. *Royal Society Open Science*, 6(4), 182103. doi:10.1098/rsos.182103 PMID:31183137
- Wadhwa, L., & Pal, V. (2012). Forensic Accounting and Fraud Examination in India. *International Journal of Applied Engineering Research: IJAER*, 7(11), 1–4.
- Walker-Munro, B. (2019a). Regulating Disruption and Development of the Disruption Calculus. *University of Western Australia Law Review*, 46(1), 111–143.
- Walker-Munro, B. (2019b). Disruption, regulatory theory and China: What surveillance and profiling can teach the modern regulator. *Journal of Governance and Regulation*, 8(2), 23–40.
- Walker-Munro, B. (2020). A Case for Systemic Design in Criminal Law Techno-Regulation. *Criminal Law Journal*, 43(5), 306–324.
- Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Wiley.
- Wall, D. (2016). Cybercrimes New wine, no bottles? In P. Davies, P. Francis, & V. Jupp (Eds.), *Invisible crimes: their victims and their regulation*. Springer.
- Wall, J. (2019). Where to Prosecute Cybercrimes. *Duke Law & Technology Review*, 17, 146–161.
- Wang, J., & Huang, Y. (2017). Field Study Report on American Financial Technology. Institution of Digital Finance, Peking University & Shanghai Finance Institute.
- Wang, J. G., Xu, H., & Ma, J. (2015). *Financing the Underfinanced*. Springer. doi:10.1007/978-3-662-46525-7
- Wang, P. (2013). The rise of the Red Mafia in China: A case study of organised crime and corruption in Chongqing. *Trends in Organized Crime*, 16(1), 49–73. doi:10.1007/12117-012-9179-8
- Wang, P., Zheng, H., Chen, D., & Ding, L. (2015). Exploring the critical factors influencing online lending intentions. *Financial Innovation*, 1(1), 1–11. doi:10.1186/40854-015-0010-9
- Wang, W., & Steinberg, M. (2010). *Insider Trading*. Oxford University Press.
- Warren, N. (2019). Estimating tax gap is everything to an informed response to the digital era. *eJournal of Tax Research*, 16(3), 536–546.
- Warren, J. D. Jr, Moffitt, K. C., & Byrnes, P. (2015). How Big Data Will Change Accounting. *Accounting Horizons*, 29(2), 397–407. doi:10.2308/acch-51069
- Warren, L. (2012). Scenario analysis for S&OP. *The Journal of Business Forecasting*, 31(1), 32–35.
- Watters, M., Casey, K. M., Humphrey, J., & Linn, G. (2007). CPA Firms Offering of Forensic Services Surprisingly Consistent Over Time: Are CPA's Missing Out on A Forensic Accounting Gold Rush. *Academy of Accounting and Financial Studies Journal*, 11(2), 89–95.

- WEC Carolina Energy Solutions LLC v. Miller, 687 F. 3d 199 (4th Cir. 2012)
- Weerman, F. (2003). Co-offending as social exchange explaining: Explaining characteristics of co-offending. *British Journal of Criminology*, 43(2), 398–416. doi:10.1093/bjc/43.2.398
- Wei, Q., & Zhang, Q. (2016). P2P Lending Risk Contagion Analysis Based on a Complex Network Model. *Discrete Dynamics in Nature and Society*, SI, 1-8. doi:10.1155/2016/5013954
- Wei, S.-J. (1999). *Corruption in economic development beneficial grease, minor annoyance, or major obstacle?* (Working Paper No. 2048). World Bank Group. Retrieved from <https://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-2048>
- Wei, T. (2015). *New development of credit reference: new era for P2P lending*. Boston: BOC International. Retrieved from <http://www.bocintl.com/en/>
- Wei, S. (2000). How Taxing is Corruption on International Investors? *The Review of Economics and Statistics*, 82(1), 1–11. doi:10.1162/003465300558533
- Wei, S. (2015). Internet lending in China: Status quo, potential risks and regulatory options. *Computer Law & Security Review*, 31(6), 793–809. doi:10.1016/j.clsr.2015.08.005
- Weisburd, D., & Waring, E. (2001). *White-collar crime and criminal careers*. Cambridge University Press. doi:10.1017/CBO9780511499524
- Weisburd, S. (1992). The problem of white-collar crime motivation. In K. Schlegel & D. Weisburd (Eds.), *White collar Crime Reconsidered*. Northeastern University Press.
- Weiss, D. C. (2009). Bradley Arant Reportedly Scammed Out of More Than \$400K. *ABA Journal*. Retrieved from [https://www.abajournal.com/news/article/bradley\\_arant\\_reportedly\\_scammed\\_out\\_of\\_more\\_than\\_400k](https://www.abajournal.com/news/article/bradley_arant_reportedly_scammed_out_of_more_than_400k)
- Weiss, G. N. F., Pelger, K., & Horsch, A. (2010). *Mitigating Adverse Selection in P2P Lending – Empirical Evidence from Prosper.com*. Retrieved from [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1650774](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1650774)
- Wells, J. T. (2011, October 1). The Fraud examiners. *Sleuthing Carrier bring CPA's Personal and Satisfaction, Journal of Accountancy*. Retrieved from <https://www.journalofaccountancy.com/issues/2003/oct/thefraudexaminers.html>
- Wells, H. (2002). The Cycles of Corporate Social Responsibility: An Historical Retrospective for the Twenty-First Century. *Kansas Law Review*, 51, 77–170.
- Wen, J., Zheng, M., Feng, G. F., Chen, S. W., & Chang, C. P. (2020). Corruption and innovation: Linear and nonlinear investigations of OECD countries. *The Singapore Economic Review*, 65(01), 103–129. doi:10.1142/S0217590818500273
- West, J., Bhattacharya, M., & Islam, R. (2014). Intelligent Financial Fraud Detection Practices: An Investigation. *Computers & Security*, 57, 47–66. doi:10.1016/j.cose.2015.09.005
- Westphal, C. (2008). *Data Mining for Intelligence, Fraud & Criminal Detection: Advanced Analytics & Information Sharing Technologies*. CRC Press. doi:10.1201/9781420067248
- Westphal, C., & Blaxton, T. (1998). *Data mining solutions: Methods and tools for solving real-world problems*. John Wiley & Sons, Inc.
- Wetsman, N. (2020, September 17). Woman dies during a ransomware attack on a German hospital. *The Verge*. Retrieved from: <https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity>
- Whiteman, J. R., III. (2017). *Social engineering: Humans are the prominent reason for the continuance of these types of attacks* (Doctoral dissertation). Utica College.

## Compilation of References

- White, R. M. (2020). Insider Trading: What Really Protects US Investors? *Journal of Financial and Quantitative Analysis*, 55(4), 1305–1332. doi:10.1017/S0022109019000292
- Wilkins, A. M., Acuff, W. W., & Hermanson, D. R. (2012). Understanding a Ponzi scheme: Victims' perspectives. *Journal of Forensic and Investigative Accounting*, 4(1), 1–19.
- Wilks, T. J., & Zimbelman, M. F. (2002). The Effects of a Fraud-Triangle Decomposition of Fraud Risk Assessments on Auditors' Sensitivity to Incentive and Opportunity Cues. *Proceedings of the 15th University of Illinois Symposium on Auditing Research*.
- Wilson, C. (2008, January 29). *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*” CRS Report for Congress, 2008, Order Code RL32114. Retrieved from <https://fas.org/sgp/crs/terror/RL32114.pdf>
- Wilson, E. (2017). Point of No Return. *EY Tax Insights*, 17, 46–48.
- Wilson, H. E., Francis, O., Emeka, E. E., & Loraver, T. N. (2017). Fraud and forensic accounting education: Prospects and challenges in Nigeria. *International Journal of Business and Management*, 12(7), 146–161. doi:10.5539/ijbm.v12n7p146
- Witt, H. (1994). Russian investors entered stock scheme with eyes wide open. *Chicago Tribune*. Retrieved from <https://www.chicagotribune.com/news/ct-xpm-1994-07-31-9407310366-story.html>
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.
- Wolfson, R. (2018, December 15). Tracing Illegal Activity through the Bitcoin Blockchain To Combat Cryptocurrency-Related Crimes. *Forbes*. Retrieved from <https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/>
- Wooldridge, J. M. (2010). *Econometric analysis of cross section and panel data*. MIT Press.
- Wooldridge, J. M. (2010). *Econometric Analysis of Cross Section and Panel Data*. MIT Press.
- Workman, D. J. (1982). The use of offshore Tax Havens for the purpose of criminally evading income taxes. *The Journal of Criminal Law & Criminology*, 73(2), 675–706. doi:10.2307/1143111
- World Bank. (2004). *Mainstreaming Anti-Corruption Activities in World Bank in Assistance – A Review of Progress since 1997*. World Bank.
- World Bank. (2020, June 26). *Nigeria's Economy Faces Worst Recession in Four Decades*. World Bank Report. Retrieved from <https://www.worldbank.org/en/news/press-release/2020/06/25/nigerias-economy-faces-worst-recession-in-four-decades-says-new-world-bank-report>
- Worldbank Group. (n.d). *Helping Countries Combat Corruption: The Role of the World Bank*. <http://www1.worldbank.org/publicsector/anticorrupt/corruptn/cor02.htm>
- Worldbank. (2020). Retrieved from <http://www.worldbank.org>
- Worldbank. (2020a). *GDP (current US\$)*. Retrieved from <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?view=chart>
- Worldbank. (2020b). *Land area (sq. km)*. Retrieved from <https://data.worldbank.org/indicator/AG.LND.TOTL.K2?view=chart>



- Worldbank. (2020c) *Population, total*. Retrieved from <https://data.worldbank.org/indicator/SP.POP.TOTL?view=chart>
- Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of *Lex Cryptographia*. Retrieved from <https://ssrn.com/abstract=2580664>
- Wright, J. P., Tibbetts, S. G., & Daigle, L. E. (2014). *Criminals in the making: Criminality across the life course*. Sage Publications.
- Wurth, E. (2012). *A will and a way: An analysis of tax practitioner preparation compliance* (Unpublished PhD thesis). Australian National University.
- Wurth, E., & Braithwaite, V. (2016) *Tax practitioners and tax avoidance: gaming through authorities, cultures and markets* (RegNet Research Paper No. 119). Australian National University.
- Wu, T. (2010). Agency threats. *Duke Law Journal*, 60, 1841–1857.
- Xiaohong, Ch. (2011). *Research on E-Commerce Transaction Cost-Benefit Characteristics and Evaluation Approaches*. Management and Service Science (MASS), 2011 International Conference. Wuhan. China.
- Xie, P., Zou, C., & Liu, H. (2016). The fundamentals of internet finance and its policy implications in China. *China Economic Journal*, 9(3), 240–252. doi:10.1080/17538963.2016.1210366
- Yamen, A., Allam, A., Bani-Mustafa, A., & Uyar, A. (2018). Impact of institutional environment quality on tax evasion: A comparative investigation of old versus new EU members. *Journal of International Accounting, Auditing & Taxation*, 32, 17–29. doi:10.1016/j.intaccaudtax.2018.07.001
- Yan, J., Yu, W. & Zhao, J. L (2015). How signaling and search costs affect information asymmetry in P2P lending: the economics of big data. *Financial Innovation*, 1(1), 1-11.
- Yan, S., & Yan, D. (2019). Volatility Estimation in the Era of High-Frequency Finance. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 99–141). IGI Global. doi:10.4018/978-1-5225-7805-5.ch006
- Yan, Y., Lv, Z., & Hu, B. (2018). Building investor trust in the P2P lending platform with a focus on Chinese P2P lending platforms. *Electronic Commerce Research*, 18(2), 203–224. doi:10.1007/10660-017-9255-x
- Ye, T. (2017). Stock forecasting method based on wavelet analysis and ARIMA-SVR model. *3rd International Conference on Information Management*, 102-106. 10.1109/INFOMAN.2017.7950355
- Yeung, K. (2016). Algorithmic regulation and intelligent enforcement. In M. Lodge (Ed.), *Regulation scholarship in crisis?* (LSE Discussion Paper No. 84, pp. 50-62). Academic Press.
- Yıldırım, I. (2019). Emergence of Insurance Technologies (InsurTech): The Turkish Case. In A. Rafay (Ed.), *FinTech as a Disruptive Technology for Financial Institutions* (pp. 42–60). IGI Global. doi:10.4018/978-1-5225-7805-5.ch003
- Yildirim, Y., & Rafay, A. (2021). Anti-Money Laundering in Insurance Sector: The Turkish Case. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Ylönen, M., & Laine, M. (2014). For logistical reasons only? A case study of tax planning and corporate social responsibility reporting. *Critical Perspectives on Accounting*. Advance online publication. doi:10.1016/j.cpa.2014.12.001
- Younas, K., & Rafay, A. (2021). (Forthcoming). Women entrepreneurship and financial literacy - Case of female borrowers in Pakistan. *Iranian Economic Review*.

## Compilation of References

- Yum, H., Lee, B., & Chae, M. (2012). From the Wisdom of Crowds to My Own Judgment in Microfinance Through Online peer-to-peer Lending Platforms. *Electronic Commerce Research and Applications*, 11(5), 469–483. doi:10.1016/j.elerap.2012.05.003
- Zakaria, M. (2015). Antecedent factors of whistleblowing in organizations. *Procedia Economics and Finance*, 28, 230–234. doi:10.1016/S2212-5671(15)01104-1
- Zaki, M., Theodoulidis, B., & Solís, D. D. (2011). “Stock-touting” through spam e-mails: A data mining case study. *Journal of Manufacturing Technology Management*, 22(6), 770–787. doi:10.1108/17410381111149639
- Zhang, G. (2005). *Environmental Factors in China's Financial Accounting Development since 1949* (PhD Thesis). Erasmus University Rotterdam. Retrieved from <http://hdl.handle.net/1765/1888>
- Zhang, Y., Wu, Y., Tian, M., & Qiao, Z. (2015). *Third market analysis: The development of P2P lending in the new third market*. Beijing: Minsheng Securities. Retrieved from <http://www.mszy.com>
- Zhang, D., & Zhou, L. (2004). Discovering golden nuggets: Data mining in financial application. *IEEE Transactions on Systems, Man, and Cybernetics. Part C*, 34(4), 513–522.
- Zhang, H. (2016). Regulation of information disclosure and the patterns of P2P lending in China. *China Economic Quarterly*, 16(1), 371–392.
- Zhang, K., & Chen, X. (2017). Herding in a P2P lending market: Rational inference OR irrational trust? *Electronic Commerce Research and Applications*, 23(3), 45–53. doi:10.1016/j.elerap.2017.04.001
- Zhang, L., Chen, Y., & He, Z. (2018). The effect of investment tax incentives: Evidence from China's value-added tax reform. *International Tax and Public Finance*, 25(4), 913–945. doi:10.1007/10797-017-9475-y
- Zhang, R. (2010). Enterprise social responsibility and tax planning. *2010 International Conference on E-Product E-Service and E-Entertainment, ICEEE2010*. 10.1109/ICEEE.2010.5661450
- Zolkafli, S., Nazri, S. N. F. S. M., & Omar, N. (2021). Factors Influencing the Outcome of Money Laundering Investigations. In A. Rafay (Ed.), *Money Laundering and Terrorism Financing in Global Financial Systems*. IGI Global.
- Zuleta, J. C. (2008). *Combating corruption in the revenue service: the case of VAT refunds in Bolivia* (U4 Brief No. 14). Transparency International. Retrieved from <https://www.u4.no/publications/combating-corruption-in-the-revenue-service-the-case-of-vat-refunds-in-bolivia>
- Zuleta, J. C., Leyton, A., & Fanta, E. (2007). Combating corruption in revenue administration: The Case of VAT refunds in Bolivia. In J. E. Campos & S. Pradhan (Eds.), *The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level*. The World Bank Group.
- Zweibon v Mitchell*, 516 F.2d 594 (1975).

## About the Contributors

**Abdul Rafay** is a practitioner cum academician. For more than 25 years, Mr. Rafay has been working as a freelance advisor, consultant & trainer to a wide variety of public & private sector national and multinational companies in the areas of Corporate Finance, Financial Policy & Implementation, Auditing & Assurance, Accountancy, Corporate Tax Management, Financial Technology and System Consultancy. He has been providing consultancy to various industries including Textile, Auto Assembling, Footwear, Industrial/Agro Chemicals, Ice Cream/Dairies, Glass/Ceramics, Healthcare, Mining/Natural Resources, Packaging/Paper Sacking, Steel/Pipe Casting, Rice Processing, Brokerage/Co-operative Financing, Software Development, Real Estate, Printing/Publishing, and Construction/Civil Engineering etc. Mr. Rafay is a Fellow member of the Institute of Chartered Accountants of Pakistan. He is also member of various national and international professional bodies including Institute of Internal Auditors (IIA), USA; Association of Certified Fraud Examiners (ACFE), USA. Since 2001, he has been a life time member of Lahore Tax Bar Association. He has served as Co-regional Director (Founding) of Lahore-Islamabad Chapter of Professional Risk Managers International Association (PRMIA), Washington, USA (2011-2013). In 2012, he was nominated as Member: Education & Training Committee (ETCOM) of The Institute of Chartered Accountants of Pakistan (ICAP). He is also a member of ICAP's "Islamic Finance working group" which is closely in liaison with State Bank of Pakistan and other stakeholders for Islamic Finance Accounting and Auditing Standards. He is Alumni of Rausing Executive Development Center (REDC), Lahore University of Management Sciences (LUMS), Pakistan. In 2014, International Finance Corporation (World Bank Group) selected him for Training of Trainers (ToT) for Corporate Governance Action Planning for SMEs. He is also an approved trainer for Institute of Financial Markets of Pakistan (IFMP) established by Securities and Exchange Commission of Pakistan, the corporate regulator. In 2013, his name got included in the list of "Certified Directors" as per Clause (xi) of The Code of Corporate Governance 2012 issued by SECP. Since 1994, Mr. Rafay has also been associated with teaching in some of the top business schools of Pakistan. His specialized subjects of interest include: Strategic Corporate Finance, Financial Derivatives, Investments/Portfolio Analysis, International Financial Reporting Standards, Corporate Restructuring (Mergers & Acquisitions), Financial Statement Analysis & Corporate Taxation. He also served as an instructor in Civil Services Academy, Pakistan to train the CSS Officers selected by Federal Public Service Commission of Pakistan (FPSC). Currently he is a Professor of Finance & Accounting at University of Management & Technology, Pakistan. He has published more than two dozen research papers in SSCI, ESCI and Scopus indexed journals published by reputed global publishers including Emerald, Sage, Taylor & Francis and IGI Global. He contributed multiple chapters in Books edited by International Editors. Since 2019, he edited multiple international books on FinTech, Islamic Finance and financial Crimes published by IGI Global, USA.

### **About the Contributors**

**Ayesha Afzal** holds a PhD in Economics from Lahore School of Economics with a concentration in Financial Economics. Her dissertation was focused on the risk and return framework of financial intermediaries, under Basel regulations, in Pakistan. Currently, she is an Associate Professor at Lahore School of Economics. She has been a fellow at the University of Oxford where she has worked on issues in growth and social policy under modern financial paradigm in comparative studies of South Asian economies. She has also received formal training for Case Method Teaching at the Harvard Business School, Boston, USA. Dr Afzal's research interests include various aspects of development, financial system, and risk management. She is currently conducting collaborative research with Professors from the University of Oxford in areas of Corruption and Gender, and the Impact of Financial Development on Resilience in South Asia. She is publishing her research in prominent international journals. Dr Afzal is a recipient of multiple International Awards for her research. She received the Best Paper Award at the 4th International Conference on Advances in Social Science, Management and Human Behavior in Rome, Italy, in December 2016. Prior to that, she was awarded Best Paper Award at the 12th International Conference on Business Management at BIMCH and University of Jayewardenepura, Sri Lanka in December 2015.

**Fábio Albuquerque** holds a PhD in Economic and Business Sciences from the University of Extremadura, UNEX, Spain. Currently, he is an Assistant Professor at Lisbon Accounting and Business School, Portugal. His professional experience includes technical work in different entities in the areas of accounting, reporting and statistics, as well as the provision of consulting and business training services on international and national accounting and financial reporting standards and risk management in Auditing.

**Alam Asadov** holds a PhD in Islamic Finance from INCEIF, Malaysia. Currently he is an Assistant Professor at the Department of Finance, Prince Sultan University, Riyadh, Saudi Arabia. He has over 15 years of teaching and research experience in Economics and Finance in several universities in the USA, Uzbekistan, Malaysia and Saudi Arabia. Alam has published several edited books and book chapters, articles in academic journals and professional magazines as well as participated in numerous conferences in various areas of Economics and Finance. His latest research interests are related to monetary systems, house prices and home financing, investment strategies in financial markets, economic and financial stability, and behavioral economics and finance.

**Aiman Asif** has completed her MSc in Economics from Lahore University of Management Sciences. Currently, she is working as Research at the Center for Research in Economics and Business (CREB), Lahore School of Economics. Her research interests include financial economics and macroeconomics.

**Robert Beeres** holds a PhD in administrative sciences from Radboud University Nijmegen, The Netherlands. Currently, he is a Professor of Defence Economics at the Faculty of Military Sciences, Netherlands Defence Academy. His research interests include defence capabilities, performance management and burden-sharing within the EU and NATO. He published numerous articles in peer-reviewed journals, books and magazines and co-edited a number of books.

**Narendra S. Bohra** holds a PhD Currently, he is a professor at Graphic Era University, India.

**Myriame Bollen** holds a PhD in social sciences from Leiden University, The Netherlands. She is a Professor of Civil-Military Interaction at the Faculty of Military Sciences of the Netherlands Defence Academy and chairs the Department of Military Management Studies. Also, she is a visiting professor at the Baltic Defence College, Estonia. Her research interests include inter-organizational cooperation and management of change.

**Maurice Dawson** holds a PhD in Cyber Security from the Intelligence Systems Research Centre at London Metropolitan University, UK. He also holds a doctorate in Computer Sciences from Colorado Technical University in 2009. Currently, he is the Distinguished Member and Director of Illinois Institute of Technology's Center for Cyber Security and Forensics Education, which is accredited by the National Security Agency and Department of Homeland Security. He is also an Assistant Professor of Information Technology and Management in the College of Computing. Before joining Illinois Tech, Maurice served as an Assistant Professor at the University of Missouri - St. Louis with Visiting Professorships to the Technical University of Munich, Polytechnic University of Puerto Rico, and the University of Tennessee Space Institute. Additionally, he has been a Fulbright Scholar to Prince Sultan University in Saudi Arabia, and South Ural State University in Russia. Dawson has a decade of experience in the defense and aerospace industry.

**Delphine Defossez** holds a PhD in Aviation Law from the University of Brasilia, Brazil. Currently, she is a Lecturer in Law at Northumbria University. Her research interests include cybercrimes and its relevant legislation.

**Jason Diodati** is a graduate from the Bachelor of Arts - Criminal Justice (Honours) degree at Mount Royal University, Jason Diodati is a tech fanatic who worked with Apple for six years. Jason continues to strive for new projects, specifically in the field of cyber crime, cryptocurrency and criminality, and social engineering.

**M. Fevzi Esen** holds a PhD in Business Administration. Currently, he is an assistant professor of quantitative techniques at the University of Health Sciences, Turkey.

**Simal Güzel** holds a PhD in Public Finance from Uludag University, Turkey. Currently, she is an Assistant Professor at Namık Kemal University, Faculty of Economics and Administrative Sciences, Public Finance Department Tekirdag-Turkey. Her main research fields are public finance, tax incentives, public expenditures.

**Kabir Tahir Hamid** holds a PhD in Accounting from Ahmadu Bello University, Nigeria. He is an Associate Member of the Association of National Accountants of Nigeria (ANAN), Chartered Institute of Stockbrokers (CIS), Chartered Institute for Securities and Investment (CISI) UK, Institute of Certified Public Accountants of Nigeria (ICPAN) and Chartered Institute of Treasury Management of Nigeria (CITMN). He is also a Fellow Chartered Institute of Finance and Control of Nigeria (CIFCON) and Institute of Debt Recovery Practitioners of Nigeria (IDRPN). In addition to lecturing at Bayero University Kano, he has also been a visiting lecturer to a number of Universities in Nigeria, as well as, a regular facilitator at training courses for both the public and private sector organizations. He actively participates in a number of community-Based Organizations and serves as an external examiner to a

### **About the Contributors**

number of Universities and Polytechnics and actively participates in other national assignments. He has published more than 50 research publications in reputable peer review journals, conference proceedings, book of readings, and technical reports to his credit. He also co-authored and edited a number of books, conference proceedings, and training compendia, in addition to being an editor to a number of journals, both within and outside the country.

**Laura Hansen** holds a PhD from the University of California Riverside, where her dissertation focused on white-collar crime and insider trading. Her publications include discussions of “diagnosing and treating” white collar and corporate crime, as well as the myth of individual greed. Her current project includes studying the potential for financial fraud after natural and human-made disasters. Dr. Hansen had a previous career as a financial paraplanner and certified tax preparer, before completing her doctorate.

**Md Harashid Haron** holds a PhD in strategic management from Universiti Sains Malaysia. Currently, he is a senior lecturer at the Accounting section, School of Management, Universiti Sains Malaysia (USM), Malaysia. Md Harashid specializes in Shari’ah-compliant research, such as Shari’ah-compliant corporate governance; accounting, finance, and waqf. He has published chapters in books; published papers in journals and proceedings; and supervised a number of Ph.D./DBA and MA/MBA students.

**Yingzi Hu** is a Suzhou-based independent researcher. Her research interests include PPP, P2P, M&A and Chinese economy.

**Merve Karacaer Ulusoy** holds a PhD in Banking & Finance from Ankara Yıldırım Beyazıt University, Turkey. Currently, she is working as Head of Department at the same university. Her areas of interest include macro-micro economics, energy economics, and financial markets/institutions.

**Junaidu Muhammad Kurawa** holds a PhD in Accounting. Currently, he is a Professor of Accounting and Finance at Bayero University, Kano-Nigeria. He is a member of a number of professional bodies including the Association of National Accountants of Nigeria (ANAN); Institute of Certified Public Accountants of Nigeria (ICPAN); Institute of Treasury Management of Nigeria (ITMN) and Chartered Institute of Stockbrokers of Nigeria (CISN). Kurawa had co-authored and edited a number of books/journals in Accounting, Taxation, Auditing and Finance.

**Sagir Lawal** is a final stage candidate for PhD Accounting at Bayero University, Nigeria. He is currently the acting HOD of the Accounting department at the Nigeria Police Academy. He is a member of the Association of National Accountants of Nigeria and Institute of Treasury Management of Nigeria. His research interests include forensic accounting and auditing. He possesses 7 years of experience and published more than twenty papers /book chapters.

**Brian K. Leonard, J.D., LL.M., Esq.,** holds a J.D.in Law from Samford University, Cumberland School of Law and a Master of Laws (LL.M.) in Taxation Law from the University of Alabama School of Law. Currently he is an Adjunct Professor at Alabama Agricultural and Mechanical University and at Mitchell Hamline School of Law. He is also the founder of Civil Rights University. His research interests include civil rights law, employment discrimination law, business law, as well as cybersecurity, and privacy Law. He possesses over 14 years of experience in public and private practice, including

serving as an attorney and consultant for state and local governments and entrepreneurs. He has published or co-authored more than seven scholarly journal articles and book chapters. He is the author of the forthcoming book, *Movement Mentors: Dred Scott, Homer Plessy, and Rev. Oliver Brown; Three Courageous Men, Their Landmark Cases, and Their Enduring Legacies*, scheduled for publication in January 2021 (Civil Writes Press).

**Anika Morshed** completed her graduation from the Department of Economics and Banking, International Islamic University Chittagong, Bangladesh. Now, she is pursuing her MS in Economics and Banking.

**Marie G. Nakitende** holds a PhD in Management from Cardinal Stritch University, USA. Currently, she is Dean, Faculty of Business Administration and Management at Uganda Martyrs University, Uganda. She published a large number of research papers in international journals.

**Julija Cassiano Neves** holds a Master degree in Accounting from Instituto Politécnico de Lisboa/Lisbon Accounting and Business School, Portugal.

**Nikolay Ivanov Nikolov** holds a PhD in Administrative Law and Administrative Procedure from Sofia University “St. Kliment Ohridski”, Bulgaria. He is a current member of the Central Election Commission appointed by the Parliament in 2019. Previously he served as a member of the first Commission for establishing property acquired from criminal activity (2005-2010), a member of the Legal Counsel of the President of the Republic of Bulgaria (2010 – 2011), a member of the Commission for Prevention and Ascertainment of Conflict of Interest (2011 – 2018), acting chairperson of the Commission (2013-2018). He is also a lecturer at the Varna University of Management, Bulgaria. He is a legal practitioner with nearly 25 years of legal work experience. He has been a speaker and lecturer at more than 150 training seminars for public or local authority employees, judges, and prosecutors on topics such as conflict of interest, incompatible activities, civil forfeiture, personal data protection, money laundering, and financial crimes.

**Tayo Oke** holds a PhD and is a principal partner at the financial and economic law firm; ASIKO Chambers. Currently, he is also a senior academician at Afe Babalola University, Ado-Ekiti, Nigeria.

**Md. Harun Ur Rashid** is serving as a full-time faculty of Accounting at the Department of Economics & Banking in International Islamic University Chittagong. He is pursuing his M.Phil. at the Bangladesh University of Professionals. He has various publications in referred journals. His research interests include CSR, green/climate financing, taxation, corporate governance, Shariah regulations. He is proficient in research tools like SPSS, AMOS, Smart-PLS, Eviews, DEAP, and STATA. He is also skilled in quantitative research methods and techniques and learning new horizons of research.

**Md. Nur Alam Siddik** holds a PhD in Finance from Dongbei University of Finance and Economics, Dalian, China. At present, he is an Associate Professor at Begum Rokeya University, Rangpur, Bangladesh. He has published twenty research papers in international peer-reviewed journals including journals indexed in SSCI, SCIE, ESCI, ABDC, and SCOPUS. He contributed multiple chapters in Books edited by International Editors. His current research interests include banking industry analysis, economic

### **About the Contributors**

growth, fraud management of banks, mobile banking and financial inclusion, Bank led financial inclusion, Digital finance and sustainable economic growth.

**Shailendra Singh** is a capital market consultant in India.

**Annamaria Szakonyi** is a Research Computing Architect of Saint Louis University, USA, and a PhD student and researcher investigating the effects of technology and technology policy on social justice and equity, with a passion for applying technology to combat human trafficking and the exploitation of women and children. She graduated with distinction from the joint master's degree program of Middlesex University, London and the University of Pecs, Hungary in Applied Management/Finance (MBA equivalent). She holds a dual master's degree in Information Technology Management and Media Communications from Webster University, USA, where she graduated with honors. She's received various distinguished academic awards, such as the Presidential Scholarship of the Republic of Hungary, Erasmus Scholarship from the European Union, and scholarships from the French Republic and the Hungary-Missouri Educational Partnership. She has over 10 years' experience in the IT and innovation sector, spanning from Fortune 500 corporations to non-profits and higher education institutions.

**Antoine Trad** holds a PhD in Computer Sciences, Currently, he is a professor and a researcher at Institute of Business and Information Systems Transformation Management (IBISTM) in Switzerland and France. He is an experienced researcher and authored more than 60 research papers on Business Innovation and Transformation Projects.

**Tutku Tuncali Yaman** holds a PhD in Quantitative Methods from Marmara University, Turkey. She is currently working as a faculty member at Beykent University, Faculty of Economics and Administrative Sciences, Department of Management Information Systems. Her research interests include Multivariate statistics, Data mining, Multi-criteria decision-making methods, Digital archeology, and Fuzzy logic.

**Umar Habibu Umar** is a member of the Institute of Chartered Accountants of Nigeria (ICAN). Currently, he is a lecturer in the Department of Accounting, Yusuf Maitama Sule (Formerly Northwest) University Kano, Nigeria. Umar's major area of research interest is Islamic Accounting, Banking and Finance. He also has a special interest in the research that links accounting to Islamic inheritance. Hence, he has a number of papers linking accounting to Islamic inheritance published in eminent journals and edited books by renowned scholars.

**Hülya Ünlü** holds a PhD in Banking & Finance from Ankara Yildirim Beyazit University, Turkey. Currently, she is an Assistant Professor at the Departments of Economics at the Cankiri Karatekin University, Turkey where she is the Head of the Department of Economic Theory. She is a Deputy Manager of the Center for Women's Studies at Cankiri Karatekin University. She is a member of the Triple Helix Association and a keynote speaker (Innovation, Obstacles, Entrepreneurship). Her research interests are innovation, finance, and econometrics.



**Jan van Lieshout** is Assistant Professor of Defence Economics at the Faculty of Military Sciences, Netherlands Defence Academy. His research interests include the economics of international arms trade (PhD track), counter-threat finance, (marketing of) terrorism and economics in general. He published articles and chapters in peer-reviewed journals and books.

**Georgios L. Vousinas** is a doctoral researcher of Supply Chain Finance (SCF) at the National Technical University of Athens (NTUA), Greece. He possesses 15 years of rich experience in Internal audit and banking in leading banking institutions of Greece. His primary areas of research interest include Supply Chain Finance, Financial Supply Chain Management, banking & finance, and internal auditing. His publications include papers published in fully reviewed academic journals in various fields (finance, banking, auditing) and scientific papers presented in both academic - and business-oriented international conferences.

**Brendan Walker-Munro** is a Director - Risk & Intelligence at the Australian Taxation Office and is completing a PhD with Swinburne University, Australia. He has a wide variety of experience with the regulation and enforcement of disciplinary, civil and criminal laws, and has published articles in a variety of journals and fields.

**Simeon Wanyama** holds a PhD in Corporate Governance from the University of Dundee in Scotland, UK. Currently, he is a Professor of Management at Uganda Martyrs University. He has an MBA from St. John's University in New York. He is a Fellow Member of the Association of Chartered Certified Accountants (FCCA), a Certified Public Accountant (CPA), a Certified International Procurement Professional (CIPP), and a member of the Institute of Corporate Governance of Uganda. He was the Chair of the Board of the Public Procurement and Disposal of Public Assets Authority (PPDA) of Uganda for 7 years and has also served on the Council of the Institute of Certified Public Accountants of Uganda where he chaired the Education Committee and was a member of the Public Accountancy Examinations Board (PAEB). He has also served as Chair of the Uganda Business and Technical Examinations Board (UBTEB) and is the current chair of the Board of Joint Health Care Investment Ltd. He also chairs the Audit Committee of the Uganda National Curriculum Centre. Previously he served as Deputy Vice-Chancellor of Uganda Martyrs University.

**Maimoona Waseem** is a Research Associate at the Office of Research Innovation and Commercialization (ORIC), University of Management and Technology, Lahore, Pakistan. She has a Masters in Business Administration (MBA) from the Lahore School of Economics, Lahore, Pakistan. Her research interests lie in Finance, Banking and Supply Chain.

**John Winterdyk** holds a PhD in Criminology from Simon Fraser University, Canada. Currently, he is a full Professor of Criminology at Mount Royal University, Canada. He has published over 35 academic books and a couple of dozen peer-reviewed journal articles across a wide range of national and international journals. His primary areas of scholarly interest include human trafficking, juvenile delinquency, crime prevention, and comparative criminal justice and criminological issues. He holds three different adjunct positions and is the recent recipient of a national scholarly activity Award (2019) in criminology and criminal justice, and is the recipient of the Faculty of Arts Distinguished Scholarship Award (2019).

### ***About the Contributors***

**Poshan (Sam) Yu** is a Lecturer in Accounting & Finance at Soochow University international co-operative education program. He is also an External Professor of FinTech & Finance at SKEMA Business School (China). Sam leads FasterCapital (Dubai, UAE) as Regional Partner (China). His research interests include FinTech, RegTech, Public-Private Partnership (PPP), M&A, Private Equity, Venture Capital, Startups, Art Finance & China's "One Belt, One Road" policy.

**Elif Yücel** holds a PhD in Business Administration from Uludağ University, Turkey. Currently, she is an Associate Professor at the same university. Her research interests include Accounting and Forensic Auditing.

# Index

## A

administrative burden 87, 89, 93-94, 103, 410  
 Administrative Corruption 83, 87, 90-91, 93, 95, 98, 101, 103  
 aggressiveness 397, 401, 406-407, 409, 415, 418, 422, 446, 550  
 Artificial Intelligence 368, 526, 559  
 asset misappropriation 21, 23, 27, 31, 37, 201, 315  
 assets 3-4, 23, 27-28, 32, 35-36, 49-50, 60, 106, 108-109, 111, 115, 119, 122-125, 130, 140, 144, 149-150, 155, 164-166, 170-171, 177, 188-189, 197, 200-201, 203, 207, 211, 219, 222, 229-231, 240, 272, 284-285, 287, 315, 319, 327, 341, 358, 372, 383, 394, 398, 404-411, 424, 434, 463, 471, 494, 515, 517, 536, 544, 549-550  
 Association of Certified Financial Crime Specialists (ACFCS) 321, 331  
 audit 18, 29-30, 32, 34-35, 37-38, 113, 146, 167, 169, 202, 213-214, 218-222, 228, 230-233, 236-239, 241-245, 247-249, 251-253, 262, 266, 268-269, 289, 309, 328, 369-370, 374, 377-378, 390-392, 394, 428, 430-432, 434, 438, 441, 444, 447, 474, 525-526, 534, 552

## B

Bitcoin 284, 289, 371, 463, 468, 473, 477-478, 480, 488, 497-500, 502, 515-517, 519, 521-523, 546, 563  
 black economy 356-357, 359-366, 368, 370-373, 375-376, 380  
 blockchain 284, 288, 379, 477-481, 498-504, 517, 523-524, 546, 552  
 bribes 40-41, 47, 67, 85, 87, 103, 160, 162, 207, 382-384, 388, 391-392, 396, 431, 447

## C

CIS countries 271-279, 282, 284-288, 291

coercion 7, 24, 49-53, 56-58, 60  
 Collective Investment Scheme 293, 297, 310, 312  
 collusion 1-2, 12-16, 20, 160, 164, 166, 487  
 committees 29, 154, 162, 168-169, 202, 238, 295, 300, 302, 306, 310, 473  
 corruption 2, 17, 21-22, 26-27, 32, 35, 37, 39-42, 44-47, 62-80, 82-87, 89-93, 95, 97-103, 105-106, 111, 115-117, 122, 124, 126-127, 129-130, 149-151, 155-160, 162-168, 170, 202, 216, 218-231, 248, 255, 265, 267-269, 315, 326, 328, 379, 381-396, 431, 445-448, 547  
 Counter Threat Finance 49, 60  
 credit 26-27, 49, 51-52, 140, 172-175, 177-178, 181-183, 185-186, 191-194, 219, 229, 239, 252, 277, 287, 297, 308-310, 314, 316, 324, 333-334, 392, 404, 408, 430-434, 445, 459, 483, 493, 501, 510-513, 515, 517, 524, 545, 547, 563  
 Criminal Justice 17, 19, 21, 139, 291, 309, 321, 475, 503, 519  
 Criminology 17-19, 34, 145, 148, 200, 212, 237, 309, 329, 356, 378, 472, 522  
 Crypto Currency 291  
 cryptocurrency 133, 284, 289, 463, 472, 477-478, 481-482, 500, 502-504, 506, 517, 522, 524, 546  
 CSR 215, 397-407, 409-419, 421-422, 424-426, 442, 446  
 currencies 49, 58, 284, 290, 371, 375, 379, 478, 499-500, 503, 515, 538, 546  
 Cyber Transactions 525  
 cybercrime 204, 240, 314, 453-475, 477-478, 493, 501, 503-504, 506-509, 511, 514-515, 518-519  
 cybercriminals 453-454, 460-463, 465, 467-468, 470-472, 515

## D

Dark Web 133, 144, 461, 463, 473, 477, 485, 488, 490, 494-495, 502, 505-506, 515-524  
 Data Breach 459, 466, 502, 511-513, 518, 520-524

## Index

data breaches 453, 506, 511, 518-519, 522-524  
data mining 30, 313, 315, 322, 325, 327-331  
deceased 196-200, 203, 206-208, 210, 212  
Deep Web 477-478  
disclosure 108, 122-123, 128, 130, 134, 139, 147, 164,  
176, 178, 180, 182, 185-186, 194, 264, 317, 333,  
360, 370-371, 376, 378, 397-399, 401-412, 414-  
418, 422, 425-427, 518, 521-522  
disposal 149-151, 155, 164-166, 170-171, 189  
disruption 64, 164, 192, 356-357, 360-361, 363-365,  
374, 376, 379-380, 550

## E

economic impact 453, 458-459, 470-471  
ego 1, 6-11, 16-17, 20, 24-25  
elite 39-43, 45, 63, 65-66, 133, 142-143, 542, 545,  
549, 562  
empowerment 45, 62-63, 68, 70, 76  
enforcement 3, 26, 32, 63, 65-67, 136, 138, 142, 145-  
147, 152, 155, 163, 169-170, 191, 209, 229, 321,  
329, 332, 334, 336, 356-357, 359-360, 363-364,  
366, 368-372, 375, 377, 379-381, 384, 390, 444-  
446, 453-454, 458, 461-467, 470, 498, 507-508,  
510, 513, 517-518, 520, 536-537, 542, 561  
Enron 12, 21, 31, 34, 136, 138-139, 234, 236, 319, 332  
enterprise 36, 67, 80, 82, 85, 98, 110, 187, 192, 219,  
222, 228, 274, 280, 413, 416, 425, 428, 433, 471,  
492, 505, 507, 523, 525-527, 534, 539-540, 550-  
551, 559, 561, 563-565  
entitlement 1, 8, 10, 24, 27, 29, 32  
entrepreneurs 76, 80, 82, 318, 327  
environmental factors 6, 250-252, 254, 256, 261-264,  
268-269, 434  
European law 121, 453  
European Union 53, 60, 67, 106, 338, 401, 453-454,  
469, 507, 540, 560-561  
evasion 23, 65, 79, 100, 253, 314, 359, 371, 375-376,  
379, 382, 386-388, 391-393, 395-397, 400-401,  
416, 422, 428-435, 437-439, 441-442, 444-450,  
485, 536, 559, 563  
Executive Order 13224 49-50

## F

familiarity 303, 428, 430-432, 434, 438, 441, 444  
FATF 49-50, 482, 503  
Federal Trade Commission 229, 509-513, 520-521, 523  
female employment 62-63, 69, 72, 76  
female participation 62, 64-65, 68, 70-72, 74-75, 431,  
434, 442

financial crime 2, 19-20, 34-35, 37, 39-40, 42-45, 48, 80,  
82, 99, 103, 106, 109, 128-129, 132-133, 144, 172,  
174, 189-191, 247, 268, 308-309, 321, 327, 331,  
340, 384, 447, 471, 473, 482, 490, 526, 541, 544  
financial crimes analysis 525  
financial development 271, 273, 275-278, 283, 285-  
286, 289, 429, 446  
financial fraud 1-3, 5, 11-16, 38, 236-239, 241-248,  
261, 265-266, 289, 296, 309, 315, 317, 322-325,  
329-331, 485, 503, 546  
financial literacy 271-279, 281-291, 302, 306, 309  
financial pyramid 280, 282, 284-285, 290, 292  
financial regulations 271, 273, 284, 463  
financial reporting 18, 23, 27, 34-35, 139, 202, 218,  
229, 232, 238, 251, 254, 267, 269, 397-398, 401,  
403, 406, 409-410, 412-414, 420, 422-424, 427  
financial sector development 271-273, 275-278, 286,  
292  
Financial Warfare 49-51, 59-60  
firm characteristics 87, 428-430, 433-434, 439  
forensic accounting 18, 36, 196-202, 210-218, 232-235,  
240-241, 246-256, 259, 261-269, 330  
framework 4, 7-8, 11, 13, 19-20, 24, 30, 41-42, 50, 65,  
68, 70, 106, 117, 154, 172, 174, 176, 179, 191,  
198, 203, 214, 218, 241, 251, 255, 266, 292, 295,  
307, 315, 317, 323, 329, 337, 357, 364, 367, 371,  
375-376, 386, 390, 400, 403, 409, 411, 414-415,  
427, 453-454, 464-467, 470, 474, 518, 525-528,  
534, 536, 540, 546, 552, 558-559, 561, 564-565  
fraud diamond theory 213, 236, 239-240  
fraud guides 477, 494-495, 501-502, 504  
fraud scale 1, 6-7  
fraud triangle theory 4, 7, 203-204, 213, 236, 239-240  
fraudsters 2-4, 7, 9, 11-14, 17, 22, 24-25, 27-32, 196,  
203, 206, 211, 298, 304, 306, 344, 471, 486-487,  
490, 492-496  
funding behavior 428

## G

gender 22, 34, 62-65, 68-70, 76-77, 79, 134, 142, 145-  
146, 201, 217, 302, 304, 309, 430  
globalization 51-52, 82, 218, 505  
governance 32, 41-42, 46-47, 51, 65-66, 70-71, 73,  
75-78, 84, 87, 100-101, 129, 145, 149, 156, 170-  
171, 202-203, 213-215, 231, 233-234, 238, 243,  
245, 247, 253, 309, 362, 374, 376, 379, 384, 387,  
393, 395, 413, 416, 419-420, 425, 445, 447-449,  
467, 502, 504, 528, 534, 536, 540, 550-552, 558  
government 26, 35, 40-41, 43, 45-47, 50, 52, 55-57,  
63-64, 66-68, 71, 76, 78, 82-84, 87, 89-91, 93,

98-99, 103, 107-108, 110, 115, 121-124, 126-127, 133, 136, 138, 140, 143, 147, 149-150, 165-166, 168-171, 173, 179, 186, 191, 202, 208-209, 216, 236, 247, 250-252, 254, 261-263, 274-276, 280-286, 290, 292, 294-295, 302, 306, 332, 334, 357-359, 373-375, 377, 380-385, 388, 390-392, 394, 396, 401, 407, 412, 415, 418, 428-431, 433, 438-439, 441-442, 444, 459, 461, 464, 474, 479-480, 487-488, 493, 507-510, 537, 544, 546, 548  
grease the wheel 82, 84, 93, 98, 103

## H

hedge funds 132-133, 142, 147, 337

## I

identity fraud 471, 477, 492-493, 511, 513-514, 522, 524  
identity theft 2, 175, 229, 459, 465, 470-471, 483-484, 492, 503, 506, 509-511, 514-515, 518-519, 521-524  
incompatibility 105-106, 115, 119-124, 127, 130  
information asymmetry 64, 172, 174-178, 182, 185-186, 190-191, 194, 303-304, 365, 377, 430, 498  
Information Cascade 305, 310  
innovation 60, 80-87, 89, 92-95, 97-103, 143, 173, 175, 179, 191-194, 269, 332-333, 368, 370, 374, 377, 459, 500, 502, 504, 526, 561, 564-565  
insider trading 132-148, 313-314, 317-318, 322-323, 326-333, 336, 341, 346, 352, 354, 487  
intermediation 49, 51, 172-173, 175, 288, 352  
internal control 5-6, 9, 29-30, 32, 34-35, 202-203, 211, 222, 227-228, 230-231, 236, 238, 240, 248  
investment 25, 40, 43, 67, 70-71, 75, 83-85, 98, 100-103, 110, 133-134, 140, 142, 144, 148, 175, 177-179, 186, 199, 239, 269, 271-277, 279-287, 291-299, 302-312, 314, 316, 318, 320, 332-334, 336-337, 340-342, 354, 381, 385, 392, 395, 407-408, 415, 417, 433, 438, 441, 449, 459, 487, 493, 537, 546  
investment decision 292, 303-305

## K

kitties 295, 300, 302-306, 310-312  
Kitty Frauds 293

## L

law 11, 17-18, 20, 22, 26, 32, 38, 50, 54, 61, 63-67, 71, 78, 103, 105-116, 118-125, 127-130, 134-135,

137-138, 142, 145-146, 148, 164, 168, 187, 192-194, 196-197, 199-200, 206-209, 211-212, 219, 221, 229, 237-238, 240-241, 252-253, 265, 268, 284, 296, 314, 317, 326-329, 356-358, 361-362, 365, 368-369, 372-381, 384, 389-390, 395-396, 411, 414, 416, 420-421, 425, 427, 429, 453-454, 456, 458, 461-475, 498, 500, 507-510, 513, 517-519, 521, 524, 526, 535-538, 542, 544, 546-547, 552, 560, 564

legal challenges 453, 458, 460, 467, 469

legislations 66, 105-110, 114-115, 118-119, 121-122, 126-127, 174, 254, 332, 454-455

lex cryptographia 356, 372, 379

logistic regression 236, 242, 245-246, 276, 324, 425

## M

Madoff 1, 11, 20, 33, 136, 140, 145, 148, 288, 299, 308-309, 319  
manipulations 218-221, 322, 325, 327, 330, 332, 536, 547, 559  
market economy 82, 271, 273-274, 276, 286, 292, 414  
market manipulation 313-314, 317, 319-320, 322, 328-329, 331-332, 340-342, 347, 351, 353  
MICE 1, 7, 11  
MiFID 332, 337-338, 341, 353  
Multi-Level Marketing (MLM) 282, 299, 310

## N

narratives 53-54, 57-58  
Network Marketing 293, 308, 310  
Nigeria 17, 36, 39, 46, 48, 101, 196-198, 201-202, 204-205, 212, 215-217, 233-234, 240-241, 248, 250-252, 254-255, 263-269, 365, 378, 472, 493, 508-509, 522, 524-525  
non-compliance 34, 40, 108, 127, 138, 196, 361, 367, 369, 372, 390, 412, 416

## O

obstacle 66, 83-84, 87, 89-90, 93, 98-99, 103, 395, 460  
offences 22, 105, 116, 121, 165, 315, 375, 456-459, 464-465, 468, 476  
ownership structure 428-431, 433, 435, 444

## P

pattern recognition 322-325, 331  
Planned (Command) Economy 292  
platform exit 172, 174, 182, 187-189, 191

## Index

political factors 250, 252-254, 256, 259, 261-264, 267, 386  
political science 18, 43, 381  
Ponzi scheme 11, 33, 140, 272-277, 279-281, 283-286, 288-292, 294, 299, 306, 309-310  
Ponzi schemes 271-291, 298-299, 302, 306, 314  
Portugal 120, 123, 125-126, 130, 397, 399, 401-403, 416-418, 421, 423-424, 427  
poverty 39-42, 44-47, 71, 77, 82, 103, 199, 203, 208-209, 274, 281, 384-385, 389  
predators 28, 31, 518, 522, 525-526, 544, 550, 558  
private gain 40, 103, 381, 383  
probit model 80, 85-87, 92, 96, 98  
procurement cycle 149-150  
proliferation 295, 477-478, 494  
Public Finance 373, 381, 387, 396, 445, 449  
public office holder 105, 108-114, 116-120, 122, 124-128, 130-131  
public power 105, 381, 383  
Pump and Dump 332, 341-342, 344, 346, 353

## R

rationalization 3-6, 8-9, 16, 18, 20-21, 23-26, 32, 222, 239-240  
red flags 35, 137, 218-219, 228-233, 308, 459  
regulations 18, 27, 39, 41, 43, 83, 87, 89-91, 93, 99, 103, 105-106, 119, 125-128, 133-139, 144, 149-150, 155-156, 159, 162, 167-168, 170-172, 174-175, 178-182, 186-187, 189-191, 209, 213, 219-220, 222, 255, 271, 273, 284, 287, 294, 317, 333-337, 339, 341, 353, 382-385, 388-389, 391, 394, 410, 414, 447, 453, 463, 470, 503, 507-508, 510, 518-519, 534, 536-537, 540, 552, 563  
regulatory ambiguity 132, 138, 142  
regulatory disruption 357, 360, 363, 380  
regulatory vacuums 172, 174, 177-178, 186, 190-191  
removal 105-106, 114, 371  
reporting 18, 23, 27-28, 30-31, 34-35, 37, 133, 139-140, 175, 202, 205, 218, 221, 229, 232, 238, 251-252, 254, 267, 269, 284, 315, 319, 322, 338-339, 370, 397-399, 401-414, 416-418, 420-427, 431, 447, 466, 484, 488, 509-510, 512  
risk management 19, 23-24, 30, 33, 37, 175, 249, 268, 341, 353, 395, 413, 416, 448, 505, 525-526, 533  
Role of State 39  
romance scams 453, 459, 461, 470, 506, 513, 518-520  
rotating savings and credit association (ROSCA) 310

## S

Sand the Wheel 82-84, 98, 103  
Scenario-analysis 49  
score 1, 8, 11-12, 14-16, 19, 65, 68, 71-75, 262, 277, 316, 450, 459  
SEC 132-137, 139, 141-142, 144-147, 155, 272, 284-285, 290, 316, 321-322, 329, 331-332, 353-354, 520, 560  
securities fraud 134, 139, 313, 315, 317, 320-323, 325, 330, 547  
securities market 314-318, 320-322, 327-328, 331-332  
social engineering 477-478, 489-491, 494-495, 497, 501-506, 511, 514-515, 519, 521, 523-524  
social media 55, 186, 220, 304, 311, 319, 330, 486, 488-490, 492, 495, 497, 506, 513-515  
State Capture 40, 83, 85, 87, 91, 93, 97-98, 102-103  
stock market manipulation 313-314, 328  
stocks 51, 120, 126, 131, 134, 138, 219, 230, 272, 303, 314-315, 319-320, 322-323, 332  
survey 17-18, 23, 26, 30, 35, 42, 63, 80, 82, 85, 98, 100, 156, 160, 162, 164, 170-171, 236, 240-242, 246, 255, 263, 269, 277, 289, 291, 319, 328-329, 388, 428, 433, 447, 474  
Systems design 356

## T

tax 27, 34, 41, 65, 67, 79, 83, 87, 89-90, 93, 100, 113, 117, 124, 137, 140, 144, 148, 219, 230, 253-254, 314, 352, 356-361, 364, 366-383, 385-435, 437-439, 441-442, 444-450, 488, 529, 536-538, 547, 559-560, 563  
tax administration 364, 367, 372, 375, 381-382, 388-392, 394-396  
Tax crime 356  
tax evasion 65, 79, 100, 253, 314, 375, 379, 382, 386-388, 391-393, 395-396, 401, 416, 422, 428-435, 437-439, 441-442, 444-450, 536, 559, 563  
Tax Officer 388, 396  
Tax Payer 396  
tax system 368-369, 375, 377, 381-382, 386, 388-389, 391-392, 394, 396  
taxpayer 164, 364, 367-368, 370-371, 374, 377, 379, 381, 383, 386, 388, 390-391, 396, 448  
Technology 21-22, 28-29, 36, 98, 102, 172-173, 175, 178, 182, 193, 214, 218-221, 224, 230, 232, 234, 247, 264, 266, 272, 284, 290-291, 296, 315, 323, 326, 330-331, 362-363, 374, 376-379, 397, 424, 453, 455-458, 461, 464, 466, 469-474, 476-481, 483, 488-489, 492, 494-495, 499-508, 511, 513-

514, 518-519, 521-522, 524-525, 527-528, 532, 538, 540, 546, 552, 560-565  
text mining 322, 325, 328, 331  
trading 132-148, 176, 230, 308, 311, 313-314, 316-318, 320, 322-324, 326-333, 336-338, 340-344, 346-348, 352, 354, 477, 487, 515, 542-543, 550, 552, 565  
Transformation 69, 188, 192, 217, 325, 391, 457, 473, 525-527, 534, 556, 558-559, 561, 564-565  
transparency 41, 62-63, 65, 67-68, 71, 76, 82, 99, 101, 149-151, 156, 160-161, 164-165, 167, 169, 175, 191, 197, 211, 251, 261, 284-285, 287, 290, 314, 317, 319, 332, 337-338, 370, 377, 384, 386-387, 390, 392, 394-396, 400-402, 413-416, 420, 426, 431, 434, 466, 497, 509, 547, 563  
Twitter 325, 327, 330, 477-478, 488-489, 502, 505, 514

## **U**

UCIS 293-307, 310-312

UCIS associations 296, 302, 306, 310  
UCIS Chains 296, 310  
Uganda 21, 26, 149-150, 154-156, 162, 165, 170-171, 394, 525  
Unorganized Collective Investment Scheme (UCIS) 293, 297, 310

## **V**

valuers 196, 206-207, 209, 211-212  
Victim Investors 296, 302, 304, 306-307, 310-311

## **W**

White collar crime theory 236, 240  
Word of Mouth (WOM) 293