

MITIGATING OCCUPATIONAL FRAUD: AN ANALYSIS OF FRAUDULENT  
ACTIONS, OPPORTUNITIES, AND RED FLAGS

by

Shashank Agrawal, CFE, MBA, PGP

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

MAR 2024

MITIGATING OCCUPATIONAL FRAUD: AN ANALYSIS OF FRAUDULENT  
ACTIONS, OPPORTUNITIES, AND RED FLAGS

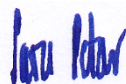
by

Shashank Agrawal, CFE, MBA, PGP

Supervised by

Sagar Bansal, DBA

APPROVED BY:



---

Prof. Saša Petar, Ph.D.

RECEIVED/APPROVED BY:

*Renee Goldstein Osmić*

---

Admissions Director

## **Dedication**

This work is earnestly dedicated to all the relentless fraud fighters and the resilient victims of fraud. Your courage, boundless strength, and incredible resilience in the face of deceit and manipulation have been a profound source of inspiration throughout my journey. You confront challenges with a determination many might never know. Your stories of struggle and success over adversity have fueled my commitment to this cause.

This dissertation is dedicated to fraud investigators, researchers, and educators. You are the unsung heroes in this ongoing battle. Your tireless efforts to expose the truth, protect the vulnerable, and bring perpetrators to justice are the backbone of hope for a future where integrity prevails over deceit.

I dedicate this work to all of you and to the memories of those who may have lost their fight against ever-pervasive fraud. May your courage and spirit live on and continue to inspire future generations.

## **Acknowledgements**

I am deeply grateful to the following individuals who have helped me along my academic journey, especially in the face of challenges and recovery.

First and foremost, I want to express my sincere gratitude to my family, who was my rock and motivator during this time. Their unwavering support and encouragement were invaluable in helping me transition to a new career in fraud examination. I feel blessed to have you all around me and your confidence in me during the times when I felt low on morale.

I also want to extend a heartfelt thanks to my friends Bhavika Varindani and Suman Saha for their encouragement, support, and unwavering positivity, which have helped keep me mentally intact.

I am grateful and would like to express my appreciation for Dr. Sagar Bansal, my mentor, who provided excellent support, guidance, and a comfortable research environment. Dr. Bansal, you have been a source of utmost positivity and confidence in this research. You and I only know how many times you uplifted me back from the phases of darkness. I also want to thank the UpGrad team, especially Ms. Richa Kapoor, for helping, hearing me out, and providing accurate suggestions during the toughest phase of the research.

Finally, I want to acknowledge the fellow fraternity of the “Association of Certified Fraud Examiners – USA,” and Mr. John Gill, President of ACFE, who confidently endorsed my debut book on fraud awareness.

Thank you all for being a part of my journey and helping me achieve this monumental accomplishment.

## ABSTRACT

# MITIGATING OCCUPATIONAL FRAUD: AN ANALYSIS OF FRAUDULENT ACTIONS, OPPORTUNITIES, AND RED FLAGS

Shashank Agrawal, CFE, MBA, PGP  
March 2024

Dissertation Chair: Saša Petar, Ph.D.

This dissertation delves into the dynamic nature of employee fraud in organizations and proposes strategies for prevention and detection. The study aims to address the question: How can organizations minimize employee fraud? Objectives include understanding fraud methods, identifying exploited weaknesses, and detecting early warning signs. This study features a qualitative approach based on content analysis of expert interviews discussing 157 real fraud conviction cases from the U.S. Department of Justice. The research advocates for an integrated approach to fraud prevention, combining theoretical insights with evidence-based strategies to protect organizational assets and integrity. It aims to advance academic discourse on employee fraud and concludes with a refined fraud model “Integrated Fraud Model (IFM)”, explaining fraud elements and their interplay in detail.

## TABLE OF CONTENTS

|  |    |
|--|----|
| List of Figures .....  | x  |
| CHAPTER 1: INTRODUCTION .....                                    | 1  |
| 1.1 Overview .....   | 1  |
| 1.1.1 Definition Of Fraud .....                                  | 5  |
| 1.1.2 Definition Of Occupational Fraud.....                      | 6  |
| 1.1.3 Definition Of Employee Fraud.....                          | 8  |
| 1.1.4 The Difference Between Occupational & Employee Fraud.....  | 9  |
| 1.2 The Cost Of Employee Fraud .....                             | 10 |
| 1.2.1 Direct Costs Of Fraud .....                                | 11 |
| 1.2.2 Indirect Costs Of Fraud .....                              | 11 |
| 1.2.3 Intangible Cost Of Fraud .....                             | 12 |
| 1.2.4 Preventive Cost Of Fraud .....                             | 13 |
| 1.3 Research Problem.....  | 13 |
| 1.4 Research Question:.....                                      | 16 |
| 1.5 Research Objectives:.....                                    | 17 |
| 1.6 Research Design.....   | 19 |
| 1.7 Research Limitations.....                                    | 19 |
| 1.8 Significance Of The Study .....                              | 20 |
| 1.9 Dissertation Outline .....                                   | 23 |
| CHAPTER 2: LITERATURE REVIEW .....                               | 24 |
| 2.1 Brief Overview .....   | 26 |
| 2.2 Preliminary Literature Review .....                          | 28 |
| 2.3 Fraud Theories.....  | 30 |
| 2.3.1 The Fraud Triangle.....                                    | 31 |
| 2.3.2 The Fraud Scale.....                                       | 33 |
| 2.3.3 The Fraud Diamond .....                                    | 33 |
| 2.3.4 The Fraud Pentagon .....                                   | 34 |
| 2.3.5 The MICE Model .....                                       | 35 |
| 2.3.6 The SCORE Model .....                                      | 35 |
| 2.4 Detailed Investigation Of Fraud Triangle .....               | 37 |
| 2.5 Critical Review of The Fraud Triangle .....                  | 43 |
| 2.6 Need For Further Exploration .....                           | 47 |
| 2.7 Detailed Review Of Fraud Diamond.....                        | 49 |
| 2.8 Critical Review Of The Fraud Diamond.....                    | 51 |
| 2.9 Discussion And Review .....                                  | 52 |
| 2.10 Summary Of Findings And Gaps In The Existing Research ..... | 53 |
| 2.11 Conclusion Of Literature Review Findings .....              | 57 |
| CHAPTER 3: RESEARCH METHODOLOGY.....                             | 60 |

|  |         |
|--|---------|
| 3.1 Initial Data Set Selection.....  | 61      |
| 3.2 Elimination Of Cases Outside Study Scope.....                              | 62      |
| 3.3 Inclusion Of Cases Of Special Importance .....                             | 63      |
| 3.4 Expert Panel Selection .....   | 64      |
| 3.5 Structured Interview Discussion .....                                      | 64      |
| 3.6 Content Analysis .....   | 64      |
| 3.7 Model Conceptualization.....   | 65      |
| <br>CHAPTER 4: MAJOR TYPES OF FRAUD .....                                      | <br>66  |
| 4.1 Asset Misappropriation .....   | 67      |
| 4.2 Fraudulent Claims And Invoices.....  | 68      |
| 4.3 Collusion And Conspiracy .....   | 69      |
| 4.4 Manipulation Of Company Systems: .....                                     | 70      |
| 4.5 Forgery And Counterfeiting .....   | 72      |
| 4.6 Financial Statement Fraud or the Investor Fraud and Misrepresentation..... | 73      |
| 4.7 Regulatory Evasion And Deception.....                                      | 74      |
| 4.8 Money Laundering.....  | 75      |
| 4.9 Identity Theft, Data Breach And Impersonation.....                         | 76      |
| 4.10 Tax Evasion And False Tax Claims.....                                     | 77      |
| 4.11 Bribery And Corruption .....  | 78      |
| 4.12 Procurement And Vendor Fraud .....  | 78      |
| 4.13 Creation Of Shell Company .....   | 79      |
| 4.14 Payroll Fraud.....  | 80      |
| 4.15 Payroll Tax Evasion .....   | 81      |
| <br>CHAPTER 5: OPPORTUNITIES AS A CATALYST TO FRAUD.....                       | <br>83  |
| 5.1 Position Of Trust & Authority .....  | 84      |
| 5.2 Lack Of Segregation Of Duties.....   | 86      |
| 5.3 Poor Audit Performance And Management Oversight .....                      | 90      |
| 5.4 Lack Of Systems Of Authorization.....                                      | 96      |
| 5.5 Poor Monitoring And Security Of Personal Data .....                        | 99      |
| 5.6 Poor Accounting System.....  | 104     |
| 5.7 Lack Of Independent Checks And Control Of Accounts In The System .....     | 107     |
| 5.8 Poor Control Of Signed Cheques.....  | 110     |
| 5.9 Poor Procurement Policies .....  | 114     |
| 5.10 Poor Payroll Management.....  | 116     |
| 5.11 Lack of Physical and digital access controls.....                         | 120     |
| 5.12 Absence Of Cash Reconciliation And Surprise Checks On Cash.....           | 123     |
| 5.13 Hiring Without Background Checks.....                                     | 128     |
| 5.14 Size Of Organization.....   | 131     |
| 5.15 Organizational structure weakness.....                                    | 134     |
| <br>CHAPTER 6: RED FLAGS AS A DETECTION TOOL FOR FRAUD .....                   | <br>139 |

|   |         |
|---|---------|
| 6.1 Behavioral Red Flags .....  | 139     |
| 6.1.1 A desire for personal Gain .....  | 140     |
| 6.1.2 Scheming Attitude.....  | 141     |
| 6.1.3 Living Beyond One’s Means .....   | 142     |
| 6.1.4 Challenge To Beat The System.....   | 143     |
| 6.2 Organizational Red Flags .....  | 144     |
| 6.2.1 Inadequate Attention To Details .....   | 146     |
| 6.2.2 Placing Too Much Trust In A Few Employees.....                                  | 146     |
| 6.2.3 Lack Of Independent Checks On Performance.....                                  | 147     |
| 6.2.4 Lack Of Separation Of Duties.....   | 148     |
| <br>CHAPTER 7: DISCUSSIONS AND CONCLUSION .....                                       | <br>150 |
| 7.1 Integrated Fraud Model - IFM .....  | 150     |
| 7.2 Interplay Of IFM Elements With Central Focus On Opportunity.....                  | 152     |
| 7.2.1 Position Of Trust And Authority.....  | 161     |
| 7.2.2 Lack Of Segregation Of Duties.....  | 162     |
| 7.2.3 Poor Audit Performance And Management Oversight .....                           | 163     |
| 7.2.4 Lack Of Systems Of Authorization .....  | 165     |
| 7.2.5 Poor Monitoring And Security Of Personal Data .....                             | 166     |
| 7.2.6 Poor Accounting System.....   | 167     |
| 7.2.7 Absence Of Independent Checks And Control Within The<br>Accounting System ..... | 169     |
| 7.2.8 Poor Control of Signed Cheques.....   | 170     |
| 7.2.9 Poor Procurement Policies .....   | 171     |
| 7.2.10 Poor Payroll Management.....   | 172     |
| 7.2.11 Lack Of Physical And Digital Access Controls .....                             | 174     |
| 7.2.12 Absence Of Cash Reconciliation And Surprise Checks On<br>Cash .....            | 175     |
| 7.2.13 Hiring Without Background Checks .....   | 176     |
| 7.2.14 Size Of The Organization.....  | 178     |
| 7.2.15 Organizational Structure Weaknesses .....                                      | 179     |
| 7.3 Guidance For Industry.....  | 180     |
| 7.3.1 Show That Ethics Are Essential .....  | 181     |
| 7.3.2 Facilitation Of Reporting .....   | 181     |
| 7.3.3 Trust But Verify .....  | 182     |
| 7.3.4 Beware Of The Slippery Slope .....  | 182     |
| 7.3.5 Keep An Eye Out For Odd Patterns.....   | 183     |
| 7.3.6 Good Results Do Not Justify Poor Decisions .....                                | 184     |
| 7.3.7 Provide Resources So Workers Can Achieve Their<br>Objectives.....               | 184     |
| 7.4 Conclusion.....   | 186     |
| 7.5 Future Research.....  | 187     |
| 7.6 Closing Statement .....   | 187     |



|  |     |
|--|-----|
| APPENDIX A: LIST OF CASES ANALYZED IN THIS STUDY ..... | 188 |
| APPENDIX B INTERVIEW GUIDE.....                        | 212 |
| APPENDIX C: ANALYSIS OF FRAUDULENT ACTS.....           | 215 |
| APPENDIX D: ANALYSIS OF OPPORTUNITIES .....            | 252 |
| APPENDIX E: ANALYSIS OF BEHAVIOURAL FLAGS .....        | 294 |
| APPENDIX F: ANALYSIS OF ORGANIZATIONAL FLAGS .....     | 327 |
| REFERENCES.....  | 361 |

## LIST OF FIGURES

|  |     |
|--|-----|
| Figure 1 - Fraud Triangle (Source: Steve Albrecht, 1982) .....   | 32  |
| Figure 2 - Fraud Diamond (Source: Journal of Islamic Accounting and Finance Research 2(1):91, 2020)..... | 50  |
| Figure 3 – Flowchart Representation Of Research Methodology.....   | 61  |
| Figure 4 - Findings On Major Types Of Fraud .....  | 66  |
| Figure 5 - Findings On Opportunities As A Catalyst To Fraud.....   | 83  |
| Figure 6 - Findings On Behavioral Red Flags As A Detection Tool For Fraud .....                          | 140 |
| Figure 7 - Findings On Organizational Red Flags As A Detection Tool For Employee Fraud .....             | 145 |
| Figure 8 - First Look At The Integrated Fraud Model (IFM) .....  | 151 |

## CHAPTER 1: INTRODUCTION

### **1.1 Overview**

Financial Fraud can be perpetrated in various ways and is an act of deception that results in monetary or personal gain for the perpetrator. It can be committed by deception, abuse of power, and failure to reveal material financial information (Fraud Act 2006). Fraud can be perpetrated by the individual on the individual, individual on corporates, individuals on society, corporates on individuals, corporates on corporates, corporates on society, society on individuals, society on corporates, society on society, etc. There are various shapes and forms of Fraud, e.g., individual Fraud, corporate fraud, government fraud (Ross 2016), etc. Generally, whenever Fraud is committed against an organization, it is often not taken as seriously as other forms of Fraud. The victim organizations are somehow to blame for being victimized (Cross 2015). The variety of fraud practices currently in use implies that fraudsters are creative in their designs of schemes with a wide range of persuasion and manipulation techniques (Wells 2001).

There are various forms of organizational Fraud to combat, including internal Fraud, external Fraud, and cyberattacks (Hart 2010, p. 16). Every business must decide whether to accept losses and account for them in the financial statements or to fight back. Despite the increased awareness of fraud control in recent times, most businesses still lack vigilance and avoid implementing better internal controls in order to prevent Fraud as much as possible (Asmuni et al. 2015; Hamid et al. 2011; Husnin et al. 2016; Nor et al. 2017; Norbit et al. 2017; Salin et al. 2017).

No organization is safe from Fraud (Rossouw et al. 2000). Regardless of industry, size, or location, Fraud affects all different kinds of organizations. It does not

discriminate between public and private organizations, environmental footprints, sustainability levels, public personas, or length of existence (Kranacher, Riley & Wells 2011). Organizations dedicated to philanthropic or nonprofit causes could be just as susceptible to Fraud as other businesses because they might not be able to afford complex internal controls or dedicate enough resources to fraud prevention and detection (Kranacher et al. 2011).

Businesses are estimated to lose an astounding \$400 billion a year due to Fraud of some kind. It is a startling amount that is double the military budget for the United States (Albrecht 2012). We can remove the national deficit if we end Fraud for only two years (Abagnale 2016). A third of the \$400 billion results from employees embezzling money from their employers (Abagnale 2016). Most businesses never disclose these thefts to law enforcement out of embarrassment. They merely terminate the employee. As a result, the employee continues to defraud other people and companies (Albrecht, Howe & Romney 2008).

It is crucial to remember that employee fraud can be committed either by a single employee, e.g., the accountant, or by a group of people, e.g., through collusion. The results are disastrous when fraud is committed through collusion (Mansor & Abdullahi 2015). Although it is well known that individuals and businesses commit Fraud, the reasons behind their fraudulent acts are not entirely understood (Albrecht 1984). In order to avoid Fraud, it is crucial to understand the driving force behind it. Hence, it is crucial to understand the psychology of a fraudster (Albrecht 2014) before, during, and after commissioning Fraud. While doing research, researchers have mostly tried to relate theories of crime with that of Fraud; however, there remains a difference between the two terminologies. Fraud is a subset of crime, and there are a variety of ways to commit a crime (Kranacher et al. 2011). In a general sense, Fraud is the financial sub-set of crime.

Although the purpose of all different fraud theories is to find the motivations behind Fraud, the Fraud Triangle Theory coined by Dr. Donald Cressey is primarily attributed to Occupational or Employee Fraud (Ghazali et al. 2014; Othman et al. 2015; Petrascu & Tieanu 2014; Rahman & Anwar 2014; Suh et al. 2019). Dr. Cressey concluded that Fraud occurs when three elements: pressure, opportunity, and rationalization, all are present (Mansor & Abdullahi 2015). In simple terms, perceived pressure, opportunity, and a way to rationalize the behaviors must all be present for an individual to make immoral actions (Donald R. Creasey 1953). However, the Fraud Triangle was not a theory at the time; Dr. Creasey researched it. It kept evolving over a period of time and was perceived by Dr. Steve Albrecht in 1982 as the universal explanation of the motivation behind Fraud.

According to criminologists, fraudulent behavior is normally motivated by financial pressure. Pressure is the prime motivating factor that causes someone to depart from being a law-abiding citizen to commit Fraud (Johansson & Carey 2016). However, in today's context, the above statement does not entirely hold good. Committing Fraud has become a habit that gives sadistic pleasure to the fraudster as their ego is satisfied after gainful results (Moore et al. 2012). While greed is the typical driver, ego, and revenge can also be motives behind Fraud (Albrecht et al. 2008; Gbegi & Adebisi 2015; Suh et al. 2019). For any reason, an employee enraged and disgruntled with the company may attempt to take revenge by committing Fraud. Sometimes the target of the fraudster is to outsmart the system (Mansor & Abdullahi 2015; Rosefield 1988 in Okezie, 2012). Fraudsters frequently assume they are more intelligent than everyone else and that no one can stop them. In many cases, Fraud is motivated by performance pressure at organizations (Noviani & Sambharakreshna 2014).

Hence, it is essential to perceive the underlying dynamics of various types of fraud in order to establish response strategies and regulations based on these dynamics.

Apart from the reasons mentioned above, Fraud is an afflicting act that thwarts business operations and their persistent expansion. Technological advancements have made today's fraud schemes more sophisticated and intricate (Clarke & Newman 2006). Hence, organizations need to apprehend the fraud risk factors and characteristics of fraud to combat the same effectively.

Any organization is vulnerable to Fraud (Steve Albrecht 2006). Fraud continues to be challenging for businesses, and preventing it is complicated. According to the Association of Certified Fraud Examiners, organizations lose approximately 5% of their revenue each year to Fraud. This is where the psychology of a fraudster plays an important role. The study of why employees commit fraud is essential for identifying potential perpetrators, stopping potential perpetrators from becoming real perpetrators, and preventing employee fraud from occurring (Dorminey et al. 2012).

Fraud is a kind of covert criminality that isn't as visible to the public or viewed as dangerous as street crime. As a result, for a very long time, governments, organizations, and enterprises around the world have ignored the significance of fraud; only recently has the detrimental effects of fraud on businesses, markets, and society as a whole been recognized. Occupational fraud is one kind of economic crime among many other types of economic crimes. Financial statement fraud, asset misappropriation, and corruption are the three main types of occupational fraud. "It is frequently observed that fraud has a greater economic impact on society than any other category of crime," asserted Free (2015, p. 190). Several other articles (e.g., Moore 2018, p. 259) and Máté et al. 2019, p. 1214) corroborate this assertion.

### **1.1.1 Definition Of Fraud**

When attempting to define fraud, one can refer to many sources such as general reference organizations, academic literature, legislation and case law, and government offices' policies, regulations, and handbooks. Although there may be slight variations in the definitions, all of them include the element of deception.

From a legal perspective, fraud is an intentional act of deception involving financial transactions for the purpose of personal gain. Fraud is punishable by law and encompasses a wide range of activities, including, but not limited to, embezzlement, identity theft, and forgery (Black's Law Dictionary).

The Association of Certified Fraud Examiners (ACFE) is an apex organization fighting fraud worldwide. According to ACFE definition, fraud is "a deliberate misrepresentation which causes another person to suffer damages, usually monetary losses. Most people consider the act of lying or lying by omission as constituting fraud. However, in a legal sense, fraud is a much more defined crime" (ACFE Report to Nations on Occupational Fraud & Abuse 2022).

The AIC is an Australian research center for crime and justice. The AIC annually conducts fraud surveys and reports data pertaining to fraud in Australia. According to the AIC, fraud involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else. Fraud Prevention and Control in Australia (Graycar 2000, p.2). Another Australian government publication, the Attorney-General's Department's Resource Management Guide (No. 201)—Preventing, detecting and dealing with fraud (Cth 2014b, p.7), states that it is "... a mental or fault element to fraud requiring intent; it requires more than carelessness, accident or error".

Fraud has also been described as "a generic term that embraces all of the multifarious means that human ingenuity can devise, which are resorted to by one

individual, to gain an advantage over another by false representations." (Albrecht et al. 2012, p. 657).

In Part 7.3 of the Criminal Code Amendment (Theft, Fraud, Bribery, and Related Offences) Act 2000, 'fraudulent conduct' is defined as a deception, either intentional or reckless, whether by words or other conduct, and whether as to fact or as to law and includes:

- A deception as to the intentions of the person using the deception or any other person;
- Conduct of a person that causes a computer, a machine, or an electronic device to make a response that the person is not authorized to cause it to do.

Donald R Cressey gives another pivotal definition of fraud. According to him, from an academic viewpoint, fraud is considered any wrongful or criminal deception intended to result in financial or personal gain. It involves complex psychological and sociological dynamics that influence individuals or groups to commit acts against the norms or laws (Cressey, Donald R. "Other People's Money: A Study in the Social Psychology of Embezzlement").

### **1.1.2 Definition Of Occupational Fraud**

Occupational fraud refers to the exploitation of a professional role for personal enrichment through the deliberate misuse of an organization's resources or assets (ACFE, 2018). According to ACFE, there are four essential components to any type of occupational fraud: (1) it must be done covertly; (2) it must breach the offender's fiduciary duties to the victim organization; (3) it must be done with the intention of providing the offender with a direct or indirect financial benefit; and (4) it must cost the victim organization resources, income, or reserves (ACFE Report to Nations on Occupational Fraud & Abuse 2004).



This broad category of fraud includes asset misappropriation, corruption, and fraudulent financial reporting. Despite ongoing efforts to combat it, occupational fraud continues to represent a significant and growing risk to businesses and governments globally. Research suggests that fraud-related losses account for about five percent of annual business revenues (ACFE 2018; Button et al. 2011; Holtfreter 2008). When applied to the global GDP, these losses could represent a sum as staggering as \$4.7 trillion, based on 2020 real GDP figures, which is about ten times the combined GDP of 31 low-income countries. The covert nature of occupational fraud, which is often resolved discreetly to protect the victim's reputation, means that these figures likely represent a conservative estimate, with the true cost of fraud potentially being much higher and perhaps incomprehensible (Manning 2016).

The cost of occupational fraud necessitates heightened vigilance within the business community and among stakeholders. Acknowledging the severity of fraud losses highlights the necessity for a deeper understanding of the conditions and risks that precipitate such losses within organizations (ACFE 2018; Bolimos & Choo 2017; PwC 2018). This understanding is not merely academic; it holds practical significance for business leaders, practitioners, and scholars in developing robust responses to mitigate the incidence and impact of fraud.

Grasping the organizational susceptibilities to occupational fraud is instrumental in refining the strategies for its prevention, detection, and resolution. For instance, auditors and fraud examiners conventionally use risk assessment, including the risk of material misstatements, as a cornerstone in planning and conducting audits or investigations. The potential magnitude of losses from occupational fraud is often mirrored in the assessment of such risks, underscoring the direct correlation between

understanding specific vulnerabilities and the effectiveness of the countermeasures employed.

### **1.1.3 Definition Of Employee Fraud**

Employee fraud has been implicated in numerous studies over the past few decades as one of the most common, pervasive, and expensive forms of crime (Astor 1972; Bacas 1987; Baker & Westin 1988; Clark & Holzer 1979, 1980; Delaney 1993; Franklin 1975; Friedrichs 2004; Greenberg & Barling 1996; Hayes 1993; Hollinger 1989; Hollinger & Clark 1983; Hollinger & Dabney 1995; Jaspan 1974; Jones 1972; Lary 1988; Lipman 1973, 1988; Mars 1982; Merriam 1977; Murphy 1993; Mustaine & Tewksbury 2002; Niehoff & Paul 2000; Robin 1969, 1970, 1974; Shepard & Dustin 1988; Slora 1989; Terris 1985; Thomas et al. 2001; Wimbush 1997).

Employee fraud cases involving employees and top management are continuously reported in all organizations across the globe (PwC 2016; 2018; 2020; ACFE Report to Nations on Occupational Fraud & Abuse 2018; 2020). According to Said et al. (2018), employee fraud is the term used to describe the purposeful or intentional misbehavior or misappropriation of a company's assets by its employees, which may result in losses for the company. Any action that involves misrepresenting one's position, abusing power, or impairing someone's ability to obtain personal gain is considered illegal. To put it another way, employee fraud is the term used to describe any criminal activity carried out by an employee or group of employees who use deception to bypass control vulnerabilities and obtain personal benefits. Thus, it causes their employers financial or non-financial harm. Types of employee fraud include embezzlement, ethical misconduct, misappropriation of assets, and petty theft.

#### **1.1.4 The Difference Between Occupational & Employee Fraud**

The difference between occupational fraud and employee fraud lies within their definitions, scope, and the entities involved in the fraudulent activities. While both terms are often used interchangeably, understanding their distinction is crucial for comprehensively addressing fraud within organizational settings.

Occupational fraud is a broad term that covers any fraudulent activity that results in financial or personal gain to the perpetrator at the expense of an organization. This type of fraud can be committed by employees, management, officers, or external parties such as vendors or customers, either independently or in collusion. The Association of Certified Fraud Examiners (ACFE) categorizes occupational fraud into three main types: asset misappropriation, corruption, and fraudulent financial statements (ACFE Report to Nations on Occupational Fraud & Abuse 2020). These categories cover a wide spectrum of fraudulent activities ranging from theft of company assets, engaging in bribery and conflicts of interest, to manipulating financial records to present a more favorable view of the organization's financial health than is accurate. Occupational fraud is particularly insidious as it not only leads to direct financial losses but can also severely damage an organization's reputation and trustworthiness (Singleton & Singleton 2010; Kranacher, Riley & Wells 2011).

Employee fraud is a subset of occupational fraud. It specifically refers to fraudulent acts committed by an organization's employees against their employer and involves the misuse or misappropriation of the organization's resources or assets for personal gain. Examples include payroll fraud, expense reimbursement fraud, theft of physical or digital assets, and the creation of ghost employees to embezzle funds. The key distinction of employee fraud is its focus on the actions of employees as opposed to the broader category of perpetrators that occupational fraud encompasses. This focus

highlights the importance of internal controls, employee monitoring, and ethical culture in mitigating the risk of fraud within organizations (Singleton & Singleton 2010; Kranacher, Riley & Wells 2011).

Understanding the difference between occupational and employee fraud is crucial for developing effective fraud prevention and detection strategies. While occupational fraud provides a comprehensive view of fraudulent activities within an organization, employee fraud zooms in on the misconduct by internal staff. Occupational fraud necessitates a broader scope of vigilance that includes external parties, whereas employee fraud emphasizes internal controls and an ethical organizational culture.

However, for the purpose of the research, the terms occupational fraud and employee fraud might be used interchangeably as the existing literature has not differentiated between the two. Whatever research has been conducted by scholars on employee-related fraud has been covered under the scope of occupational fraud.

## **1.2 The Cost Of Employee Fraud**

Fraud represents a significant challenge to the global economy, affecting businesses across all sectors and regions. Its impact is far-reaching, including direct financial losses, reputational damage, and various indirect costs. The Association of Certified Fraud Examiners (ACFE) regularly reports on the cost of fraud globally through its "Report to the Nations on Occupational Fraud and Abuse," which offers comprehensive insights into fraud's economic impact. The Association of Certified Fraud Examiners (ACFE) estimates that occupational fraud costs businesses worldwide more than \$4.7 trillion a year. This is the equivalent of around 5% of the sales of an average business. Every case results in an average loss above \$1.78 million.

### **1.2.1 Direct Costs Of Fraud**

The most immediate and apparent cost of fraud is the direct financial loss incurred by businesses and society. These losses include stolen funds, assets misappropriated, or unauthorized transactions that directly subtract from an organization's bottom line. According to the Association of Certified Fraud Examiners (ACFE) 2020 report, organizations lose an estimated 5% of their annual revenue to fraud, which, when extrapolated to the global economy, represents a staggering figure likely amounting to hundreds of billions of dollars annually (ACFE Report to Nations on Occupational Fraud & Abuse 2020). These direct losses are the first and most quantifiable impact of fraud, but they only represent the tip of the iceberg in terms of the total cost.

### **1.2.2 Indirect Costs Of Fraud**

Beyond direct financial costs, fraud inflicts several indirect costs that can significantly burden organizations, including:

- **Legal and Investigation Costs:** Upon discovering fraudulent activities, organizations often need to engage legal counsel and forensic investigators to understand the scope of the fraud, pursue recovery of losses, and navigate potential legal proceedings. These services are usually costly and time-consuming (Smith et al. 2018).
- **Increased Insurance Premiums:** Companies that fall victim to fraud may face increased premiums for fraud insurance or find it more difficult to obtain comprehensive coverage without significant cost increases (Jones 2019).
- **Regulatory Fines and Penalties:** In cases where fraud involves regulatory non-compliance, organizations may be subjected to fines and penalties, further exacerbating financial losses (Doe & Roe 2017).

- **Reputational Damage:** One of the most insidious indirect costs is the reputational damage suffered by organizations. The loss of trust from customers, investors, and partners can have long-term implications on market position, sales, and business opportunities. Restoring reputation requires significant effort and resources, often involving public relations campaigns, improved governance structures, and transparency initiatives (Public Company Accounting Oversight Board [PCAOB] 2021).
- **Operational Disruptions:** Fraud leads to operational disruptions as businesses may need to halt certain operations to investigate the fraud, implement new controls, or retrain staff. These disruptions can lead to lost productivity and revenue (Taylor & Brown 2020).

### **1.2.3 Intangible Cost Of Fraud**

The intangible costs of fraud are difficult to quantify, yet they are significantly impactful, such as:

- **Employee Morale and Trust:** Discovery of employee fraud can erode trust within an organization, leading to decreased employee morale and engagement. The sense of betrayal and the subsequent atmosphere of suspicion undermines teamwork and productivity (Smith 2019).
- **Customer Trust:** For businesses that suffer fraud, especially those that compromise customer data, rebuilding customer trust can be a long and challenging process. The perception of a company's inability to safeguard data leads to customer attrition and decreased acquisition rates (Johnson 2021).
- **Market Value:** Publicly traded companies that experience significant fraud witness immediate negative reactions in their stock price, reflecting the market's diminished confidence in management and the company's future profitability (Securities and Exchange Commission 2020).

#### **1.2.4 Preventive Cost Of Fraud**

Fraud prevention and detection measures are proactive costs intended to mitigate the risk of fraud. They represent a significant allocation of resources that could otherwise be invested in core business activities (Greenwood & Shaw 2022). This includes the cost of implementing and maintaining sophisticated security systems, conducting regular audits, training employees on fraud awareness, and potentially hiring dedicated anti-fraud personnel (ACFE Report to Nations on Occupational Fraud & Abuse 2021).

#### **1.3 Research Problem**

Although current theories on occupational and employee fraud offer valuable insights into the motivations and behaviors of employees involved in fraudulent activities, it is important to acknowledge the gaps in the existing literature. Various theories pertaining to employee fraud have been formulated based on case studies, surveys, and interviews conducted within distinct industries or organizations. Hence, the extent to which these theories can be applied to alternative industries or contexts may be constrained. The generalizability of findings and conclusions derived from a single industry may not be universally applicable, underscoring the importance of employing more diverse and representative research samples. The majority of research on occupational fraud is conducted using a cross-sectional design, which involves collecting data at a single point in time. Longitudinal studies that monitor fraudulent behaviors over an extended duration are relatively infrequent in occurrence. Current theories oversimplify and generalize the intricate permutations of factors contributing to employee fraud. Various individual, situational, and organizational factors shape the complexity of human behavior. The existing theories neglect various psychological, social, or

organizational dynamics, which can result in a limitation of their explanatory capacity. While numerous theories on occupational fraud place significant emphasis on individual factors such as motivation, opportunity, and rationalization, the role of organizational factors is often overlooked or given limited attention. The occurrence and detection of fraud can be significantly influenced by factors such as organizational culture, leadership, control systems, and internal processes. There is a need to examine the intricate relationship between individual and organizational factors in understanding the occurrence of employee fraud. Further, the swift progression of technology and evolving work environments pose newer challenges and prospects in the study of employee fraud. The current theoretical frameworks may not sufficiently encompass the implications of emerging technologies, such as the proliferation of remote work, the prevalence of digital transactions, and the escalating fraud risks.

Every business is prone to Fraud, and Fraud does not discriminate the businesses by size, industry, geography, or any other factor. People and money have always been a combustible concoction since the beginning of time. The profit margin of quite a few businesses does not even touch 5% of their sales. Hence, the severity of Fraud cost can be understood in the terms that most businesses succumb to Fraud even after being financially viable. The verdict of the above statement is that businesses certainly lose money if they do not fight Fraud which has posed a greater threat to the global financial system (Lakis 2008; Mackevius 2012).

However, preventing Fraud is not a simple task; instead, it requires extensive and specialized knowledge of the company's economic affairs, potential fraud incidences, and the nature of these instances. However, according to Rezaee (2002), fraud practitioners have an essential responsibility, i.e., preventing fraud from occurring; thus, it is crucial to



analyze the reasons for the occurrence of fraud and possible motivations behind fraudulent conduct.

Businesses have struggled for many years to answer the mystery of "why people commit fraud." Numerous studies have been conducted throughout the years with the aim of better understanding fraudulent behavior. In order to understand the psychology of Fraud and the factors that drive fraudsters to perpetrate Fraud, many studies have been developed over time (Dorminey et al. 2012).

When it comes to studying corporate fraud, the literature in the field of corporate governance has not paid enough attention to employee fraud. Instead, it has focused on firms as the ones who commit fraud. First, most current Research still defines fraud at the firm level and uses firm-level data to measure fraud, e.g., litigation, restatements, and enforcement announcements (Karpoff et al. 2017) and focuses mainly on financial or accounting fraud (Hogan et al. 2008). However, these definitions only cover a small part of corporate fraud. The ACFE classifies fraud into three main types: corruption, asset misappropriation, and financial statement fraud. While 86% of fraud cases involve asset misappropriation (Employee fraud), only 9% involve financial statement fraud (White-Collar Crime). Second, current Research has focused on firm-level factors when looking for the causes of fraud (Bao et al. 2020; Dechow et al. 2011; Perols et al. 2017; Xu et al. 2022) and has not paid enough attention to employee-level factors that account for a larger part of the variation in fraud losses (Holtfreter 2008; Timofeyev 2015). According to a meta-analysis by Pusch and Holtfreter (2021), the number of individual predictors of white-collar crime is 76%, and the number of organizational predictors is only 24%.

The fraud triangle, the fraud diamond, the fraud scale, and the MICE model are among the most popular and well-accepted models for elucidating why people commit Fraud (Cooper et al. 2013; Free & Murphy 2013; Morales et al. 2014; Neu et al. 2013;

Sikka 2010a). However, the problem with the available literature is that the existing theories behind the motivation of fraud are so widely scattered that no one fits all conditions. The theories developed over time to study the psychology of fraudsters seem to have become redundant and do not fit the current arena of fraud instances. The fraud triangle thrived in 1953, almost seven decades ago, and a lot has changed since then. Hence, there is a dire need to look at new elements that may significantly contribute to finding the reasons behind "why people commit fraud?"

This research thoroughly examines the theories surrounding fraud motivation, from the traditional fraud triangle theory developed by Donald R. Cressey to the recent developments introduced in the field, and explores the viability of the existing fraud theories in the current business environment. Based on the findings, the need for developing an integrated fraud model is discussed. Hence, this study explores the pivotal influences of employee fraud and suggests prevention strategies that could be adopted by organizations against employee fraudsters rather than focusing more on "Why employees commit fraud."

#### **1.4 Research Question:**

The central research question of this study seeks to explore "How Can Organizations Minimize Fraud Perpetrated By Employees?"

Hence, this study explores what strategies and practices organizations can implement to curtail the vulnerabilities and opportunities for fraudulent activities within their operations. Specifically, the study aims to explore the common fraudulent methods adopted by employee fraudsters, organizational weaknesses causing vulnerabilities to such fraudulent actions, and identify the early warning signs of fraud using both organizational and behavioral indicators to limit the scope for employee-induced fraud.

This includes a thorough examination of organizational weaknesses in internal controls, corrective actions, making use of fraud red flags, and other preventive measures. By scrutinizing these elements, the research attempts to provide a comprehensive understanding of how organizations can fortify their defenses against the detrimental impact of fraud, thereby safeguarding their assets, reputation, and stakeholder trust.

The research problem highlights the persistent and evolving nature of employee fraud despite the wealth of insights provided by existing theories and studies. These insights, while valuable, have not led to a significant reduction in fraud incidents, pointing to gaps in the literature and the application of these theories across various industries and contexts (ACFE Report to Nations on Occupational Fraud & Abuse 2020). The research question directly addresses these gaps by exploring actionable strategies and solutions that can be universally applied to mitigate the risk of fraud.

### **1.5 Research Objectives:**

The objective of this research is to suggest a course of action that will assist organizations in preventing employee fraud, which could subsequently contribute to the reduction of fraud in the organizations. Whilst this study investigates the real fraud conviction cases from the business organizations from the United States of America, it is expected that the findings will be applicable to all industries, worldwide. It is anticipated that the research findings will encourage organizations to re-examine their approach to combating fraud, and to focus on ensuring that the fraudulent activities of the employees are put under vigilance, thus reducing the system weaknesses inducing fraud.

To effectively address the main research question of how organizations can achieve the minimization of fraud caused by employee fraudsters, the study outlines three specific research objectives, which are designed to explore different dimensions of

employee fraud, providing a comprehensive understanding that will explore effective fraud minimization strategies.

The first objective focuses on preparing a list of various possible methods/fraudulent actions taken by fraudsters to exploit the opportunities.

The second objective of the study is to identify various opportunities utilized by fraudsters to commit fraud in their employer organization. The focus is on finding common vulnerabilities within organizational structures and processes that create opportunities for fraud. By understanding these vulnerabilities, the study aims to pinpoint specific areas where organizations can strengthen their defenses against fraud. This knowledge directly supports the main research question by offering insights into targeted strategies for fraud minimization that are tailored to the unique needs and risk profiles of various organizations.

The third objective focuses on suggesting red flags for fraud that organizations may look for in order to prevent and detect fraud in a timely manner. By analyzing behavioral and organizational red flags, the research aims to provide actionable recommendations for organizations seeking to minimize the incidence of employee fraud. This objective directly contributes to answering the main research question by identifying best practices in fraud prevention that can be adopted by organizations to protect against employee fraud.

Collectively, these objectives support the research question by dissecting it into manageable, focused inquiries that offer an understanding of how organizations can successfully minimize fraud caused by employee fraudsters.

## **1.6 Research Design**

This study used the techniques of qualitative content analysis, gathering information from openly accessible secondary sources. The research design is discussed in detail in chapter 3.

However, for an introduction purpose, 157 real conviction cases related to fraud were chosen from the press releases of the website of the Department of Justice, USA from the period 2021 to 2023, selected randomly to analyze the conditions giving rise to employee fraud.

Since the Department of Justice, USA, hears cases involving fraud, child and human trafficking, firearm abuse, medical crimes, and other crimes, the data is narrowed down from 1500 to 157 cases exclusively related to conviction cases that belong to employee fraud. These cases were discussed with experts and content analysis of the transcribed interviews was conducted to gather common patterns and themes. The findings are reported in chapter 4-7 along with the conceptualization of a new Integrated Fraud Model that acts as practical guidance for the organizations to minimize fraud.

## **1.7 Research Limitations**

It is important to note that the research design for this study has certain limitations that must be considered when interpreting the findings.

The study is based on qualitative research. Unlike quantitative research, which relies on statistical analysis, qualitative research often involves the interpretation of data, which can introduce subjectivity. The researcher's perspectives, biases, and interpretations can influence the analysis and conclusions, potentially affecting the objectivity of the findings.

This qualitative research typically focuses on samples of real conviction cases from the website of the Department of Justice, USA. The depth and detail provided by the study are specific to the particular contexts, times, and participants studied, limiting the applicability of results to other settings or groups.

The qualitative analysis, primarily based on secondary data from the Department of Justice, USA, limits the scope to documented cases of fraud, potentially overlooking undocumented or lesser-known instances.

The study's reliance on case analyses from a specific time frame (2006-2023) may not capture the evolving nature of fraud in different economic or technological conditions.

The findings, particularly those related to the most common vulnerabilities in organizational structures that increase fraud opportunities, are specific to the contexts of the analyzed cases.

### **1.8 Significance of The Study**

There has been limited research and resultant progress on the topic of employee fraud. There are various constraints for not having done so far. Most businesses don't report fraud due to social barriers. That is why an exponential rise in organizational crime rate smears all the countries around the globe. The concept of fraud is of great sensitivity to organizations, as it often entails legal and reputational implications. The limited availability of data for researchers may arise due to the hesitancy of certain organizations to disclose comprehensive information regarding incidents of fraud. Consequently, investigating fraudulent activities presents inherent difficulties, thereby necessitating researchers to depend on data that is self-reported or obtained through surveys, both of which may possess certain limitations. Further, instances of underreporting fraud are

often observed in various contexts attributable to individuals' apprehension regarding retaliation, adverse publicity, loss of faith, or a general lack of confidence.

Underreporting of fraud poses a significant challenge for researchers in their pursuit of obtaining precise and all-encompassing data pertaining to the frequency and characteristics of fraudulent activities. Certain studies pertaining to employee fraud may choose to examine various forms of misconduct, including corruption, embezzlement, and insider trading, without explicitly classifying them as instances of "fraud." The potential consequence of this is the emergence of a fragmented corpus of scholarly works pertaining to different types of occupational offenses rather than a unified and comprehensive body of literature specifically focused on the subject of employee fraud. The occurrence of fraud is a complex and multidimensional phenomenon subject to the influence of many factors. These factors encompass a wide range of disciplines, such as psychology, economics, criminology, and organizational behavior. The investigation of fraudulent activities within organizational settings often necessitates the collaboration of multiple disciplines. The existing body of literature on the subject may give rise to an impression of insufficiency despite the potential presence of research within academic spheres. Hence, organizations must first identify what can be various types of fraud, what motivates an employee to compromise their integrity while committing fraud, what opportunities are available to a fraudster or what opportunities can be created by them, what rationalization they may offer, thinking like a fraudster, and more importantly how to be able to prevent a fraud occurring in an organization.

As per ACFE, Report to Nations on Occupational Fraud and Abuse, 2020, almost 86% of frauds were categorized as occupational or employee fraud. To demotivate occupational fraudsters, for example, a few countries have developed "Whistleblower Policies." However, even after a whistleblower policy is in place, most employees are

deterred from reporting fraud because they fear consequences (Vega & Comer 2005). Studies have shown that top management itself is the perpetrator of fraud most of the time (Dechow et al. 2009). Hence, this is a constraint in fraud prevention. There has been limited progress in classifying various such constraints according to their characteristics in a comprehensive manner.

The field of fraud prevention is complicated. The prevention of organizational vulnerabilities necessitates a thorough comprehension of the various factors that contribute to these vulnerabilities, including technological, human, and environmental aspects. A meticulous risk assessment is imperative in order to identify and evaluate potential threats and their potential impact on the organization. The intricate nature of fraud prevention poses a significant hurdle in offering universally applicable, comprehensive guidance to all organizations. Implementing effective fraud prevention measures necessitates meticulously considering various contextual elements, including the size of the organization and the specific nature of its operations. The inherent dynamism of fraud poses a significant challenge in formulating comprehensive guidelines that include a vast array of potential scenarios. The study shows that there is a lot more to do in financial fraud prevention and detection as, despite numerous efforts, there is no guarantee to eliminate fraud completely. Still, with new research in the field and analyzing the organizational weaknesses in detail, we can achieve fraud minimization.

Previous research shows that only limited work has been done by other scholars in the field of occupational and employee fraud. Whatever work has been done is mostly attributed to fraudulent financial statements (White-Collar Crime) (ACFE Report to Nations on Occupational Fraud & Abuse 2022). The idea of this research would be to analyze, for the benefit of corporates and society as a whole, how organizations can protect themselves from the fraudulent activities of their employees.



## **1.9 Dissertation Outline**

This chapter serves as an introductory exploration into the pervasive issue of fraud and its substantial costs to both organizations and society at large. It begins by framing the research question, focused on devising strategies to mitigate internal fraud perpetrated by employees. Subsequently, it delineates the principal objectives of the study aimed at addressing this inquiry. Additionally, it offers a preliminary overview of the research methodology along with its inherent limitations. Finally, the chapter underscores the significance of this research endeavor.

In Chapter 2, an in-depth analysis is undertaken on established fraud theories, including the Fraud Triangle, the Fraud Diamond, the Fraud Scale, the MICE model, and the SCORE model, evaluating their applicability within the contemporary business landscape. The overarching aim of this chapter is to establish a foundational framework drawing upon existing literature, thereby exploring the subsequent investigation.

Chapter 3 provides a comprehensive elucidation of the research methodology employed, encompassing aspects such as dataset selection, participant recruitment, and analytical techniques.

Chapters 4, 5, and 6 serve as repositories for the empirical findings of the research. Each chapter furnishes a succinct overview of the findings derived from the conducted analyses, followed by a detailed exploration of these findings.

Chapter 7 constitutes the concluding segment of this dissertation. It culminates in the conceptualization of the Integrated Fraud Model, elucidating the intricate interplay among its constituent elements. Furthermore, this chapter proffers pragmatic recommendations for industry stakeholders derived from the research insights and delineates avenues for prospective inquiry.

## CHAPTER 2: LITERATURE REVIEW

This chapter seeks to examine the existing theories related to occupational fraud and their viability in the current organizational landscape. With the analysis of the results, the study further explores the significant weaknesses in the existing fraud models.

Edwin H. Sutherland, a criminologist at Indiana University, was one of the first researchers in the field of employee or occupational fraud. Sutherland challenged the common belief that the urge to commit Fraud was the product of some mental paucity or socioeconomic defect. For this purpose, he initially focused on the professional actions of the elite business executive. Later, Sutherland crafted differential association theory, according to which criminal behavior is a learned trait, just like learning a language (Donegan & Ganon 2008, p. 3; O'Connell 2007, p. 733–784). He proposed that learning to commit fraud entailed developing the necessary technical proficiency and the attitudes, urges, rationalizations, and reasons of the criminal mind.

According to research done by Donald R Cressey (1953), a person may commit fraud if there is pressure, opportunity, and rationalization” (Purnamasari & Amaliah 2015; Tuanakotta 2012). Crime theories must contribute to the prevention of crime. Recent "opportunity" crime theories have highlighted principles that are grounded in reality and ready to implement. The routine activity theory, rational choice theory, and crime pattern theory are some of the theories that are based on elements of opportunities for fraud or crime. These views are based on the adage that "opportunity makes the thief” (Felson. M. and Clarke R.V., 1998).

After Sutherland, Donald R. Cressey (1953) developed the Fraud Triangle, which has been reformed and reconceived since its introduction. The fraud triangle considers the factors that induce an employee to commit a crime. The three corners of the fraud

triangle are perceived pressure, perceived opportunity, and rationalization. The fraud triangle has been reshaped by other criminologists into fraud scale, fraud diamond, etc.

Further, Dr. Steve Albrecht analyzed 212 fraud cases committed in the early 1980s. He gave an in-depth questionnaire to internal auditors familiar with the fraud instances. In one area of the study, which focused on the frauds' motivations, some likely traits emerged, including gambling and personal debts, a desire for personal gain coupled with dissatisfaction with compensation, collusion with customers, and a desire to "beat the system." Albrecht and his colleagues discovered that "fraud is difficult to predict" and "occupational fraud offenders are hard to profile." Hence, he conceived the theory of fraud Scale, replacing integrity with rationalization as originally developed by Donald R Creasey.

Like fraud triangle and fraud scale theories, there are other theories that criminologists have developed from time to time. After the fraud scale, David Wolfe and Dana Hermanson developed the fraud diamond theory in 2004. In the fraud diamond theory, one additional " capability " element was added to the existing fraud triangle theory. The other theories that evolved over time are "The Fraud Pentagon," "The MICE Model," "The SCORE Model," etc. Two of these theories have been critically examined in the "Literature Review" section of this document.

There are few justifications for studying fraudulent behavior. The existing theories of fraud literature need to be updated according to the current times. Fraud Triangle was first coined in 1953, over seventy years from now (Duffield & Grabosky 2001). A lot has since changed in terms of technological development, the profile of fraudsters and victims, the amount involved, etc. According to reports by ACFE, Fraud results in significantly greater losses than traditional property crimes such as theft, robbery, and burglary (ACFE Report to Nations on Occupational Fraud and Abuse 2020).

Beyond financial loss, Fraud causes severe physical and emotional harm to victim organizations. Fraud raises people's costs of living, weakens consumer confidence, and depresses the economy (West & Bhattacharya 2016).

## **2.1 Brief Overview**

When they occur, occupational frauds result in huge financial loss and dilapidate the organization's stake. If a material fraud is discovered, it shakes the investors' confidence in business, resulting in corroding. With the advancement of business practices and more reliance on technology, a silhouette of potential occupational fraud walks along with business development. The concept of occupational fraud is not new to the business world; it has been committed since time immemorial. In general terms, fraud is a deplorable intentional deception, whether by omission or commission, causing the victim to suffer financial loss and the fraudster to realize a gain. Commonly, fraud includes four elements: A knowledge of materially false statements, victim reliance on false statements, and Damages resulting from the victim's reliance and intention of deception.

Occupational fraud is a problem that demands immediate attention. Top management or company personnel may commit employee or corporate fraud, also called white-collar crime. White Collar Crime is also connoted as Occupational Crime or fraud. However, there remains a difference between the two. Occupational Fraud is defined as the misuse of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. The Association of Certified Fraud Examiners (ACFE) provides extensive insights into occupational fraud, highlighting it as a subset of fraud committed by an individual or individuals within an

organization to benefit personally at the expense of the organization. Occupational fraud can include actions like embezzlement, payroll fraud, and procurement fraud.

White-collar crime, a term coined by sociologist Edwin Sutherland in the late 1930s, refers to financially motivated, nonviolent crimes committed by business and government professionals. It encompasses a wide range of frauds committed by business and government professionals. White-collar crimes include, but are not limited to, financial fraud, bankruptcy fraud, bribery, insider trading, and cybercrime. It involves deception, concealment, or violation of trust and is not dependent on the application or threat of physical force or violence.

The main difference between the two lies in their scope and context. Occupational fraud is a specific form of white-collar crime that occurs within the context of employment, where the fraudster exploits their position within the organization to commit fraud (Green 1993). On the other hand, white-collar crime is a broader category that includes any nonviolent crime committed for financial gain, regardless of the employment context. Therefore, while all occupational frauds can be considered white-collar crimes, not all white-collar crimes are occupational frauds.

The Association of Certified Fraud Examiners (ACFE) describes occupational fraud as abuse of a position of trust. The term "Occupational Fraud" has been defined by many with different connotations since then. Hence, occupational fraud is a kind of fraud where an employee intentionally misappropriates corporate assets or manipulates resources by using their position of employment within an organization. Since it violates an employee's fiduciary duty to the company, all types of fraud, including occupational fraud, are committed covertly. The goal of fraud is to provide the perpetrator with a direct or indirect financial gain at the expense of the organization.

Unlike the usual criminal activities in any culture, which are mostly public and visible, occupational frauds are disguised and committed in the workplace and usually do not involve physical danger. However, this does not make it any less harmful or costly to society. One of the most challenging aspects of occupational fraud is that we only hear about the cases that come to light, and the rest go unnoticed. Further, it is not easy to list down the wide variety of frauds perpetrated differently by different fraudulent minds. However, there could be some common elements inducing a person to commit fraudulent financial activities.

## **2.2 Preliminary Literature Review**

Fraud is a raging concern. What makes it more pernicious for society is that the past research conducted on fraud and its motives is very limited in scope (ACFE Report to Nations on Occupational Fraud & Abuse 2002). As discussed, fraud is the sub-set of crime, which essentially means that all frauds are crimes, but all crimes are not frauds. Hence, the question arises if fraud is a subset of crime if the theories of crime can be directly applied to the study of fraud literature. The main motives behind crime may be greed, revenge, or ego (Cook 1986; Cornish & Clarke 1986; Cohen & Cantor 1981; Cohen & Felson 1979; Cohen, Kluegel & Land 1981; Felson & Cohen 1980, 1981; Hindelang, Gottfredson & Garofalo 1978). In contrast, the main motive behind fraud is the insatiable need to benefit oneself. Fraud is a human behavior that involves deception, deliberate intent, the intensity of desire, breach of trust, utilization of opportunity, and rationalization (Morales et al. 2014, p. 177; Albrecht & Albrecht 2004, p. 5). Therefore, psychological reasons should be sought in order to comprehend the fundamental causes of fraud.

Organizations are exposed to various forms of fraud perpetrated by employees. Not only organizations but many people are impacted by these fraud occurrences, including management, employees, auditors, creditors, and investors (Abagnale 2002). Businesses have been working to lower, prevent, and proactively manage the risk of fraud. Organizations face significant difficulty in preventing fraud since fraudsters are constantly coming up with newer ways to defraud organizations, and they typically try to hide the trail to avoid being caught.

Therefore, businesses should determine the motivation of fraudsters, available opportunities, vulnerabilities organizations are exposed to, and the fraudulent acts that are committed by the employees. Using various approaches, fraud research has looked into elements that might motivate people to commit fraud (Becker et al. 2006; Boyle et al. 2015; Dellaportas 2013; Murphy & Free 2016; Schuchter & Levi 2013; Zakaria et al. 2016). These researches have offered crucial insights into the motivations behind why people engage in fraudulent behavior. Most fraud research has focused only on the elements of the fraud triangle (Cressey 1953; Huber 2016; Ramamoorti et al. 2013; Wells 2005). Even though the Fraud Triangle provides a baseline to explore aspects influencing fraud, many more variables may affect a person's desire to commit fraud.

There have been calls to perform cross-disciplinary research incorporating well-established sociological, psychological, and criminological theories to advance fraud research beyond the fraud triangle and the fraud diamond (Ramamoorti 2008; Trompeter et al. 2014). By outlining two established theories from criminology (Routine Activity Theory and Self-Control Theory) that apply to fraud research, this research seeks to address the request for expanding fraud research beyond the fraud triangle.

### **2.3 Fraud Theories**

The Literature review highlights the studies conducted by different sociologists and criminologists to understand the motivation and psychology of employee fraudsters. The Fraud Triangle Theory (Donald Ray Creasey 1953) and the Fraud Diamond Theory (David Wolfe & Dana Hermanson 2004) are among the most commonly used and highly recognized models for understanding why people commit fraud. Also, other fraud theories developed over time, such as the fraud scale (Steve Albrecht 2008), MICE model (Kranacher et al. 2010), Fraud pentagon (Marks 2012), and SCORE (Vousinas 2019) model are all based on tenets of the fraud triangle. In all the theories mentioned above, there have been few reforms in the already presented elements of the fraud triangle; for example, fraud scale replaces rationalization with integrity, fraud diamond adds one more element of the capability to the existing elements of the fraud triangle, fraud pentagon adds two angles of "competence" and "arrogance" to the existing elements of the fraud triangle, MICE model introduces Money, Ideology, Coercion, and Ego as elements of the theory, and SCORE models coins Stimulus, Capability, Opportunity, Rationalization, and Ego as the elements of fraud research. In one view or the other, a critical analysis of all the theoretical frameworks suggests that all the elements of different theories have a resemblance with each other; for example, the Stimulus defined in the SCORE model is nothing, but the financial pressure as defined by Creasey in the fraud triangle. The ideology and Ego of the MICE model are based on tenets of Rationalization whereby the fraudsters at senior hierarchal levels rationalize their criminal conduct by shaping the ideology of their actions.

The Fraud Triangle and Fraud Diamond Theory make an effort to highlight the factors that motivate fraudsters to perpetrate fraud against their employer by identifying the psychological causes of fraud. They pinpoint the conditions that encourage fraudulent



behavior. Poor internal controls, for instance, will enable a fraudulent mind to perpetrate fraud in an organizational contest. However, it is crucial to underline the causes of employee fraud so that controls can be implemented to prevent and deter those causes. The Fraud triangle theory asserts the presence of three elements (pressure, opportunity, and rationalization) together for fraud to perpetuate. Before moving on to the theoretical explanations, an analysis of the fraud triangle and fraud diamond models for explaining why people commit fraud is being presented here in order to emphasize the existing theoretical foundations, as well as to identify grey areas and scope for improvement.

### **2.3.1 The Fraud Triangle**

The fraud triangle is the most widely acknowledged paradigm for explaining why people commit fraud. Donald Ray Cressey (1953), a sociologist whose research centered on embezzlers, or "trust violators," established this theory.

One of the elements of the fraud triangle signifies a Non-shareable Financial Pressure. The second element stands for perceived opportunity, while the third indicates rationalization. The first leg of the fraud triangle is pressure. Pressure, according to Cressey, is a non-shareable financial situation or motivation that leads to dishonesty.

The second leg of the fraud triangle is Perceived Opportunity. According to the fraud triangle theory, an employee will not commit fraud if they have a non-shareable financial pressure only. The ability to perpetrate fraud is subject to the presence of opportunity. Put another way, the employee must believe they have an opportunity to perpetrate the crime without being caught.

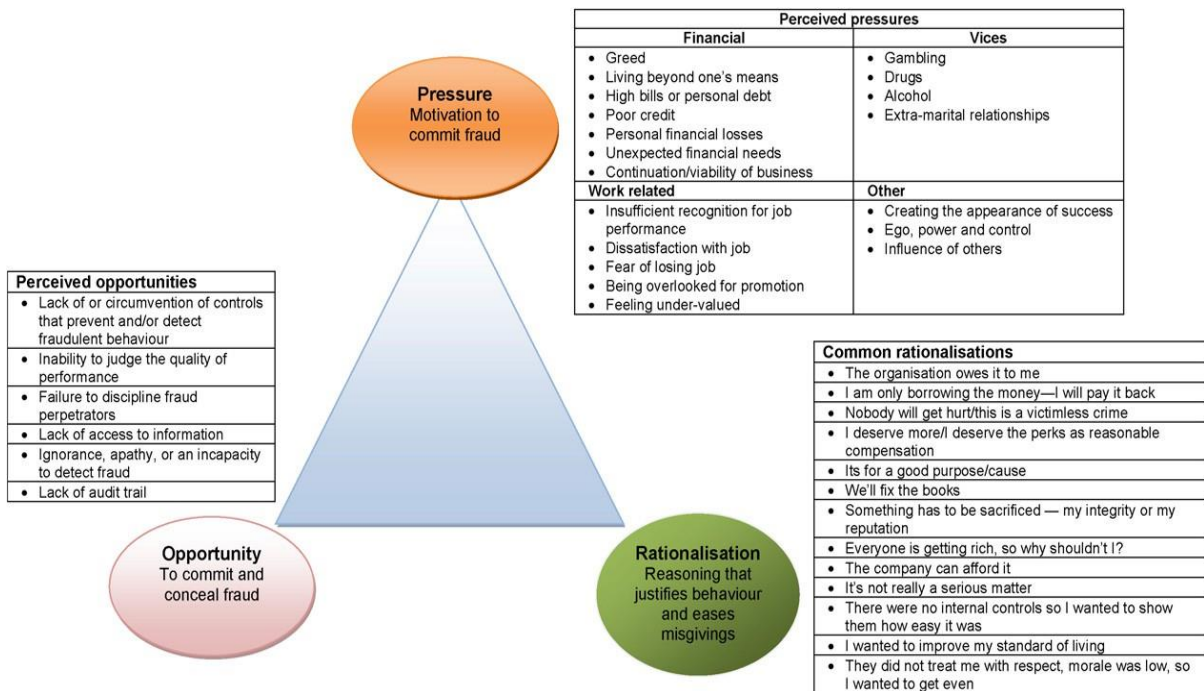


Figure 1 - Fraud Triangle (Source: Steve Albrecht, 1982)

According to Cressey, the perceived opportunity has two components: general information and technical skill. The understanding that the employee's position of trust may be violated is known as general information. This knowledge could come from knowledge about prior embezzlements, witnessing dishonest behavior by other employees, or simply being aware that the employee is in a position where he can exploit his employer's trust in him. The talents required to commit the violation are referred to as technical skills. These are frequently the same skills that the individual requires for the smooth functioning of his job.

Rationalization is the third and last component of the fraud triangle. Rationalization permits the fraudster to justify his illegal conduct while maintaining his image as trustworthy. Rationalization is an essential component that must be present prior to the occurrence of the crime. In fact, rationalization is a driving force behind crime.

Since the embezzler does not consider himself a criminal, he must defend his wrongdoings before doing them.

Cressey discovered that the embezzlers viewed their actions as essentially non-criminal, justified, or part of a larger pattern of irresponsibility for which they were not entirely responsible. He also discovered that trust offenders' rationalizations were frequently tied to their positions and the manner in which they committed the violations. For a trust violation to occur, all three legs of the fraud triangle must be present.

### **2.3.2 The Fraud Scale**

Albrecht, Romney & Howe (1984) coined the fraud scale, which suggests that each fraud incidence requires three essential elements: pressure, opportunity, and integrity. Thus, this model replaces rationalization with the integrity of fraudsters.

Personal integrity has the advantage of being a more visible attribute than rationalization (Dorminey et al. 2010).

According to Albrecht (2008), compared to someone with low integrity, a person with higher integrity is less likely to commit fraud. Hence, if a person breaks the law under pressure and opportunity, it indicates that they lack integrity.

### **2.3.3 The Fraud Diamond**

After the advent of the fraud scale, the need for refinement of the fraud theory was further perceived. Resultantly, David Wolfe & Dana Hermanson (2004), came up with the idea of the “Fraud Diamond.”

It was observed as an expansion of the fourth element of the fraud triangle theory, namely “Capability.” The authors articulated that an individual's characteristics, personality behaviors, and capabilities influence the occurrence of fraud.

The authors also claimed that pressure might exist with opportunity and rationalization. However, if an individual's capability to commit fraud is considered, it may give more weight to the fraud's occurrence.

According to Mackevicius (2012), it is not always possible for each person with the motivation, opportunity, and realization to commit fraud due to a lack of skill to conceal it. In the words of Abdullahi and Mansor (2015), "The potential perpetrator must have the capability to perpetrate fraud."

The fraud diamond also shows that significant frauds are perpetrated by individuals who are clever, deliberate, knowledgeable, innovative, and who have a great understanding of organizational controls. Ramamoorti (2009), for example, discovered that wealthy and influential people were involved in community fraud. These individuals have strong egos and believe they will never be caught.

According to the ACFE (2020) survey, the majority of frauds are perpetrated by management and upper-level executives, implying that these people have a high level of competency in the business and are seen as trustworthy individuals due to their prominent roles.

#### **2.3.4 The Fraud Pentagon**

Marks (2012) discovered the "Fraud Pentagon" as a further advancement to the fraud triangle by Donald Cressey. "Competence" and "Arrogance" are other elements added to understand fraud occurrence.

Competence is understood as an individual's capacity to commit any illegal, fraudulent act. The arrogance can be linked to the theory of capability by Wolfe and Hermanson.

Arrogance is a characteristic of an individual who believes they have power over anything in the organization and disregards organizational internal controls.

### **2.3.5 The MICE Model**

Kranacher et al. (2010) suggested that Money, Ideology, Coercion, and Ego acronym MICE are the driving forces for fraud. According to Kranacher, most financial frauds are committed due to greed for money.

Ideology is nothing but rationalization again. For a person, killing someone is a crime, but stealing money for survival is not. In both cases, crime occurs, which solely depends on the ideology of that very person. Hence, ideology justifies stealing money or engaging in fraudulent acts to attain some greater good that is consistent with their values.

Coercion occurs when people are unwillingly forced to become part of a fraud scheme. However, this is most likely that these people turn into whistleblowers subsequently.

People typically do not like to lose their reputation or position of authority in front of their community or family. Hence ego can be a motivator for fraud.

### **2.3.6 The SCORE Model**

Further expansion in the field of fraud theories has been the development of the SCORE model, which offers improvement in understanding the primary variables that contribute to the commission of fraud. Stimulus, Capability, Opportunity, Rationalization, and Ego are the elements of this approach.

The first four elements of the model (Stimulus, Capability, Opportunity, and Rationalization) come from the Fraud Diamond, while the ego is added to understand the significant determinants of fraudulent activities.

The urge to commit fraud is known as stimulus (or incentive), and it can be both financial and non-financial in form. High financial needs, work-related pressures, professional aspirations, etc., are all examples of stimulus.

When pressure, opportunity, and rationalization are present, capability refers to the human ability actually to perpetrate fraud. Many frauds, particularly multibillion-dollar financial statement frauds, would not have occurred if the capable person with the required skills had not carried out the intricacies of the scheme.

Opportunity opens the door, and incentives entice the potential fraudster to walk through it. However, the individual must be capable of walking through it. Hence, the ability to commit fraud is known as an opportunity. The culprit feels they can plan and carry out fraudulent conduct without being detected. It should be noted that the perpetrator must view opportunities as genuine. Studies on fraud have found that the position and authority of personnel within the organization create opportunities.

Rationalization refers to the act of justifying the fraudulent act. Because many fraudsters see themselves as honest, everyday people rather than criminals, they must devise a rationale to make the act of fraud more acceptable to them.

The sense of superiority, mastery, and adoration of others appears to be one of the critical motivations for committing white-collar crimes (Scotland 1977). Further, aspects of motivation that may apply to some or all types of fraud include financial strain and ego (Duffield & Grabosky 2001). This can refer to having power over individuals as well as situations.

## 2.4 Detailed Investigation Of Fraud Triangle

The Fraud Triangle, developed by Dr. Donald Cressey, is a foundational framework for understanding the motivations behind fraudulent behavior. It posits that fraud occurs when there is a convergence of pressure, opportunity, and rationalization. Despite its widespread adoption and utility in academic and professional fields, the dynamism of fraud in today's technologically advanced and globally interconnected society calls for a more detailed analysis and review of the Fraud Triangle. This necessity arises from several critical areas.

Firstly, technological advancements and globalization have exacerbated the evolution of fraud. It introduces complex challenges missed in Cressey's original model. As noted by Free and Murphy (2015), the digital era has introduced new mechanisms for the execution of fraud. It, thereby, questions the Fraud Triangle's adequacy in capturing these modern complexities (Button et al. 2015; Sikka 2010). Additionally, the original Fraud Triangle addresses internal pressures leading to fraudulent acts. However, contemporary research suggests that external factors—including societal, cultural, and technological pressures—significantly influence fraudulent behavior. Morales et al. (2014) argue for a more inclusive consideration of these external pressures, suggesting that they interact complexly with individual rationalizations and perceived opportunities to commit fraud.

The concept of "opportunity" within the Fraud Triangle also requires reevaluation in today's digital landscape. The anonymity and accessibility afforded by the technology have expanded the avenues through which fraud can be perpetrated. It necessitates understanding opportunities beyond physical access to resources (Neu et al. 2013). Rationalization, moral disengagement, and the normalization of unethical behavior within certain organizational cultures indicate a sophisticated rationalization mechanism that

deserves further exploration. Cooper et al. (2013) suggest that understanding the diversity in rationalization processes could lead to more effective strategies in combating fraud.

Moreover, introducing additional elements by subsequent models, such as the Fraud Diamond's inclusion of capability, underscores potential areas for expanding the Fraud Triangle. These models illuminate the complicated nature of fraud and the limitations of Cressey's original framework in capturing the factors contributing to fraudulent behavior (Free & Murphy 2015). The empirical validation of the Fraud Triangle and its adaptations are critical for future research. Validating the components of the Fraud Triangle with real-world data is essential for identifying gaps in the theory and informing the development of more comprehensive models that reflect the current realities of fraud (Dorminey et al. 2012).

The fraud triangle is the most widely acknowledged paradigm for explaining why people commit fraud. Donald Cressey (1953), a criminologist whose research centered on embezzlers, or "trust violators," established this theory. The Fraud Triangle is helpful for more research and study for criminologists and social scientists who are interested in investigating or researching fraud or embezzlement. The Fraud Triangle model is broadly based on studies conducted in the 1930s and 1940s by three academicians (Ernest Riemer, Edwin Sutherland, and Donald Ray Cressey) who studied a population of "middle-class white male embezzlers" (as defined by Swedish or US law, respectively) who had been convicted and were in prison at the time of the studies.

One of the elements of the fraud triangle signifies a "non-shareable financial pressure." The second element stands for "perceived opportunity," while the third indicates "rationalization."

According to Cressey, the first leg of the fraud triangle, i.e., pressure, is a non-shareable financial situation or motivation that leads to dishonesty. Most of the reported



fraud incidents entailed some form of financial pressure on the perpetrator (Albrecht et al. 2008; Wells 2011). Poor personal financial management, unemployment, and gambling habits can all lead to financial problems (Dellaportas 2013; Neu, Everett & Rahaman 2013; Rezaee 2005). Nearly 95% of all fraud cases have been committed as a result of the fraudster's financial circumstances (Albrecht et al. 2008). Employees who are under pressure from their employer to perform may lead to fraud, as was evidenced by fraudulent accounts at Wells Fargo (Bartlett et al. 2004; Baucus 1994; Hollinger & Clark 1983; Holton 2009; Peterson & Gibson 2003; Sridharan & Hadley 2018). Positive pressures can motivate people to accomplish their goals. When a person's career, salary, or employment are at risk, and their ambitions are unattainable or unachievable, they may turn to commit fraud (Howe & Malgwi 2006; Kelly & Hartley 2010; Sakurai & Smith 2003). Employee motivation can be increased by offering incentives like bonuses, pay-related rewards, or meeting sales targets. However, in some circumstances, employment pressure from organizational structures and the financial interests of the management are also likely to encourage staff members to engage in fraudulent behavior in order to achieve those objectives (Sridharan & Hadley 2018). Even if pressures and incentives might not be sufficient to encourage fraud, they can still motivate people to defraud others (Albrecht, Albrecht, & Albrecht 2004; Sikka & Hampton 2005).

The second element of the Fraud Triangle theory is perceived opportunity, which enables fraud because internal controls and governance are weak (KPMG Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response 2006, 2008, 2010). Opportunity is a significant factor attributable to fraud (Albrecht & Albrecht 2004; Alleyne & Howard 2005; Dellaportas 2013; Fleak, Harrison, & Turner 2010; Kelly & Hartley 2010; Rae & Subramaniam 2008; Norman, Rose & Rose 2010). According to the fraud triangle theory, an employee will not commit fraud if he or she merely has a non-

shareable financial pressure. The ability to perpetrate fraud is subject to the presence of opportunity. Put another way, the employee must believe that he can perpetrate fraud without being caught. Organizations cannot control their employees' financial pressures or rationalizations, but they can ensure that internal control gaps do not exist that could be used by employees to commit fraud (Felson & Clarke 1998; Haelterman 2016; Tunley et al. 2018). Conditions are ideal for an employee to commit fraud once they believe there is an opportunity to do so, such as when there is a lack of segregation of duties, poor internal controls, or irregular audits (Nor et al. 2017; Norbit et al. 2017; Asmuni et al. 2015; Husnin et al. 2016; Hamid et al. 2011; Salin et al. 2017). In such situations, if one or the other elements, such as pressure, incentive, or rationalization, are present, fraud results are more disastrous. Both perceived pressure and perceived opportunity are the perceptions of the fraudster (Wells 2011). For one person, the pressure may be so grave that he engages in fraudulent behavior while another does not.

Similarly, one person may see poor internal controls as an opportunity to commit fraud while another may still deter engaging in fraud. It is all about individual perception (Wells 2011). Many things might influence a fraudster's opinions or ideas regarding opportunities to perpetrate fraud. An employee can see a lack of sound internal controls in the organization or the absence of the segregation of duties and think he can commit fraud without being caught. Similarly, an employee may observe a coworker who defrauds the company and remains undetected. If no disciplinary actions exist for an employee who has been found guilty of fraud, the perceived opportunity may also grow (Sausser 2007). Similar views are expressed by Kenyon and Tilton (2006) regarding the increase in the belief of opportunity by fraudsters as a result of poor monitoring and supervision, inadequate internal controls, a lack of an audit trail, and irregular job rotation. According to Cressey, the perceived opportunity has two components: general

information and technical skill. The understanding that the employee's position of trust may be violated is known as general information. This knowledge could come from knowledge about prior embezzlements, witnessing dishonest behavior by other employees, or simply being aware that the employee is in a position where he can exploit his employer's trust in him. The talents required to commit the violation are referred to as technical skills. These are frequently the same skills that the individual requires for the smooth functioning of his job.

Rationalization is the third and last component of the fraud triangle. Rationalization permits the fraudster to justify his fraudulent conduct while maintaining his image as a trustworthy individual (Hogan et al. 2008; Wells 2004). Rationalization is an essential component that must be present prior to the occurrence of the crime (Albrecht 2003; Ashforth & Anand 2003; Cohen et al. 2010; Cooper et al. 2013; Morales et al. 2014; Neu, Everett, & Rahaman 2013). Rationalization is a driving force behind crime (Akomea-Frimpong et al. 2016; Amin 2018). Since the embezzler does not consider himself a criminal, he must defend his wrongdoings before doing them. Cressey discovered that the embezzlers viewed their actions as essentially non-criminal, justified, or part of a larger pattern of irresponsibility for which they were not entirely responsible (Creasey 1953). He also discovered that rationalizations of the embezzlers were frequently knitted to their positions and the manner in which they committed the violations. Researchers have defined rationalization differently. Rationalization, according to Rae and Subramaniam (2008), is the justification of unethical behavior by a fraudster who lacks moral integrity. According to Lister (2007, p. 63), rationalization is "the oxygen that keeps the fire burning," and the company culture may be the reflection of the individual's own value systems. Rationalization is crucial for a fraudster to commit deviant behavior; therefore, if an action cannot be rationalized as moral, the fraud will not

be committed (Dorminey et al. 2010; Jackson et al. 2010). The fraudster may use many defenses, such as "I am only borrowing, and I will pay it back," "My firm can afford it," "I did not get a raise, but I deserve one," and "Everyone else is doing it, so why shouldn't I," to justify these fraudulent activities (Zikmund 2008; Ramamoorti 2008). Someone may use one or more of these justifications to rationalize their fraudulent activity.

The rationalization element of Cressey's fraud triangle agrees with Hollinger and Clark's (1983) finding that employees commit fraud primarily due to poor working conditions. Employees find it easier to rationalize fraud as recompense for enduring difficult working conditions. Simply, the employees justify their theft by convincing themselves that "they owe me." According to Hollinger and Clark (1983), the following correlations exist: 1) There is little link between personal income and fraud. Employees of all income levels perpetrate fraud, so income does not appear to be a predictor of theft. 2) Job dissatisfaction and employee deviance, including fraud, have a positive relationship. 3) There is a negative relationship between internal controls and employee deviation.

When someone can rationalize fraudulent activity, a link is built between pressures and opportunity, and the fraud triangle is formed (Creasey 1953). Organizations must decrease opportunity by enforcing strict internal controls and lowering perceptions of pressure and incentives by providing training, awareness campaigns, and penalties. The likelihood and manner of fraud, as well as its scope, may be influenced by the potency of each component and the organizational setting. Fraud researchers can use this as an opportunity to determine how these factors affect fraudulent behavior in various circumstances (Howe & Malgwi 2006). For a trust violation to occur, all three legs of the fraud triangle must be present (Ghazali et al. 2014; Othman et al. 2015; Petrascu & Tieanu 2014; Rahman & Anwar 2014; Suh et al. 2019).

## **2.5 Critical Review of The Fraud Triangle**

The fraud triangle was developed by Donald R. Cressey in 1953. If we closely observe the legs presented by Donald Cressey, we notice that the first leg is perceived financial pressure, which is non-sharable. However, over the period of time, this has been researched that many occupational frauds have been committed through collusion. If the financial pressure is non-sharable, collusion will not be present. Employees may resort to vendor fraud, bank fraud, customer fraud, etc., by collusion with vendors, customers, or even among themselves. Employees commit fraud when they have the opportunity to override the controls. This override of controls can be achieved by either a single person or multiple employees working in collusion (Vona 2008). Major financial frauds are believed to be committed by a group of individuals (Dooley & Skalak 2011). When there are accomplices, thus, collusion is present, which is the case of the bad bushel (Ramamoorthy 2009). The instances of collusion constitute a significant issue in an organization. When collusion occurs at the highest levels, internal controls like the segregation of duties are at risk of being completely ineffective against it.

Further, due to collusion, there may be no or fewer whistleblowers left to raise the alarm (Davis 1996; Elliston 1982; Johnson & Kraft 1990; Jubb 1999; Park et al. 2008; Park & Blenkinsopp 2009; Tsahuridu & Vandekerckhove 2008). Occupational fraud perpetrated through collusion is more challenging to prevent or even identify by external or internal auditors. COSO fraud study 2010 indicated that the CEO and/or CFO were engaged in 89 percent of the fraud cases. In many cases, fraudsters have participated in fraudulent behavior in the past. If they frequently operate in collusion, their allies help suppress any doubts auditors or regulators raise (COSO Fraudulent Financial Reporting:

1987-1997 – Analysis of US. Public Companies 2010). Another COSO Fraud Study (1999) found that the CEO and CFO had colluded in 83 percent of the fraud cases.

Further, the Sarbanes-Oxley Act 2002 has assigned a crucial role in the supervision of financial reporting matters to the audit committee of public companies. Recognizing that high-level fraud typically involves collusion and is frequently a "team sport" is a crucial behavioral observation of audit committees. Internal controls frequently assume sufficient segregation of duties; hence, they are mostly ineffective against collusion.

The fraud perpetrators in an organization can be classified into First-time offenders, repeat offenders, organized crime groups, and internal fraud perpetrated for the alleged advantage of the organization. In organized crime, fraud is perpetrated by professionals outside the company who exploit poor internal controls by working together with clients or vendors or by employees through kickbacks (Vona 2008). When two or more employees conspire to defraud a company, this is collusive fraud (Padgett 2015). Management fraud is an example of collusive fraud. Even an audit committee or a member of the audit committee may participate in collusive fraud (Silver, Fleming, & Riley 2008). Employees from different organizations and those from the same organization may collude (Kranacher et al. 2011). Internal controls are frequently weak when collusion occurs, making it easier to get around good internal controls (Kranacher et al. 2011; Wells 2017). Organizations are at risk from collusive fraud because it causes significant losses and is challenging to identify (Rossi, n.d.). It is crucial to remember that many fraud schemes can involve collusion when evaluating fraud risk by their very nature. Over time, supervisors and employees engage in collusion, which may have started between a customer or vendor and an employee.

According to Cressey (1973), the financial pressure to commit fraud can be connected with the internal motives of the person. However, he emphasized that financial difficulty does not mean people will always commit fraud. He also emphasized that pressure might come in three forms: personal pressure to pay for the promoted lifestyle, pressure from the employer to meet business targets, and external pressure. However, pressure may include other types of financial difficulties, such as debt, greed, a challenge, a strong desire to go against the system, dissatisfaction with earnings, etc. (Cressey 1973). All of these characteristics are defined as the reason for committing fraud in the scientific literature.

The second element, opportunity, remains the critical ingredient of crime causation, as, without opportunity, no one can conduct the fraudulent act while maintaining dignity (Turner, Mock & Srivastava 2003). The opportunity for fraudsters involves access to resources to both perpetrate and conceal the crime. An opportunity is attractive as a means of responding to desires, wishes, and ambitions. Aguilera and Vadera (2008: 434) describe a criminal opportunity as "the presence of a favorable combination of circumstances that renders a possible course of action relevant." An opportunity arises when individuals or groups can engage in illegal and unethical behavior and expect to avoid detection and punishment with a reasonable degree of confidence.

Rationalization, on the other hand, is fading away (Grace & Peter 2001). In a practical world, research has shown that sometimes criminals have no repentance or rationalization for their actions (American Journal of International Law, Volume 39, Issue 2, pp 257 to 285). Before committing the crime, they knew that the criminal act was unlawful and pernicious to the interest of society, yet they went on to commit it (Akomea-Frimpong et al. 2016; Amin 2018).

Hence, although Cressey's fraud triangle demonstrates that certain characteristics increase the likelihood of fraud, it does not provide full coverage. The fraud triangle can assist in explaining the character of most of the occupational offenders, but it does not describe the persona of all of them. As a result, it signifies that no single model will hold well under every circumstance. Critics of the fraud triangle, Kassem & Higson (2012), Anandarajan & Kleinman (2011), Charles & Christopher (2006), have argued that it cannot identify and explain the reasons for fraud appearance because it ignores such factors as fraudster's capability and skills. Moreover, Cressey's study is more than half a century old, and much has changed in society since then. That is why other models have been developed to understand fraudulent minds (Gottschalk 2016, 2017).

For the prevention of employee fraud, organizations may be able to reduce the opportunities by implementing sound internal controls and corporate governance. Organizations may also be able to reduce the financial pressure through financial assistance and loan programs; however, the Fraud Triangle fails to assist an organization in assessing the risk that an employee may or may not be psychologically inclined to perpetrate the fraud. From a social science perspective, this is likely the major criticism of the theory because it does not explain why some employees commit fraud while others do not in similar situations of apparently identical pressure and opportunity.

Another fundamental weakness of the Fraud Triangle theory is that it, by its very nature, focuses on studying offenders who have already been convicted of fraud. The fraud triangle was evolved by Creasey after studying and interviewing the embezzlers who had been sentenced to imprisonment, i.e., they had committed fraud in their organization. By definition, a fraudster who has been convicted has been unsuccessful, and their case is being taken into consideration after the event. Fraud Triangle does not consider research on the motives and rationalizations of successful or currently active



fraudsters. Further, it lacks research on whether the same person might commit fraud in one set of circumstances but not in another.

Despite its widespread use, the fraud triangle has been the subject of much discussion and criticism in recent years (Free & Murphy 2015; Morales et al. 2014). To provide deeper insight into fraud offender tactics and motivations and increase an organization's ability to prevent, detect and investigate fraud, researchers and practitioners have worked to offer insights beyond the fraud triangle (Dorminey et al. 2012).

From an organizational perspective, just one of the Fraud Triangle's three components, opportunity, can be seen as most relevant. Most businesses of any size will have mechanisms in place to identify fraud risks, such as the potential for a person to defraud the organization. Most organizations will also have internal control systems intended to lessen the risk of fraud, such as audits and inspections, fraud awareness training, and whistleblower policies. Therefore, a successful organization can have efficient and effective preventive measures in place, but no system solution guarantees to prevent all fraud for any organization.

## **2.6 Need For Further Exploration**

The Fraud Diamond theory was introduced by Wolfe and Hermanson in 2004. It represents an evolution of the traditional Fraud Triangle by adding a fourth dimension: capability. This addition seeks to address a critical gap in the Fraud Triangle, which primarily focuses on the motivation behind fraudulent acts without directly linking these motivations to the specific types of fraudulent conduct an employee might engage in. The Fraud Diamond posits that for fraud to occur, an employee must not only be motivated by pressure and have the opportunity to rationalize their actions, but they must also be

capable of carrying out the fraud (Wolfe & Hermanson 2004). This concept of capability covers an employee's position within an organization, skill set, confidence, and ability to coerce or influence others. Hence, it provides a direct link between the potential for fraud and the execution of fraudulent activities.

Including capability in the Fraud Diamond theory enhances our understanding of how fraud is perpetrated. It acknowledges that while many employees within an organization may experience pressure, perceive opportunities, and rationalize unethical actions, not all possess the capability to convert these factors into fraudulent acts. Capability acts as the enabler, turning potential into action. Despite similar motivations, it delineates those who can orchestrate and execute complex schemes from those who cannot (Ramamoorti, Morrison, & Koletar 2009). Moreover, capability introduces a spectrum of fraud actions ranging from simple embezzlement to sophisticated schemes like financial statement fraud or cyber fraud. It suggests that the nature and complexity of fraud an individual commits are directly related to their unique capabilities. For instance, an employee with advanced technical skills and access to sensitive information might engage in cyber fraud. At the same time, someone with a deep understanding of financial systems might manipulate accounting records (Singleton, Singleton, & Bologna 2006).

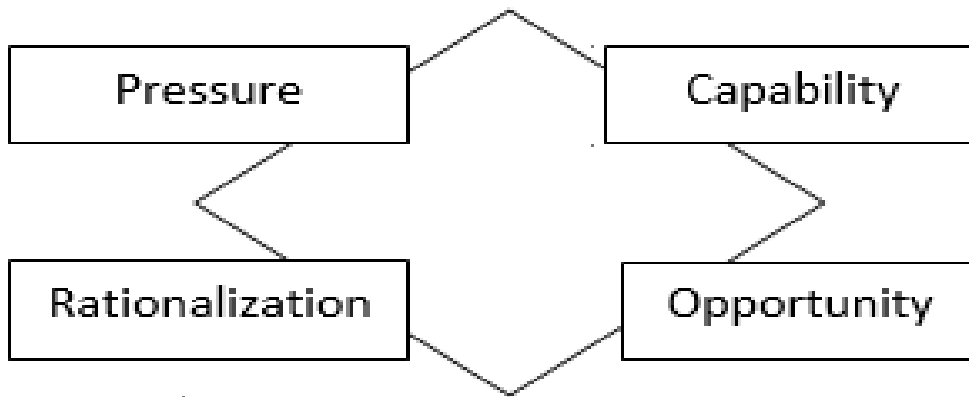
Research has further elaborated on how capability influences the method of fraud committed. Cohen, Ding, Lesage, and Stolowy (2010) argue that the capability enables individuals not only to commit fraud but also to conceal their actions effectively, complicating detection efforts. This aspect of capability points out the importance of tailored fraud prevention and detection strategies that consider the specific skills and opportunities unique to potential fraudsters within an organization. The relationship between capability and fraudulent acts emphasizes the need for organizations to adopt a holistic approach to fraud risk management. By understanding the capabilities of their

employees, organizations can better anticipate the types of fraud they may be susceptible to and implement targeted controls to mitigate these risks. For example, organizations might limit access to sensitive information, implement dual control systems, or invest in specialized training for those in positions of trust (Cressey 1953; Albrecht, Albrecht, & Albrecht 2008).

Hence, the Fraud Diamond theory's introduction of capability as a critical element in understanding fraud provides a more comprehensive framework for analyzing the direct relationship between an individual's abilities and the fraudulent acts they might undertake. It highlights the importance of considering the specific attributes and skills that enable fraudulent behavior, offering valuable insights for both theoretical exploration and practical application in fraud prevention. Further research into the nuances of capability and its implications for different types of fraudulent conduct remains a vital area for scholars and practitioners in the ongoing battle against fraud.

## **2.7 Detailed Review Of Fraud Diamond**

David Wolfe and Dana Hermanson (2004) came up with the idea of the "fraud diamond." The concept of "fraud diamond" was first published in the CPA Journal in December 2004. Fraud Diamond Theory (Wolfe & Hermanson 2004) extends the fraud triangle by including another element of the capability to it. According to Wolfe and Hermanson, while the pressures, opportunity, and rationalization of the fraud triangle may exist, it is unlikely that fraudulent activity will occur until a fourth element of capability is also present. According to their description, opportunity creates a window for fraud, pressures and incentives push people in that direction, and rationalization convinces them to go through it. The capability enables the fraudster to repeatedly walk through the window and exploit the opportunity.



*Figure 2 - Fraud Diamond (Source: Journal of Islamic Accounting and Finance Research 2(1):91, 2020)*

A fraudster's capability to engage in fraudulent behavior might be a culmination of many characteristics and skills. The position of authority in the organization is the first of these characteristics mentioned by Wolfe and Hermanson (2004). For instance, a CEO or CFO may be more powerful or have access to system overrides than other employees, which raises the opportunity that they will perpetrate fraud. In other words, the capability is a sub-set of opportunity as the fraudster holding a position of authority is more opportune to find gaps in the system and hence becomes capable of defrauding the organization. The skill to conduct fraud is the second of these characteristics. The employee has a greater opportunity of committing fraud if they are intelligent enough to identify internal control gaps and are familiar with the workings of the system. This is called finding or creating opportunity. A fraudster is less likely to perpetrate fraud if they lack the knowledge and aptitude to do so. For instance, a person may have financial pressure at home, have the rationalization to commit fraud, and may have discovered internal control flaws that could enable him to steal from the business. The fraud is unlikely to occur, though, if the perpetrator is unaware of how to take advantage of flaws in the system. The third characteristic is personal ego and the confidence that the fraud

would go undetected. Therefore, egoistic, confident people are more inclined to engage in deception. The last characteristic is the ability to handle the stress of being discovered over the long term. A fraudster who defrauds people for a long time will need to continuously lie, hide, and cover their tactics to convince people that no fraud is being committed. Only someone who can handle the stress can continue with the fraudulent act. Capability may directly affect fraudulent behavior and be a moderator of such behavior.

The authors also claimed that pressure might exist with opportunity and rationalization. However, if an individual's ability to commit fraud is considered, it may provide more weight to the fraud's occurrence. According to Mackevicius (2012), it is not always possible for each person with the motivation, opportunity, and realization to commit fraud due to a lack of skill to hide it. According to Abdullahi and Mansor (2015), the potential perpetrator might have the capability to perpetrate fraud.

The fraud diamond also shows that significant frauds are perpetrated by individuals who are clever, deliberate, knowledgeable, innovative, and who have a great understanding of organizational controls. These individuals have a strong ego and belief that they will never be caught. According to the ACFE (2020) survey, bigger frauds are perpetrated by management and upper-level executives, implying that these people have a high level of competency in the business and are seen as trustworthy individuals due to their prominent roles. Six personality traits of a capable fraudster identified by Wolfe & Hermanson are 1) position of trust to exploit the opportunities, 2) smartness to understand the internal control weaknesses, 3) strong ego and great confidence that fraud will not be detected, 4) coercion to commit or conceal the fraud by others 5) effective and consistent lies 6) ability to handle the stress (CPA Journal 2004)

## **2.8 Critical Review Of The Fraud Diamond**

As fraud diamond covers the initial three elements of the fraud triangle, the element of "capability" is a unique feature of fraud diamond theory. Capability is a circumstance in which a potential fraudster possesses the required skills, attributes, and abilities to perpetrate fraud. It is the point at which a fraudster recognizes the existence of a possible fraud opportunity and then uses his or her abilities and skills to make that possibility a reality. Position, intelligence, ego, coercion, deception, and stress are all factors that contribute to capability (Wolfe & Hermanson 2004). According to Gbegi and Adebisi (2013), pressure, opportunities, and realization alone cannot persuade a potential fraudster to perform such a deception. According to Wolfe and Hermanson (2004), people may use their organizational positions to manipulate the system and create opportunities for fraud. Beasley et al. (2010) discovered that Chief Executive Officers were implicated in more than 70% of all frauds recorded in publicly traded companies in the United States. The study also found that many organizations lacked adequate checks and balances to restrict their CEO's capabilities, which could impact the continuation of unethical behavior. A person capable of unethical action can influence others into committing or concealing fraud (Rudewicz 2011). Such people induce others to engage in unethical behavior or turn a blind eye.

A critical examination of the fourth element of fraud diamond, i.e., capability, reveals that capability is nothing but the authority of the fraudster to "create the opportunity" for himself. Hence, capability is a sub-set of opportunity, which is perceived as the most essential element of fraud. Though a person may be capable enough to perpetrate the fraud, the absence of available opportunity or inability to create the opportunity likely deters the fraud commissioning.

## **2.9 Discussion And Review**

The fraud theories reviewed above hold some or other significance in understanding the psychology of an employee fraudster. However, following an examination of the theoretical basis behind the variables that drive people to commit fraud, it becomes evident that current fraud models need to be revisited to reflect current developments in the field and the rising number of fraud instances. Fraud is hard to detect once committed; hence, it is better to prevent the same. In order to prevent fraud, it is always better to understand what goes into the mind of a fraudster before, during, and after the commissioning of fraud.

## 2.10 Summary Of Findings And Gaps In The Existing Research

On the basis of the review of the existing research, the study presents the summary of findings and explores the gaps in the existing research, which is tabulated below:

| Study                                     | Findings  | Gaps   |
|---|---|--|
| The Fraud Triangle (Donald Creasey, 1953) | Three elements of occupational fraud: 1) Perceived Pressure, 2) Perceived Opportunities, 3) Rationalization | 1) The pressure is perceived by Creasey as non-sharable. However, if fraud is perpetrated through collusion, i.e., shared with other perpetrators, results are more disastrous. 2) The Fraud Triangle is over 70 years old and does not fit the current landscapes. 3) Focuses on the study of |

|   |  |   |
|---|--|---|
|   |  | embezzlers rather than fraudsters   |
| The Fraud Scale (Dr. Steve W. Albrecht, 1982)                 | Replaced Integrity with the Rationalization element of The Fraud Triangle.                                     | Limited to only one typology of fraud, i.e., Financial Statement Fraud, ignoring all other fraud types. |
| The Fraud Diamond (David Wolfe & Dana Hermanson, 2004)        | An element of capability added to the existing elements of the Fraud Triangle                                  | The capacity, as perceived by the researcher, aligns with the element of opportunity itself.            |
| ABC Model (Sridhar Ramamoorthi, 2008)                         | Three elements of deception: 1) Bad apple, 2) Bad Bushel, and 3) Bad crop.                                     | Ignores the conditions that give rise to fraud and focuses only on psychology                           |
| The MICE Model (Kranacher et al, 2010)                        | Four elements of deception, i.e., Money, Ideology, Coercion, and Ego   | Ignores the concept of Opportunity  |
| The Fraud Pentagon (Marks, 2012)                              | Two elements of competence and arrogance added to the existing elements of the Fraud Triangle.                 | Insufficient elaboration on competence  |
| The SCORE Model (Georgios L. Vousinas, 2019)                  | Five elements of Fraud, i.e., Stimulus, Capability, Opportunity, Rationalization, and Ego                      | No newer invention. It just combines the existing elements into new Research.                           |
| <b>Other Research not concluding in a conventional theory</b> |  |   |
| (Becker et al., 2006)   | Each Fraud Triangle Theory component was influential in student cheating behavior. Methods to reduce pressure, | The study was conducted on 476 business students on student cheating behavior. It                       |



|                            |   |   |
|----------------------------|---|---|
|                            | opportunities, and rationalization of students to cheat are discussed.  | is not directly proportional to employee fraud.   |
| (Dellaportas, 2013)        | Findings differed from inmate to inmate. Pressures varied from financial to non-financial. Opportunities were mostly control deficiencies, and they demonstrated several rationalizations for their acts. | A very small sample of ten accountants who were serving sentences in prison for fraud   |
| (Schuchter and Levi, 2013) | Perceived pressure salient to fraudster offenses. Fraud Triangle Theory's elements are highly influenced by corporate culture.  | A very small sample size of thirteen white-collar fraudsters in Switzerland and Austria                                       |
| (Boyle et al., 2015)       | Fraud Diamond provides better fraud risk assessments for auditors.  | A study was conducted on auditors, limiting its scope only to financial statements fraud.                                     |
| (Murphy and Free, 2016)    | The instrumental climate was found to be a critical factor in fraud cases.  | Instrumental climate refers to Internal control weaknesses; however, Internal control weaknesses have not been elaborated on. |
| (Zakaria et al., 2016)     | Internal control weaknesses are the major contributing factor to fraud.   | Very small sample size consisting of a single oil and gas company.  |

As presented by data in Table in section 2.10, various models and other Research indicating employee fraud are discussed. However, there remains a gap in Research done so far with respect to the understanding of employee fraud and its elements. All Research conducted so far seems to revolve around the fraud triangle theory developed by Donald Creasey (1953), which was never conducted to study employee fraudulent behavior; instead, it covered only a small portion of fraud, i.e., embezzlement.

For the purpose of the study, a few theories that have looked into the causes of fraud are the Fraud Triangle Theory, Fraud Diamond Theory, Fraud Pentagon Theory, MICE Model, and SCORE Model. Among these, the Fraud Triangle Theory and the Fraud Diamond Theory have been discussed in detail for the reasons mentioned below.

The fraud triangle theory is the oldest among all, and all other theories, as mentioned above, are the extension or modification of the fraud triangle theory. The summary of findings and gaps in the existing theories is explained vide Table above. As discussed in the Literature Review, the elements identified by the above fraud theories coincide with each other. At the same time, the prime focus has been kept on the elements of the fraud triangle. For example, “Stimulus,” identified by the SCORE Model, and “Money,” identified by the MICE model, are described as the financial pressure identified by the fraud triangle. Similarly, the capability element of the SCORE model resembles the capability element of the fraud diamond.

On critical examination of various fraud theories, the elements that emerge are perceived pressure, perceived opportunity, rationalization, capability, ego, and coercion. Hence, the study identifies these elements as a crux of the above existing fraud theories.

## **2.11 Conclusion Of Literature Review Findings**

In 2016, Murphy and Free conducted a survey of fraud offenders who were in prison, fraud investigators who investigated the fraud cases, and employees who witnessed fraud in organizations. They looked at the situational opportunities in which a person made fraudulent decisions to advance their or the organization's interests. Their findings reveal that "situational opportunity" was a crucial element that existed when the fraud was committed. Zakaria et al. (2016) looked into how fraud occurs in an oil and gas business due to flaws in internal controls. They discovered that internal control flaws were a significant contributor to fraud. Additionally, they discovered numerous employees had conspired to commit fraud, taking advantage of weaknesses, including ineffective supervision and poor document control procedures.

The study conducted by Boyle et al. (2015) examined the CEO risk level, the fraud triangle, and the fraud diamond among a sample of 89 public accounting auditors. According to their findings, auditors who evaluated fraud risk factors using the fraud diamond displayed a greater likelihood of fraud than those who evaluated using the fraud triangle. Further, Dellaportas (2013) used the fraud triangle to explore the elements that lead accountants to commit fraud. Ten accountants serving prison sentences for fraud and other charges were interviewed face-to-face to collect the data. The overall result of the study was that when faced with a crisis, the offenders used their position as accountants to deceive their companies. The results also imply that the offenders took advantage of opportunities such as internal control weaknesses and financial or non-financial pressures. Additionally, the offenders gave several justifications for their deceptive behavior.

Fraud researchers have extensively studied the Fraud Triangle Theory. However, critics argue that the fraud triangle has been misused by fraud researchers (Huber 2016).

He contends that Cressey's (1953) initial objective was to explain theft or embezzlement, not to explain fraud. Fraud researchers frequently used the terms "fraud" and "embezzlement" interchangeably. The fraud triangle and associated research are also criticized by Donegan and Ganon (2008) due to a lack of robust empirical support, the exclusion of other causes of fraud, and the one-dimensional psychological examination of fraud perpetrators. The fraud triangle has also drawn criticism for assuming only individual deceptive acts and ignoring group dynamics (Trompeter et al. 2013), ignoring the explanation of collusion and cultural differences (Cieslewicz 2010), failing to adequately address every instance of fraud (Lokanan 2015); and making fundamentally incorrect translations from criminology to fraud examination (Dorminey et al., 2012; Morales et al., 2014).

Despite criticism, the fraud triangle is the most widely used framework in forensic accounting and fraud investigation (Huber 2012; Smith & Crumbley 2009). The comprehension of the motivations for fraudulent behavior has improved due to studies based on the fraud triangle theory and its elements. According to Trompeter et al. (2014), fraud researchers must look beyond the fraud triangle and consider the results of forensics and non-accounting research related to fraud. To take fraud research to the next level, they advise examining theories from fields other than accounting, such as general strain theory (Merton 1938), cognitive dissonance theory (Festinger 1957), social identity theory, and game theory. Ramamoorti (2008) advocates integrating behavioral sciences into the study of fraud by examining the psychology and sociology of fraud. He suggests the A-B-C model, which allows for the classification of fraud as an individual offense (bad apple), collusive fraud (bad bushel), and societal, cultural, and organizational factors that encourage fraud (bad crop). Later, he expanded the use of psychology to prevent and detect financial fraud (Ramamoorti et al. 2013, 2014).

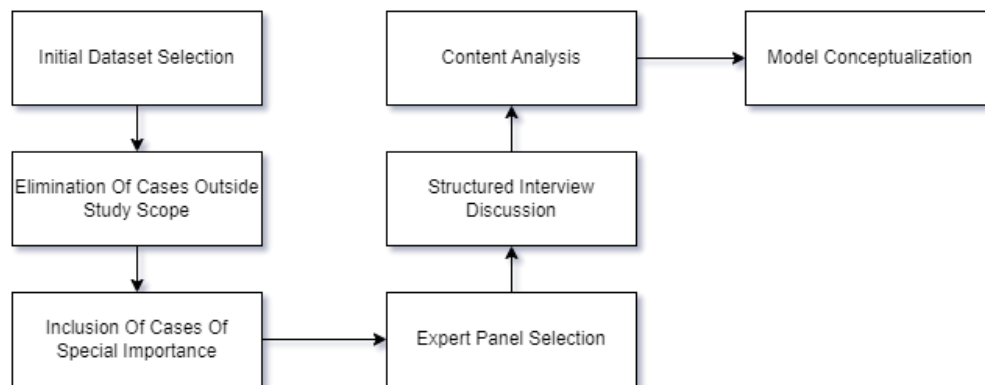
Hence, in order to respond to recent calls for the inclusion of additional behavioral sciences theories (Ramamoorti 2008; Ramamoorti et al. 2013, 2014; Trompeter et al. 2014), this research identifies that the significance of opportunity must be studied in vast detail rather than merely as an element of the cause of fraud. The global cost of fraud is approximately \$400 billion annually, equating to 5% of the revenue earned by organizations worldwide (ACFE Report to Nations on Occupational Fraud and Abuse 2020). Many organizations operating at a lower margin are struck off the business due to the severity of fraud. Fraud has financial consequences and causes other significant damages, e.g., job losses, mass economic recession, loss of faith in the organization, and severe unemployment across the industry. This study aims to find an effective prevention model consisting of ethical governance, sound internal controls, and management participation to limit the opportunities available for fraud.

Based on the findings of the literature review and the need to develop a concrete theory for fraud reasoning, this research aims to analyze the opportunities available to fraudsters to commit employee fraud, its consequences for the organization and introduce a model composed of fraudulent actions, utilization of the organizational vulnerabilities by the fraudsters, and red flags analysis that the organizations can apply to prevent the employee frauds to a larger extent. Further, the opportunity has been thus far perceived as an element of fraud psychology; the study aims to develop a fraud prevention model in the area of employee fraud using the above three elements of fraudulent acts by the employees, utilization of organizational vulnerabilities by employees and analysis of red flags for fraudulent behavior.

## CHAPTER 3: RESEARCH METHODOLOGY

After identifying “Availability of Opportunity” as a major factor contributing to occupational fraud, the study was further explored to conduct a secondary data analysis to understand the practical aspects of various opportunity elements that might occur in an organization. The purpose of finding such elements is to advise organizations to focus on such elements and ensure the minimization of fraud opportunities that might intentionally or accidentally be available to potential fraudsters. Here, in Research Methodology the secondary data is collected from the website of the Department of Justice, USA. The Department of Justice upholds the rule of law and protects civil rights. The Federal Bureau of Investigation is a supporting wing of the Department of Justice that investigates the incidents of White-collar Crime (<https://www.fbi.gov/investigate/white-collar-crime>) along with Terrorism, Cyber Crime, Corruption, Civil Rights, Organized Crime, and Violent Crimes.

This Research is focused on finding the primary catalysts of employee fraud, the most common vulnerabilities in organizational structures and processes that increase the opportunities for fraud; hence, all other types of criminal investigations are being ignored while collecting the data for Research. For this purpose, the press releases issued by the Department of Justice, USA, are analyzed. Each case of employee fraud is presented with a brief summary of the case, source, and analysis of the sub-element of fraud opportunity. Then, based on the analysis of the frequency of the fraudulent opportunity element, a detailed analysis is presented that can be used by senior management to deter fraud in their organization.



*Figure 3 – Flowchart Representation Of Research Methodology*

### **3.1 Initial Data Set Selection**

The data set for the research that forms the basis of this study includes a thorough examination of over 1,500 criminal cases that were prosecuted in the US between 2021 and 2023 by the Department of Justice. This particular time period, spanning from 2021 to 2023, was chosen methodologically to ensure that the sample size would be sufficient for a reliable content analysis and guarantee that the study records a current picture of fraudulent activities, represents the most recent strategies, trends, and legal reactions related to occupational fraud.

The choice to concentrate on cases that the Department of Justice prosecuted offers a base of legal rigor and procedural consistency. It further guarantees that the fraud cases in the data set have gone through a rigorous examination of the legal system. This methodology improves the dependability of the conclusions drawn from this analysis, and also guarantees that the research is based on confirmed cases of fraud, so reducing the possibility of biases related to self-reported data or cases that have not been decided by a court. Moreover, examining a large enough sample size enables a thorough and varied

investigation of the motivations, incentives, and controls of fraud in an organizational setting. Consequently, it enhances the understanding of the patterns and indicators of fraudulent conduct, thereby making a substantial contribution to the corpus of information in the domain of occupational fraud research.

### **3.2 Elimination Of Cases Outside Study Scope**

After conducting a thorough analysis of over 1,500 criminal conviction cases, it is observed that the Department of Justice, USA, handles a wide range of criminal cases. This covers various crimes, such as Terrorism, Cyber Crime, Corruption, Civil Rights violations, Organized Crime, occupational fraud, white-collar crime, and Violent Crimes. A purposeful filtering procedure was used to narrow the scope of this large dataset to instances of occupational fraud. As a result, a sample of 147 cases specifically related to occupational fraud incidents was carefully chosen for further examination.

This selection procedure highlights a focused strategy to separate occupational fraud from the larger range of illegal activities that the Department of Justice prosecutes. To better understand the dynamics specific to occupational fraud within the criminal justice system, 147 cases out of the original 1,500 were examined. By doing this, the study draws out insights and patterns that are specifically relevant to understanding the mechanisms, perpetrators, and organizational vulnerabilities associated with occupational fraud. The extraction of these cases for further examination facilitates a concentrated analysis of occupational fraud, enabling the study to explore the specifics of how such fraud is executed, detected, and prosecuted. This in-depth investigation is essential to clarifying the details of occupational fraud, highlighting its various manifestations, and identifying potential preventive measures. Through this rigorous selection and analysis process, the study seeks to improve the effectiveness of fraud prevention and detection



techniques in organizational settings by adding significant knowledge to the academic and practical discourse on combatting occupational fraud.

### **3.3 Inclusion Of Cases Of Special Importance**

During the first phase of the empirical data collection for this research project, 147 cases related to occupational fraud were found through a systematic review of records accessible on the Department of Justice website. This identification process spanned the years 2021 to 2023, defining the temporal scope of the initial dataset. The cases selected during this period were allocated based on their explicit connection to occupational fraud, which established the groundwork for a focused study into this specific form of criminal conduct that occurs in organizational settings.

After the compilation of the initial dataset, a thorough assessment procedure was carried out to determine the extent and quality of the dataset in relation to the study's overall research objectives. During this meticulous review, the decision was made to include an additional 10 cases in the research corpus. This decision was based on the understanding that certain cases could provide special insights with their industry-specific relevance. The purpose of including these cases was to ensure the dataset accurately reflects the diverse manifestations of occupational fraud across various sectors, improving the study's findings. As a result, for a more thorough examination, the study dataset was expanded to include a total of 157 cases of occupational fraud. This larger dataset strengthens the study's factual foundation and reflects a methodological commitment to capturing the complex nature of occupational fraud.

### 3.4 Expert Panel Selection

The selection process for the expert panel was conducted with meticulous attention to ensure that the assembled group possessed the necessary breadth of expertise and knowledge in the fields of audit and fraud investigation. A total of 20 participants were included in the panel. The demographics of the panel are as follows:

- **Gender:** Male: 13, Female: 7
- **Age:** 25-35 years: 5, 36-45 years: 8, 46-55 years: 5, Over 55 years: 2
- **Position in the Organization:** Senior Management: 4, Manager: 8, Auditor: 3, Professional: 5
- **Years of Experience in the Corporate Sector:** < 5 years: 4, 5-10 years: 4, 11-20 years: 3, > 20 years: 9
- **Department:** Finance/Accounting: 12, Audit: 6, Fraud prevention: 2
- **Education Level:** Bachelor's Degree: 20, Master's Degree: 17, Professional Certification 12

### 3.5 Structured Interview Discussion

To analyze the 157 cases of occupational fraud conviction that were obtained from the DoJ earlier, each member of the expert panel was assigned 7-8 cases. They were given time to study each case and interviews were scheduled with each. The interview guide is available in Appendix B.

### 3.6 Content Analysis

Comments shared by the experts during the interviews were transcribed and open coding was performed. The procedure of assigning codes played a crucial role in

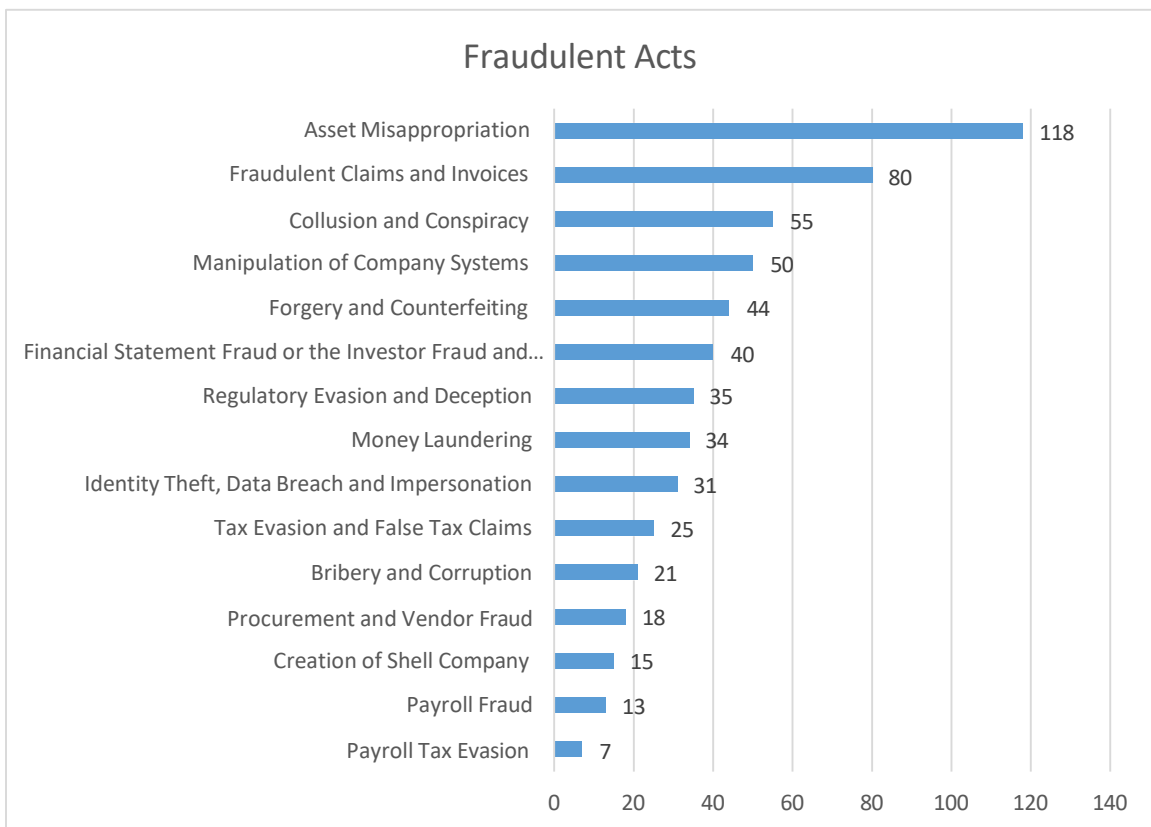
condensing the expert observations into concise major themes and patterns. The analysis data is available in Appendix C, D, E and F.

### **3.7 Model Conceptualization**

“Integrated Fraud Model” was conceptualized from the insights gained from the content analysis of the discussions. The model acts as a guide for organizations to recognize early warning signs of fraudulent activities, enabling timely intervention and the implementation of corrective measures. Based on it, the study culminated with strategic recommendations for the industry available in chapter 7.

CHAPTER 4:  
MAJOR TYPES OF FRAUD

After meticulous examination and discussion with the group of fraud professionals, fifteen key fraudulent methods were identified as the primary actions by the fraudsters to commit fraud within their organizations.



*Figure 4 - Findings On Major Types Of Fraud*

Despite the diversity in the nature of these frauds, a consistent theme of personal gain was found across the spectrum of cases. This categorization facilitates a structured understanding of a variety of ways in which occupational fraud can be executed.

Each category includes a range of sub-actions, indicating the diverse nature of fraud. The examination of case studies led to the elucidation of various specific

fraudulent actions. These actions, while distinct, sometimes overlap or co-occur within the same fraudulent scheme, demonstrating the complexity of employee fraud.

#### **4.1 Asset Misappropriation**

One of the most frequently observed fraudulent acts in the studied cases has been Asset Misappropriation, where the fraudster employees have misappropriated the company's assets (Cash, inventories, credit cards, tangible or intangible assets) for personal gain. The act of Asset Misappropriation, along with its other forms, as briefly explained here, occurred almost 118 times (75%) in the studied cases. An employee's activity is referred to as asset misappropriation when they "steal or misuse the organization's resources e.g. theft of company cash, false billing statements or inflated expense reports." This type of occupational fraud is thought to be the most common among all (ACFE Report to Nations on Occupational Fraud & Abuse 2012). In this case, the fraudster steals or misuses an organization's assets by employing deceitful techniques. "The "act" of asset theft, concealment, and conversion must all be present" for asset misappropriation to happen (Albrecht et al. 2008, p.1). These fraudsters are the company's workers, employees, clients, or vendors, either working in isolation or otherwise (Albrecht et al. 2008).

Asset misappropriation is considered to be the most prevalent type of fraud (ACFE Report to Nations on Occupational Fraud & Abuse 2018; Global Fraud Examiners 2016; Padgett 2015). However, asset misappropriation does not cause significant direct losses (Global Fraud Examiners 2016). On the other hand, asset theft deprives businesses of resources that they could have utilized to improve productivity and profitability. According to ACFE (2018), from their 2016 report, the number of asset misappropriation instances rose by approximately 7%, or from 83.5% to 89%. According

to the ACFE's 2018 report to the nations, asset misappropriation schemes fall into two primary categories: cash misappropriation and misappropriation involving inventory and all other assets. These categories have been used to identify five different misappropriation schemes: cash-on-hand theft; cash receipt theft via skimming or cash larceny; fraudulent disbursements through payroll, expense reimbursement, or check tampering; register disbursement; misuse of assets; and asset larceny (ACFE Report to Nations on Occupational Fraud & Abuse 2018).

As the most prevalent kind of occupational fraud (ACFE Report to Nations on Occupational Fraud & Abuse 2018), asset misappropriation has not gotten much attention in previous research (Zahari et al. 2020). Any employee within a company might perpetrate this crime. When the perpetrator has access to the firm's resources, it is easier for them to commit fraudulent acts like asset misappropriation. In order to steal resources from the workplace without being discovered, they must also have specific character attributes and skill sets (Wolfe & Hermanson 2004). When someone is capable of understanding and taking advantage of internal control systems, they tend to misappropriate assets in order to avoid detection or, in the event that they are discovered, to ensure that they can escape with ease and handle any resulting stress (Albrecht, Williams & Wernz 1995). A positive correlation has been observed between capability and fraud in previous research on the subject (Mackevicius & Giriunas 2013; Albrecht et al. 1995; Kassem & Higson 2012).

#### **4.2 Fraudulent Claims And Invoices**

The fraud cases involving Fraudulent claims and Invoices were observed 80 times in the studied cases. Such a case can also be categorized as the abuse of the expense reimbursement system. This is another form of asset misappropriation. In the studied

cases, this fraud has been committed by fraudulent employees to siphon funds from an organization under the guise of legitimate business transactions. This fraudulent practice allows to obtain financial gain through the misrepresentation of facts. It can range from overstatement of expenses and submission of fake invoices to claiming reimbursement for non-existent purchases or services (Wells 2017). The ACFE has identified these practices as among the most common methods of committing employee fraud (ACFE Report to the Nations on Occupational Fraud and Abuse, various years).

The abuse of expense reimbursement systems can be committed by employees by submitting false, inflated, or personal expenses for reimbursement, thereby costing companies substantial financial losses. One common method is the submission of fictitious expenses. Employees might fabricate receipts or invoices for services or products they never purchased (ACFE Report to Nations on Occupational Fraud & Abuse 2020). For instance, an employee could submit a receipt for a business dinner that never occurred or inflate the cost of a legitimate expense. Another method involves personal expenses being passed off as business-related. Employees might disguise personal travel, entertainment, or other personal costs as business expenses. For example, an employee may add personal vacation costs to a business trip and claim the entire amount as a work-related expense (Singleton & Singleton 2010). Another common tactic is the misrepresentation of the nature of expenses. Employees might misclassify expenses to fit categories that are reimbursable or have higher reimbursement limits. An employee might, for instance, claim a high-end personal purchase as a necessary business expense (Wells 2017).

### **4.3 Collusion And Conspiracy**

Collusion and conspiracy among employees, vendors, or customers manifest in various forms, including procurement fraud, asset misappropriation, and financial statement fraud, fundamentally undermining the integrity of organizational operations. The instances of collusion among employees and engaging in a conspiracy to commit fraud were observed in 55 studied fraud cases. Collusion refers to secret agreements or cooperation between two or more parties, often for fraudulent purposes. In the context of employee fraud, this usually involves coordination among employees or with external entities to commit fraud. Conspiracy, a closely related concept, involves a plan or agreement between two or more people to commit an illegal act. Both collusion and conspiracy are harder-to-detect frauds than those committed by an individual employee acting alone (Button & Brooks 2019).

One common area where collusion and conspiracy are prevalent is procurement fraud. Employees may conspire with vendors to over-invoice, create shell companies, or engage in bid rigging in favor of certain suppliers in exchange for kickbacks (ACFE Report to Nations on Occupational Fraud & Abuse 2020). Similarly, asset misappropriation schemes involving multiple employees can involve the theft or misuse of company resources, while financial statement fraud might include manipulating records and reports to present a misleading picture of the company's financial health (COSO 2013). The severity of collusion and conspiracy in employee fraud is amplified due to the involvement of multiple actors, which can lead to more significant losses for the organization. According to the Association of Certified Fraud Examiners (ACFE), frauds involving collusion are typically more costly than those perpetrated by an individual fraudster (ACFE Report to Nations on Occupational Fraud & Abuse 2020).

#### **4.4 Manipulation Of Company Systems:**



Fraud through manipulation of company systems, particularly accounting records, significantly impacts an organization's financial integrity. Such instances were identified in 50 studied cases. Employees, often those with access to accounting systems or in positions of trust, exploit these systems by altering accounting entries, adding fraudulent accounting entries, adding fraudulent invoices and payments, and manipulating audit trails to conceal their illicit activities. Altering accounting entries is a common tactic in this form of fraud. Employees modify financial records to disguise unauthorized transactions, such as embezzlement or misappropriation of funds. This manipulation often involves overstating expenses or underreporting revenues, leading to distorted financial statements (Rezaee & Riley 2010). Fraudulent invoices or payments are another method employed by fraudsters. These could involve creating fictitious vendor accounts or invoices for goods and services never received, with payments then redirected to accounts controlled by the fraudster (Singleton & Singleton 2010). Manipulating the audit trail is a more advanced fraudulent action, aiming to give legitimacy to these unauthorized activities. This involves creating false documentation or altering existing records to hide the true nature of transactions (Golden, Skalak, & Clayton 2006). Such tampering can be challenging to detect, especially if the perpetrator possesses a thorough understanding of the accounting system and internal controls.

Another method to manipulate the company's systems is the financial records tempering, which is often scrutinized within the broader discourse of occupational fraud and financial statement fraud. According to the Association of Certified Fraud Examiners (ACFE), tampering or manipulating financial records is a pervasive method used by fraudsters to conceal theft, inflate company worth, or mislead stakeholders about an organization's financial health (ACFE Report to the Nations on Occupational Fraud and Abuse, various years). Financial records tampering involves altering, fabricating, or

destroying accounting documents to conceal theft, inflate company earnings, understate expenses, or evade taxes. Research by Rezaee (2005) indicates that common methods include overstating revenue, understating liabilities, and using complex financial instruments to obscure actual financial conditions. The consequences of such fraud are far-reaching. Albrecht et al. (2015) highlight that besides financial loss, it leads to legal repercussions, loss of investor confidence, and reputational damage. A notable example is the Enron scandal, which demonstrated how extensive financial records tampering could lead to catastrophic corporate collapse (Healy & Palepu 2003).

#### **4.5 Forgery And Counterfeiting**

The cases of fraud involving forgery and counterfeiting by employee fraudsters were observed in 44 cases studied for this research. It is another form of asset misappropriation that presents a significant challenge in the corporate sector. It involves the unauthorized replication or alteration of documents, signatures, or checks for personal gain. The prevalence of such acts reflects deeper issues of trust, internal controls, and ethics within organizations. Forgery involves replicating the signature of an authorized person to transfer company funds illicitly. Counterfeiting, on the other hand, can include creating fake checks or altering existing ones for personal benefit. Both these actions not only result in financial losses for the company but also breach the trust vested in employees (ACFE Report to Nations on Occupational Fraud & Abuse 2020). Organizations suffer direct monetary losses due to unauthorized transactions (Wells 2017). Discovery of such fraud can lead to a loss of credibility and trust among stakeholders (Kaptein 2008). Legal ramifications not only affect the employee involved but can also lead to regulatory scrutiny for the company (Singleton & Singleton 2010).

#### **4.6 Financial Statement Fraud or the Investor Fraud and Misrepresentation**

Investor fraud and misrepresentation, particularly in the form of financial statement fraud, were found in 40 studied cases. This fraud involves the deliberate misstatement or omission of financial information to mislead investors about a company's financial health and performance. The intention behind such fraud is often to inflate stock prices or attract investment under false pretenses, causing significant harm to investors who rely on accurate information for investment decision-making. The act of misrepresenting a company's financial condition typically involves manipulating earnings, concealing debts, or inflating assets. The Sarbanes-Oxley Act of 2002, a regulatory response to major accounting scandals, underscores the importance of accurate and transparent financial reporting for investor protection (Sarbanes-Oxley Act 2002). The Act holds senior executives accountable for the accuracy of financial statements, reflecting the severity with which financial statement fraud is viewed.

Financial statement fraud is particularly perpetrated by senior employees. It is a deceptive practice aimed at presenting an inflated or misleading view of a company's financial health. This type of fraud can have severe consequences, not only for investors but also for the overall financial market's integrity. Senior employees, due to their authoritative positions, often have the ability and means to manipulate financial statements. This manipulation typically involves overstating assets and revenues, understating liabilities and expenses, or disclosing incomplete or misleading information about the company's financial status (Wells 2017). For instance, they might recognize revenue earlier than appropriate or use complex financial transactions to hide debt off the balance sheet, misleading investors about the company's true financial position (Singleton & Singleton 2010).

The motivation behind financial statement fraud can vary but often relates to maintaining or increasing the company's stock price, meeting market expectations, or securing personal financial benefits, such as performance-based bonuses (Rezaee 2005). Such misrepresentations can temporarily boost investor confidence, resulting in an artificial rise in stock prices or investment inflows based on misrepresented financial health (Pacini, Hillison, & Sinason 2000). Financial statement fraud leads to significant financial losses for investors, erodes public trust in capital markets, and prompts regulatory investigations, leading to legal penalties and reputational damage for the company (Unerman & O'Dwyer 2004). The global financial crisis of 2008 highlighted the systemic risks posed by such fraudulent activities, leading to increased regulatory scrutiny and calls for more robust corporate governance and financial oversight (Coffee 2006).

#### **4.7 Regulatory Evasion And Deception**

Regulatory evasion and deception occur when employees engage in activities that contravene regulatory standards and legal requirements. This category of fraud involves was observed in 35 studied cases. It is a broad spectrum of unethical actions, including the manipulation of bank loans, application for fraudulent loans, deception of insurance regulators, and tax evasion. These fraudulent practices undermine the integrity of financial and regulatory systems and also inflict significant harm on organizations and stakeholders. Regulatory evasion and deception are often characterized by deliberate efforts to circumvent laws and regulations for financial gain or competitive advantage. It manifests as manipulating loan applications to secure undeserved funding, deceiving insurance regulators to gain illicit benefits, or evading taxes to increase personal or organizational wealth (Sutherland 1949; Clinard & Yeager 1980).

The motivation behind these fraudulent actions often includes personal financial gain, the desire to meet organizational targets, or the intention to avoid negative consequences, such as penalties or business failures. Factors that contribute to this type of fraud include inadequate regulatory oversight, complex regulatory environments that provide loopholes, and a corporate culture that prioritizes profit over ethical compliance (Punch 1996). Moreover, they can create unfair market conditions where law-abiding entities are at a disadvantage (Shover & Hochstetler 2006).

#### **4.8 Money Laundering**

Though, the instances of Money laundering were observed in only 34 cases in the observed data; the regulatory loss inflicted by money laundering can never be underestimated. Money laundering by employees typically involves the process of disguising the origins of illegally obtained money, often through a sequence of transfers and transactions, so it appears to originate from a legitimate source. Employees may engage in money laundering activities by misusing their position within the company to facilitate these transactions. This could involve creating false invoices, manipulating financial records, or using the company's accounts to transfer and receive illicit funds. For instance, an employee might over-invoice a client and then redirect the excess payment to a different account, effectively cleaning the money (Levi 2015).

One common method is the use of shell companies, which appear legitimate but are actually created for the sole purpose of laundering money. These entities can be used to create false transactions, such as sales or services, that never actually occurred, allowing dirty money to be integrated into the company's financial system (Sharman 2010). Another method is "smurfing," where large transactions are broken down into smaller ones to avoid detection, a tactic often employed by employees who have access

to the financial operations of a business (Reuter & Truman 2004). The integration of laundered money into the financial system of a legitimate business can impose legal penalties for the company and reputational damage. Moreover, it can lead to regulatory scrutiny and potential loss of business opportunities (Halliday, Levi, & Reuter 2014).

#### **4.9 Identity Theft, Data Breach And Impersonation**

Identity theft, data breaches, and impersonation perpetrated by employee fraudsters severely undermine the credibility and trustworthiness of the organizations. Employees who engage in such misconduct often exploit their access to sensitive and personal data, leading to serious repercussions for the individuals and entities involved. In the cases studied for the purpose of this research, Identity Theft and data breaches occurred in 31 cases; however, the significance of such fraud is far more severe on victims.

Identity theft involves unauthorized access and use of personal information, such as social security numbers and bank account details, belonging to customers or fellow employees. This form of employee fraud can lead to financial fraud, where victims' identities are used for unauthorized transactions (Titus, Heinzelmann, & Boyle 2008). Data breaches occur when stolen information is leaked outside the organization, either intentionally or through negligent handling of data (Kshetri 2018). These breaches can have far-reaching consequences, affecting not only individual privacy but also the organization's reputation and customer trust.

Impersonation in corporate fraud involves employees assuming the identity of a trusted individual or entity to manipulate stakeholders. This could involve misleading people into investing in fraudulent schemes or divulging sensitive information (Willison & Warkentin 2013). The motivations behind these actions are varied and can include

financial pressures or workplace dissatisfaction (Cressey 1953). The opportunity for such fraud is often facilitated by inadequate security measures, including poor monitoring of data access and a lack of robust cybersecurity protocols (Cavusoglu, Mishra, & Raghunathan 2004).

#### **4.10 Tax Evasion And False Tax Claims**

Tax evasion and the submission of false tax claims by employee fraudsters represent fraudulent manipulation of tax systems to benefit individuals at the expense of public finances. It has been observed 25 times in the studied cases. This form of fraud typically involves underreporting income, inflating expenses, or hiding funds to reduce tax liability. One common method of tax evasion is the underreporting of income. Employees, especially those in positions with access to financial records, might intentionally omit or undervalue their income on tax returns. This could involve not declaring certain bonuses, commissions, or other forms of remuneration that they have received (Slemrod & Yitzhaki 2002). Inflating business expenses is another tactic used to reduce taxable income. Employees might create fictitious expenses or exaggerate the cost of legitimate business expenditures. This can be particularly prevalent in roles where there is little oversight or verification of expense claims, allowing individuals to submit false information with minimal risk of detection (Alm & McKee 2006).

Another form of tax evasion involves hiding funds or assets to avoid taxation. Employees might divert company funds to offshore accounts or invest in complex financial instruments that are difficult for tax authorities to trace. This type of evasion is more sophisticated and often requires a deeper understanding of financial systems and tax laws (Johannesen & Zucman 2014). Tax evasion not only results in a loss of revenue for governments but also undermines the fairness and integrity of the tax system. It places an

undue burden on honest taxpayers and can lead to increased scrutiny and regulation for businesses (Slemrod 2007).

#### **4.11 Bribery And Corruption**

Bribery and corruption are pervasive forms of financial malpractice that were observed in 21 studied cases. These cases are more prominently present in contract and procurement processes. These unethical practices involve the exchange of money, goods, services, or favors to influence business or government decisions. While bribery includes offering, giving, receiving, or soliciting something of value for influence, corruption is broader, encompassing various forms of misuse of power for personal gain. Bribery and corruption distort market mechanisms, undermine ethical standards, and have severe legal repercussions (Rose-Ackerman 1999). Globally, these practices hinder economic development, distort public policies, and erode trust in institutions (World Bank 2020).

In the domain of procurement, bribery, and corruption occur when employees collude with vendors to inflate prices, manipulate tender processes, or award contracts unethically (Søreide 2002). It leads to financial losses for the organization and damages the integrity of procurement processes, often resulting in subpar goods or services being procured. Bribery and corruption represent a conflict of interest where employees prioritize personal gains over the organization's interests (Jensen & Meckling 1976). The impacts of bribery and corruption are multifold, such as, operational inefficiencies, financial losses, legal penalties, and reputational damage. Corruption and bribery can also lead to distorted market practices, reducing competitiveness and economic efficiency (OECD 2019).

#### **4.12 Procurement And Vendor Fraud**



Procurement fraud has become a risk for many organizations. Although estimates of the problem's scope differ—for instance, Kroll (2013) estimates that 19% of the organizations have been victims, while PwC (2014, p. 8) estimates 29%. It is acknowledged as a global issue that is not specific to any one industry (European Commission 2014, p. 2; PwC 2014, p. 37). Kroll's assertion that procurement fraud has increased by 7% from the previous year and that PwC (2014, p. 8) claims it is the second most commonly reported global economic crime. In the studied case, it is observed that the employee fraudsters have been involved in various kinds of procurement and vendor fraud, including but not limited to bid rigging, kickbacks, bribery, and a sub-set of corruption. Such instances were observed in 18 studied cases. In general, kickbacks are unethical payments paid by an outside vendor to a company employee. The ultimate effect of kickback payments or gifts is to give one party an unfair advantage over another. It is common for relationships between vendors and workers to be concealed. What looks to be a commercial partnership at arm's length is usually much more than that.

The general definition of Bid Rigging is that the competitors agree in advance that one of the bids of many will be the winning one on a contract that a public or private entity wants to let through the competitive bidding. In many studied cases, the fraudsters were engaged in bid rigging to obtain the unfair advantage of their company's procurement systems. On the other hand, the term "vendor fraud" refers to a wide variety of fraudulent behavior, from fraudsters who create fake companies and submit invoices for payment to trusted providers that overcharge. It also encompasses the vendors colluding with the employees of the victim organization to bypass internal controls.

#### **4.13 Creation Of Shell Company**

The creation of fake or shell companies is a form of asset misappropriation that is achieved by submitting false claims and invoices by the employee fraudster. In this scheme, the employee establishes shell companies for submitting fake invoices to the victim organization, where such an employee holds a significant position of authority. Utilizing such an authoritative position, the illicit transfer of funds through fictitious transactions is facilitated in the favor of the fraudster. Shell companies are entities without active business operations or significant assets. These are created by employee fraudsters for the sole purpose of financial manipulation. In the context of employee fraud, these entities become tools for illicit financial gain. The shell company then ostensibly provides goods or services to the employer, invoiced at inflated prices or for non-existent deliveries (Singleton & Singleton 2010). The payment is made to the shell company, effectively funneling organizational funds to the fraudster (Kaptein 2008). In the studied cases, for the purpose of this research, 15 cases involved employee fraudsters establishing the Shell companies and causing significant harm to their organizations.

#### **4.14 Payroll Fraud**

Payroll fraud is a critical issue in organizational financial management which was observed in 13 studied cases. It often involves employees, particularly those in authoritative positions, manipulating payroll systems for personal gain. This form of fraud can take various forms, such as inflating time sheets, creating ghost employees, or unauthorized alterations in pay rates. Inflating time sheets is a common method of payroll fraud. Employees in positions of authority or those with access to payroll systems may falsely report hours worked, leading to payment for time not actually worked (Collins, Bloom, & Abernathy 2016). It is particularly prevalent in organizations lacking automated timekeeping systems or those that do not regularly audit time records.

The creation of ghost employees is another significant aspect of payroll fraud. This occurs when employees in charge of payroll processing add fictitious employees to the payroll system and divert these payments to themselves or accomplices (Button & Brooks 2016). It can be challenging to detect, especially in large organizations with numerous employees, where tracking individual employment status may be cumbersome. In addition to these methods, payroll fraud can also involve unauthorized changes to pay rates or the issuing of unearned bonuses and commissions. Employees with access to payroll systems might increase their hourly wage or salary in the system without approval, or they might process bonuses or commissions that were never earned (Wells 2017).

#### **4.15 Payroll Tax Evasion**

The failure to submit payroll taxes to the government by employee fraudsters is referred to as "payroll tax evasion," and involves the deliberate misappropriation of funds that are withheld from employee salaries for tax obligations but are instead diverted for personal use. In the studied cases, the instances of payroll tax evasion were observed 7 times. An employee in a position of financial authority, such as an accountant or financial manager, deducts the appropriate taxes from employees' wages but intentionally fails to remit these funds to the tax authorities. Instead, the funds are embezzled, leading to a direct financial loss for the government and potential legal repercussions for the organization (Slemrod 2007). This fraudulent activity undermines the trust between the employer and the employee. The employer may face significant penalties, interest charges, and potential criminal charges for failing to fulfill tax obligations. Further, they can also severely damage the reputation of the organization and lead to a loss of employee morale and public trust (Alm & Torgler 2006).

It is important to note that payroll tax evasion often goes hand in hand with other fraudulent activities, such as falsifying financial records to conceal the embezzlement of funds. These actions indicate a broader issue of internal control weaknesses within an organization (McGee 2006).

CHAPTER 5:  
OPPORTUNITIES AS A CATALYST TO FRAUD

Based on the comments from the experts, the opportunities that are exploited by the fraudsters were analyzed. A significant realization that emerged during these dialogues was the multilayered nature of fraud opportunities within each case. It was observed that several cases exhibited not just one but multiple elements of fraud opportunity. This led to comprehensive discussions, wherein the panel discussed each identified element, exploring its relevance and impact within the context of the case.

After meticulous examination, fifteen key sub-elements were identified as the primary enablers or catalysts for fraud within organizations.



*Figure 5 - Findings On Opportunities As A Catalyst To Fraud*

These sub-elements represent vulnerabilities or loopholes in the organizational structure and processes, which, if present, can significantly increase the likelihood of fraud being committed by employees.

### **5.1 Position Of Trust & Authority**

The first thing that gives a fraudster the opportunity to perpetrate fraud is their position in an organization. According to Wolfe and Hermanson (2004), the employee's position and role could be the key to breaking organizational trust. The findings of Beasley et al. showed that over 70% of the fraud cases involving publicly traded companies involved the CEOs being found to be responsible for the fraud. Additionally, they note that many businesses lack adequate checks and balances, enhancing the power of the CEOs to encourage and sustain fraud.

Previous studies show senior-level employees are more prone to committing fraud (Goldstraw et al. 2005; Peltier-Rivest & Lanoue 2012; Wells 2002). Many studies have revealed the situations in which accountants and executives utilized their positions to commit and conceal fraud (ACFE Report to Nations on Occupational Fraud & Abuse 2010, 2014, 2016, 2020; Donegan & Ganon 2008; Tinker & Okcabol 1991). According to Mitchell, Sikka, and Willmott (1998), there has been relatively little research on the apparent linkages between the position of authority and employee fraud. However, positive research on fraud and criminality focuses primarily on executive-led fraud (Piquero, Tibbetts, & Blankenship 2005; Rossouw, Mulder, & Barkhuysen 2000; Weisburd, Waring, & Chayet 1995), ignoring specific occupational roles such as senior positions. According to the “Report to the Nations on occupational fraud and abuse” (2020) issued by ACFE, fraud committed by top management and senior employees is

sixteen times more severe than fraud committed by an average employee. Hence, it can be inferred that the cost of fraud varies with time and the status of the fraud perpetrators.

The sociology and criminology literature, beginning with Cressey (1953), refers to fraud perpetrators as "trust violators." with Cressey defining fraud as "a violation of a position of financial trust." In other words, trust violators are the employees that an organization would never suspect of defrauding it. According to Cressey (1953), "trusted individuals" become "trust violators" when they perceive themselves as having a non-shareable financial problem and are aware that this problem can be secretly solved by violation of the position of financial trust and are able to rationalize the fraudulent conduct that enables them to assume themselves as trusted people (Albrecht, Howe & Romney 1984). Abuse of position of authority has further been defined by Shover (1998) as "the abuse of a fiduciary position by an agent in charge of custody, discretion, information, or property rights." Persuasion (Cialdini 2001, 2007; Hogan & Speakman 2006) and social engineering (Hinson 2008; Mitnick & Simon 2002) are two methods mostly employed by trust violators to conceal their fraudulent actions.

Researchers have proposed numerous theories to explain why prominent people are willing to commit financial crimes despite holding privileged positions. The most suitable situation here is the availability of opportunity, which refers to the organizational context in which a potential offender has legitimate access to resources and can perpetrate fraud by abusing their position and trust. Illegal profit can be obtained more easily in an organizational setting where the offender has power and influence based on position and trust. The ability of fraudsters to commit fraud is closely related to their privileged social status and preference for genuine and reputable employment (Friedrichs et al. 2018). Privileged criminals understand that they can easily earn unlawful money in

an organizational setting where they can wield power and influence based on their organizational position.

Senior employees leverage their position of trust to circumvent internal controls and gain access to company resources (Kennedy 2018; Wells 2002). The findings reveal that having a position of authority significantly impacts employee fraud (Wolfe & Hermanson 2004). According to other studies, most employee fraud is perpetrated by senior-level employees (Omar et al. 2016; Kennedy 2018). Since occupational fraud is an opportunity crime, greater opportunities to perpetrate fraud exist with the higher organizational position of the employee (Kennedy 2018). According to the findings of Kennedy (2017) and Peltier-Rivest & Lanoue (2012), employees in managerial positions committed fraud for a longer period of time than those in nonmanagerial positions.

An employee's position or function within an organization determines their capabilities, which may include the capacity to create or take advantage of a fraud opportunity that is not available to others (Wolfe & Hermansen 2004). The fraudster is a skilled individual who knows how to take advantage of internal control weaknesses and leverage his position. The findings of extensive research emphasize that employees in senior positions were the primary initiators in the majority of employee fraud (Wolfe & Hermanson 2004). ACFE & KPMG 2011 survey concluded that the majority of fraud perpetrators work in the finance function and hold the position of chief executive or managing director (KPMG Global profiles of the fraudster: Technology enables, and weak controls fuel the fraud 2011, p.4).

## **5.2 Lack Of Segregation Of Duties**

The segregation of duties within an organization is a fundamental “social internal control.” The core idea behind the principle is that at least two people must be involved at



each stage of a transaction or operation, whether directly or indirectly (Clinard & Yeager 1980; Sutherland 1983; Vaughan 1983, 1990; Weisburd et al. 1991). In its general guidelines for the governance and control of financial firms and institutions, the Swedish financial supervisory authority Finansinspektionen states that "an organization may achieve sound internal control by ensuring that an employee does not handle a transaction alone throughout the entire processing chain (Finansinspektionen 2005a). The main idea here is that no single person should be able to complete a whole work assignment from beginning to end on their own (Partnoy 2003; Drummond 2008). Specifically, it can entail a separation of business processes into distinct functions handled by different people, such as initiating, approving, recording transactions, handling assets, and reviewing and monitoring processes (Simpson 2002). Segregation of duties is therefore considered to be a crucial component of any internal control system aiming to lower the risk of unlawful use of assets, thereby enhancing compliance by preventing and deterring employee theft and fraud (Clinard & Yeager 1980; Friedrichs 2010). The principle of segregation of duties has roots embedded in the principle of duality (Braithwaite 1998, 2008; Tomlinson 2010; Tyler 2009). Duality is better captured by terms like "the four-eye principle," "the two-man rule," or "dual custody."

Segregation of duties is defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as "dividing or allocating tasks among multiple employees, making it possible to reduce the risks of error and fraud." For instance, a manager who approves the granting of loans should also not be in charge of maintaining customer accounts or handling cash receipts. This description shows that the goal of the segregation of duties is to lower risk by separating operational and monitoring duties (Braithwaite & Drahos 2000; Friedrichs 2010; Levi 2010), hence putting necessary checks and balances in place for crucial processes (Boritz & Wensley 1996). It might also

prevent the theft of proprietary data. Hence, the segregation of duties is a crucial internal control strategy for all organizations (Elsas et al. 1998).

A Segregation of duties policy lays down standards for task division within an organization (Ayres & Braithwaite 1992; Braithwaite 2008; Feldman & Lobel 2010; Mascini 1998; Miller & Thomas 2005). The policy also offers instructions on how to set up a process for assigning, modifying, and restricting an employee's tasks (Clark & Wilson 1987). External and internal auditors view such a policy as an essential first step in correctly managing the segregation of duties (van Wijngaarden 2007). Several businesses often incorporate their segregation of duties policy into internal control or security administration policies.

The segregation of duties framework identifies the duties inside a company that poses risks if they are given to one individual (Blokdijs & Elsas 2004; Blokdijs 2006; Elsas et al. 2006; Elsas 2007; Ernst & Young 2006; van Wijngaarden 2007; Veenstra 2007; Veenstra & Heertje 2006). When defining employee job duties, the segregation of duties framework is based on the ideal situation in which tasks are divided up front. Like other internal control components, management is ultimately responsible for developing a segregation of duties policy and framework and carrying out appropriate job separation (Brooks & Lanza 2006). It is necessary to delegate authority and responsibility to the proper level in order to manage organizational boundaries between processes and departments (Lightle & Vallerio 2003).

The purpose of the segregation of duties is to mitigate the possible harm caused by the acts of a single employee. As a result, no single employee should have influence over a critical set of business transactions (Martínez & Silva 1982). Segregation of duties prevents fraud by collusion, such that no employee may commit fraud without the involvement of another individual (Kobelsky 2014; Elsas 2008). Some guiding principles

of segregation of duties are: only limited transactions must be allowed for each employee to perform; employees should have non-coinciding, preferably opposed interests; and custody, operation, checking, and approval are preferably in different hands.

The cornerstone of the segregation of duties is the division of custodial, recordkeeping, and authorization responsibilities throughout the organization (Holmstrom & Milgrom 1991; Itoh 1991). For instance, in the case of accounts receivable, the custodian would be in charge of the money or cheques from the customers. If the person in charge of the receivables steals the money, the reconciliation of the bank account and client accounts performed by another independent employee will reveal the theft. Hence, the employee responsible for collecting the money should not be posting entries into client accounts or reconciling them.

Establishing segregation of duties is required for various positions inside a company. Hence, no employee should be responsible for overseeing the entirety of a financial transaction, including account reconciliation, inventory management, financial statement preparation, etc. Leaving the accounting and finance-related work under a single layer of management simply increases the opportunities for theft and fraud (Clark & Wilson 1987). Having one employee individually in charge of the company's accounts receivable, payable, check-issuing, and bank account reconciliation, without surprise audits, is a prime example of the absence of segregation of duties that invites theft and fraud (van Kesteren & Stachowiak 2015).

However, the justification for granting access to financial and accounting operations to a single employee is based on a few business choices:

1. The choice can be based on restricted budgets. Because of financial restrictions, there could not be enough staff members to handle the business-related functions.

2. The choice could be influenced by trust. Many smaller businesses eventually give one or more dependable long-term employees the opportunity to take on additional responsibilities. This choice could be made to avoid spending money on employing more workers. These choices commonly result in the long-term employee taking advantage of the opportunity and engaging in embezzlement.

The relevance of the segregation of duties in measuring the strength of internal controls has been acknowledged and documented in fraud studies. Research by Ashton (1974), Ashton & Brown (1980), and Hamilton & Wright (1982) have shown that the degree of segregation of duties explains a significant degree of the variance in internal control judgments.

Organizations must ensure that no accounts payable or receivable decisions are made without going through a dual control verification process. The accounts payable, accounts receivable, and payment disbursement departments must be distinct from one another (Knorr & Weidner 2001). No one employee should be in charge of overseeing the goods delivered by vendors or suppliers and the accounting tasks associated with it. It requires dual supervision to confirm that the goods or services offered by vendors or suppliers are from the parties who have been granted permission to work for the organization. The accounts payable process also requires the involvement of multiple employees. It is necessary to confirm that the supplier or vendor is qualified to receive the payment before any payments are authorized for disbursement.

### **5.3 Poor Audit Performance And Management Oversight**

An auditor conducting an audit must obtain reasonable assurance that the financial statements as a whole are free of material misstatement, whether caused by error or fraud (Petrascu & Tieanu 2014). According to ISA 200, there is an unavoidable risk

that some material misstatements of the financial statements will not be detected, even if the audit is properly planned and performed following the ISAs (Krambia-Kapardis & Papastergiou 2016).

The risk of failing to discover a material misrepresentation due to fraud is greater than failing to detect one due to error (Omoteso & Obalola 2014). This is because fraud might involve sophisticated and well-planned tactics to conceal it, such as forgeries, deliberate failure to record the transactions, or intentional misrepresentations to the auditor (Reinstein et al. 1984). Such concealing tactics may be considerably more challenging to identify if they are accompanied by collusion because collusion may lead the auditor to assume that audit evidence is persuasive when it is, in fact, incorrect.

According to research, more than 70% of investors expect a complete assurance that the material misstatements related to fraud in the financial statements would be detected (Epstein & Geiger 1994). The auditing industry has been criticized for both failing to detect fraud and reporting it after it has been detected. According to reports, independent auditors only catch 5% of fraud (Zeune 1997; KPMG Peat Marwick 1998). Most accounting professionals are aware of and agree that external auditors are repeatedly unable to identify instances of fraud. The ongoing presence required for the development and implementation of fraud prevention and deterrent programs is lacking with external auditors. Contrary to other crimes that may be observed, fraud often requires concealment on the part of the offenders.

As stated in Statement on Internal Auditing Standard (SIAS) 3 – “Deterrence, Detection, Investigation, and Reporting of Fraud,” issued by the Internal Auditing Standards Board (IASB), the implementation of both SAS 82 and section 10A gives new meaning to the importance of the role and responsibility of internal auditors in the deterrence, detection, investigation, and reporting of fraud (Ratliff et al. 1996). SIAS 3

makes it clear that management is responsible for preventing fraud, although it is well known that internal auditors are in charge of assessing the sufficiency and efficacy of management's actions. Analyzing and evaluating an entity's internal controls is fundamental to this function. Preventing fraud is an important objective of internal controls (Flesher 1996).

The auditor's capacity to discover fraud is determined by criteria such as the perpetrator's skill, the frequency and extent of manipulation, the degree of collusion involved, the relative size of amounts manipulated, and the seniority of those involved (COSO 2013). While the auditor may be able to detect possible opportunities for fraud, determining whether misstatements in judgment areas, such as accounting estimations, result from fraud or error is difficult.

Moreover, since employees in senior positions have more opportunities to manipulate accounting records, present fraudulent financial information, or override control procedures designed to prevent similar frauds by other employees, the risk of the auditor not detecting a material misstatement resulting from employee fraud is greater.

When establishing reasonable confidence, the auditor must retain professional skepticism throughout the audit, considering the possibility of management overriding controls and acknowledging that audit techniques that are effective in detecting error may not be effective in detecting fraud (Glover & Prawitt 2013). The provisions in ISA 240 are intended to help auditors identify and analyze the risks of significant misstatements due to fraud, as well as to create processes to detect such misstatements.

At least two types of audits in addition to the regular scheduled statutory or interim audit are suggested by SAS and AICPA in order to guarantee the integrity of the entire internal business operations:

1. Surprise audits: Refers to an audit of financial sections of the organization where employees are unaware of such audit operations.
2. Independent audit: An independent third party conducts the audit, which might be random or scheduled.

Employers must explain the internal auditing procedures to all employees. Employees should be aware that their operations may be the subject of a surprise or independent audit. Since employees are unaware of when does audit start, they are less likely to engage in embezzlement of assets or records. The audits serve the following purposes:

1. They serve as a deterrent to theft and fraud.
2. They can be used to find deceptive and fraudulent conduct against the organization.
3. The aim of surprise audits is to prevent employees from engaging in theft or fraud.
4. Independent audits help to avoid internal collusion.

Most studies have found that auditors only catch about 20% of employee fraud (Doig & Levi 2009). In most cases, fraud is discovered through tips or employee alertness. However, the mere presence of auditors around is a significant deterrent to fraud. Auditors conduct independent checks of transactions, making it difficult for a fraudster to escape if caught. If the audit is ineffective, the auditor's assurance may not be relied upon, and management and staff can engage in financial statement fraud.

However, management is ultimately responsible for preventing and detecting fraud within the organization (Bolton & Hand 2001; Huang et al. 2008) and ensuring that fraud does not occur at any level of the organization (Deloitte 2012). Since the position of seniority is more prone to commit fraud against the organization, they must be adequately supervised, and corrective actions must be taken to ensure an anti-fraud culture within the

organization (Wright et al. 2004; Tittle & Botchkovar 2005). In fraud situations, the management override of supervision causes severe damage.

Management is responsible for establishing and maintaining a cost-effective control system (Bolton & Hand 2002; Huang et al. 2008). This includes developing some controls to alert when other controls are not working properly. Following up on these clues may lead to the conclusion that fraud has occurred. One form of monitoring control is the construction and communication of a hotline or similar mechanism that consumers or workers can use to report complaints or identify issues (Clarke 1992; Brantingham et al. 2005). Other monitoring and detection controls are as follows:

- Alarm systems for facility doors and windows,
- Installing security cameras,
- Creating alteration checks for information systems,
- Carrying out inventory counts,
- Auditing,
- Invoices and cost center charges are reviewed and approved,
- Account reconciliations, etc.

It has been observed that management oversight of internal controls poses a serious obstacle to attempts to prevent fraud. For instance, the American Institute of Certified Public Accountants (AICPA, 2005, 2016) called management oversight "the Achilles' Heel" of anti-fraud initiatives. "Because management is primarily responsible for the design, implementation, and maintenance of internal controls, the entity, whether publicly held, private, not-for-profit, or governmental, is always exposed to the risk of management oversight of controls" (AICPA 2005, 1-2). Additionally, overriding existing controls is the second most commonly observed internal control weakness that contributed to occupational fraud (ACFE Report to Nations on Occupational Fraud &



Abuse 2016). The only internal control weakness that respondents to the ACFE survey cited more often was the management oversight of controls.

Management oversight is comparatively more common outside of the United States. The most striking finding is that the likelihood of management oversight fraud versus fraud involving a lack of internal controls is positively correlated with the strength of the organization's anti-fraud environment, which includes having an internal audit function, independent audits of the financial statements, an anti-fraud policy, or a code of conduct in place. Therefore, it seems that a robust anti-fraud environment acts as a barrier to fraud, which motivated perpetrators are forced to overcome through management oversight.

Management oversight of the processes and controls is arguably an organization's most basic control failure because it leaves out essential safeguards. Such failures result in large losses. On the other hand, some companies put in place internal controls that appear to be well thought out and functional, but management circumvents them in order to perpetrate fraud (AICPA 2002; Caplan 1999; Tipgos 2002).

Earlier writers have noted the serious hazards associated with management oversight. The AICPA (2016, 6) asserts that "With very few exceptions, senior members of management circumvented or overrode seemingly sound systems of internal control in the majority of the major fraud cases in the past fifty years that had catastrophic results for the organization." Similarly, Beasley et al. (2010) discovered that the CEO and/or CFO are involved in financial statement fraud cases approximately 90% of the time. The management coerced lower-level employees to circumvent controls in numerous instances of fake financial reporting (Pulliam 2003).

According to Dorminey et al. (2012, 576), managerial oversight is extremely severe and management oversight is the most severe fraud exposure of all. The possibility

of management oversight needs to be immediately evaluated as a fraud opportunity. Academic study on management oversight is severely hampered by a lack of data, despite the longstanding focus on management oversight as a key danger to fraud prevention efforts and a wealth of cases to emphasize the importance of management oversight (Beasley et al. 2010).

#### **5.4 Lack Of Systems Of Authorization**

An appropriate authorization system is one of the best internal control mechanisms. The system of authorization is one of the internal controls that lays down its foundations from the principle of segregation of duties and delegation of authority. The authorization mechanism ensures that every financial transaction is initiated by one, processed by another, and authorized by an independent person. Limiting authorizations prevents employees from engaging in wrongdoing and fraud (Parkes et al. 2016; Kranacher et al. 2017; Stuff 2012b). Lack of systems of authorization creates opportunities to commit employee fraud (Albrecht 2004). An employee creating a vendor master, accepting invoices from vendors, and posting them into the system should not be allowed to authorize the payment to such a vendor. Identifying employee fraud needs to ensure that the internal accounting control system upholds standards like the separation of duties and authorizations. Therefore, management must establish and maintain appropriate authorization policies for financial transactions.

Lack of authorization is prevalent, especially in smaller businesses (Hogan et al. 1999), which is one of the most basic internal controls in the accounting function. Under the authorization policy, responsibilities for specific accounting processes should be divided between supervisors and subordinates so that no one person has excessive access to or control over the entire transaction. Internal fraud is more likely to occur in

organizations with lax standards surrounding the authorization of transactions. A company should have measures in place to limit the authority granted to employees to only specific preset levels, and there should be a procedure for tracking those levels to gauge compliance.

Employees who do not get the required authorization or try to circumvent the controls are more prone to become fraudsters. For instance, if an employee is permitted to spend up to \$10,000 without prior authorization but makes two purchases from the same vendor for \$6,000 each (\$12,000 total), this should be investigated. It can be a single \$12,000 project split into two to bypass the authorization process.

An employee often needs some level of authorization within the company and is in a position to collide in a conspiracy with a vendor to engage in fraud (Ramamoorthy 2009). Such authorization can entail the capacity to recommend a purchase contract, authorize payments to vendors, alter invoices, and conceal fraud. Organizations require employees in positions of trust who can authorize transactions and exercise business judgment.

Regular review of the authorization of transactions must be a part of preventive efforts in order to deter bribery, kickbacks, and corruption (Ramamoorthy 2009). Controls that have been bypassed, forged approvals, altered paperwork, and genuine work orders must all be investigated by management. Against evaluating whether the documentation accurately reflects reality, actual goods or services must be compared to purchase orders, receipts, and invoices.

The level of authority of the employee initiating, approving, and recording transactions is related to the proper authorization of transactions. This category of actions can include signing off on transactions (either with a handwritten signature or a digital approval), checking that the right kind of authorization was given before a transaction

was finished, and responding appropriately if transactions are carried out without the right kind of authorization. For instance, a company may have a policy that an area supervisor can approve every transaction under \$10,000. However, any transaction over \$10,000 requires approval from the management of such area supervisor. This is an illustration of an authorization control, and further elements would include internal follow-up to ensure that the appropriate level of authorization was obtained for transactions above \$10,000.

Determining that authorizations are not being falsified is also crucial. A fake signature on a piece of paper or unauthorized access to computer data used to grant electronic authorization are two ways this can occur. Determining whether the authorization system is being abused is the final aspect of verifying authorizations. An employee might be tempted to split a \$14,000 transaction into two \$7,000 transactions if it needs a higher level of authorization in order to avoid the requirement for more authorization.

Organizations must ensure that anyone who generates payments on their behalf is not authorized to initiate the transaction with the financial institution. This includes electronic transfers of funds from the company to third parties. The login credentials and passwords for the financial institution's online bank accounts must be appropriately controlled by the company owner or the head of the accounting department.

A system for Authorization of internal control is a sound system for giving permissions. Authorization control procedures can be of various types. People need passwords to use computers and get into certain databases. Signature cards authorize individuals to enter safe deposit boxes, cash checks, and perform other functions at financial institutions. People are allowed to spend only what is in their budget or has been approved. When people are not allowed to do something, there are fewer opportunities

for fraud. For example, if someone is not allowed to enter a safe deposit box, they cannot steal the things inside. When someone is not allowed to make purchases, they cannot order things for themselves and have their companies pay for them. As the above fraud cases show, it is effortless to commit fraud when authorization controls are not in place.

### **5.5 Poor Monitoring And Security Of Personal Data**

According to the Bureau of Justice Statistics of the U.S. Department of Justice, in 2016, one in every fourteen Americans was the target or a victim of identity theft (Harrell & Langdon 2013). This led to \$124.7 billion in financial damages. Identity theft affected 16.6 million people, most of whom came from households with annual earnings of \$75,000 or more. The average financial loss for the victims was \$1,769. Relatively just 50,000 people were found to be the victim of identity theft in the middle of the 1990s, resulting in \$745 million in total losses (Hemphill 2001).

Identity theft is among the most common financial crimes (Smith & Jorna 2018b). Studies suggest that a greater percentage of the world population is affected by identity theft each year than by any other crime (Attorney-General's Department 2016; Smith & Jorna 2018b). Identity theft has been defined by many scholars in a variety of ways. Golladay and Holtfreter (2017: 741-42) define identity theft as the unauthorized use of another person's identity information without that person's consent. Wall (2013: 437) refers to a wide variety of crimes under the general phrase "identity crime" that involves identification document theft to commit identity fraud (Jamieson et al. 2008; Kraemer-Mbula, Tang & Rush 2013; Saunders & Zucker 1999).

Identity theft, also known as identity fraud (Pontell 2002), has become a threat to international financial markets (Allison, Schuck, & Lersch 2005, Gordon et al. 2004; Pontell 2009). Identity Theft is typically understood to involve the wrongful use of

another person's personal identifying information (Allison et al. 2005; Copes & Vieraitis 2009a; White & Fisher 2008). In its broadest sense, Identity theft is the unauthorized use of another person's personal information (Bellah 2001, p. 222). The person's name, address, social security number, date of birth, registration number, taxpayer identification number, government passport number, information from their driver's license, parental maiden name, or biometric data like a fingerprint, voice print, or retinal image can all be considered personal identifying information (U.S. Government Accounting Office 2002c). In this context, unlawful refers to the unauthorized and malicious use of another person's personal data.

The Identity Theft Assumption and Deterrence Act (ITADA), passed in 1998 in the USA, states that identity theft occurs when a person “knowingly transfers, possesses or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.”

Identity thieves have evolved a variety of tactics, both low-tech (offline) and high-tech (internet), to steal the personally identifying information of their victims (Copes & Vieraitis 2012). Criminals get this information from various sources, including companies or organizations that keep records of their clients, staff, patients, or students. In order to gain access to information, organized rings may "plant" an employee in a company or a human resources department (Copes & Vieraitis 2012). Other thieves claim to have purchased information from other criminals (Copes & Vieraitis 2012; Duffin et al. 2006). Underground websites and forums offer for sale of stolen information (such as credit card and bank account details) for relatively low prices (Holt & Lampke 2010).

There are several ways an identity thief can benefit financially and/or materially once they get access to a victim's information. Some fraudsters order new credit cards using the information, or they persuade the credit card company to issue a second card for an existing account. They use their credit cards to purchase goods for their own use, resale to friends and/or acquaintances, or return the goods for cash (Copes & Vieraitis 2009a, 2009b, 2012; Duffin et al. 2006). Offenders also use the cheques that are routinely sent to credit card holders to deposit in the victim's account and then withdraw cash or open new accounts (Koops & Leenes 2006). Additionally, it has been reported that identity thieves have used stolen identities to apply for credit cards (Newman 1999; Office of Inspector General 1999). Producing counterfeit cheques, opening new bank accounts to deposit cheques, taking money out of an existing account, and applying for and receiving loans (such as home mortgages and auto loans) are some additional common methods for converting information into money or goods (Copes & Vieraitis 2009b, 2012; Duffin et al. 2006). Additionally, some criminals use the information to obtain government benefits like Social Security, Medicare, and Disability (Copes & Vieraitis 2009a, 2009b, 2012). Offenders use various methods to steal and manipulate information for fraudulent reasons, many of which need some level of competence to carry it out successfully.

Low technology methods are most widely used due to their relative simplicity, e.g., theft of wallets or handbags or dumpster diving. In dumpster diving, identity thieves search through a person's trash to obtain personal information. On the other hand, high-technology methods demand some capability and knowledge as compared to low-technology methods. High-tech techniques include using the Internet, skimming, pretext calling, etc. Skimming is the practice of using computers to read and save the data encoded on the magnetic strip of an ATM or credit card. After being obtained, that data is

re-encoded onto any other card with a magnetic strip, immediately converting a blank card into an ATM or credit card like the victim's (Federal Trade Commission 2000b). When criminals contact a victim under false pretense in order to collect their personal information, this is known as pretext calling (Newman 1999).

Victims of identity theft suffer severe mental and physical consequences (Shapland & Hall 2007). A unique aspect of identity theft victims is that they may no longer be able to access the goods and services for which the credentials were originally designed due to damage to the credibility or reliability of those credentials. Criminals may damage a victim's credit history or make them have a criminal record, which can have long-term impacts on the victim's capacity to gain employment, qualify for various benefits, travel, and engage in other aspects of society (Lacey & Cuganesan 2004; Smith, Brown & Harris-Hogan 2015). According to earlier research, victims face emotional problems such as depression, shock, insecurity, anger, and fear (Agnew 2002; Langton & Truman 2014; Macmillan 2001; Shapland & Hall 2007). Victims of identity theft frequently experience the same psychological consequences as other financial crimes (Marsh, Cochrane & Melville 2004). This victimization may lead to severe physical and mental health issues. Studies have shown that identity theft victimization frequently results in stress, anxiety, and depression, while many also experience guilt, shame, and rage comparable to those of violent crime victims (Button, Lewis & Tapley 2014; Cross, Smith & Richards 2014; Ganzini, McFarland & Bloom 1990; Golladay & Holtfreter 2017; Spalek 1999). Additionally, research has shown that identity theft victims experience social and behavioral consequences, such as lifestyle changes (Averdijk 2011; Gale & Coupe 2005; Xie & McDowall 2008). Identity theft victims suffer significant indirect losses in addition to emotional losses (Macmillan 2001; T. R. Miller et al. 1996). Reduced trust in families, friends, financial institutions, and law enforcement agencies is



one of the emotional consequences that victims of identity theft endure (Golladay & Holtfreter 2017; Sharp et al. 2004). These victims also face the additional challenges of remediating the financial, health, legal, and criminal activities for which they have been victimized (Green et al. 2020; Harrell 2019; Sharp et al. 2004). Victims of identity theft also experience relationship issues, reputational damages, and in severe situations, suicidal tendencies (Button, Lewis & Tapley 2014; Cross, Smith & Richards 2014). Some victims incur financial costs associated with loss of wages, medical care, and expenses for regaining the integrity of their identities (Identity Theft Resource Centre 2003, 2005; Jefferson 2004; LoPucki 2001). Poor credit ratings may lead to secondary victimization in the form of credit denial, higher insurance and credit card interest rates, cancellation of credit cards, and denial of services (phone, utilities), etc. (Baum 2006; Identity Theft Resource Centre 2005; Synovate 2003). For those who find it difficult to quickly fix identity theft-related issues, the psychological, emotional, and physical effects of identity theft also worsen (Sharp et al. 2004). The greatest strategy for dealing with identity theft is to adopt preventative measures (Milne 2003; Milne et al. 2004; Piquero et al. 2011).

Since its advancement, the Internet has expanded the geographical scope of illegal activity, giving new methods for carrying out existing criminal behavior or developing new kinds of criminal activity (Savona & Mignone 2004). Due to information and communication technologies making data collection easier and more affordable (in terms of time, money, and location), "traditional" identity theft has been replaced by cyber identity theft.

Hacking, phishing, pharming, traffic redirectors, advance-fee scams, false tax forms, keyloggers, and password stealers are some of the techniques used in cyber-identity theft, which often combines the affordances of new information and

communication technologies with social engineering (Paget 2007). Hacking has been used successfully to get large amounts of personal information (Haygood & Hensley 2006). Identity tokens and identifying information are now easy to access online, changing the scope of identity theft and broadening the pool of possible victims (Finch 2007; Marshall & Tompsett 2005).

### **5.6 Poor Accounting System**

Reliability of accounting data is one of the fundamental principles of Internal controls as defined by COSO (Albrecht 2012). Accounting records are frequently used to cover up fraud (Fama 1980). Transaction documents, either on paper or electronically, form the basis of accounting records. Paper or electronic records are altered, misplaced, or made fraudulent in order to conceal fraud (SEC v. Equity Gold et al.) Accounting records can be examined for fraud by looking at transactions with no supporting documents or by probing the transaction amount that is not reasonable. It is frequently challenging to distinguish between actual fraud and unintentional errors without a sound accounting system (Albrecht 2004). A sound accounting system should guarantee that transactions are 1) legitimate, 2) appropriately authorized, 3) complete, 4) appropriately classified, 5) reported in the appropriate period, 6) appropriately valued, and 7) correctly summarized (Albrecht 2008).

According to Hiscox Embezzlement Watchlist 2015, over 40% of fraud losses occurred due to companies' poor accounting policies and practices. Poor control over the accounting system and access to accounting records give rise to the opportunity for engaging in employee fraud using poor accounting controls (ACFE Report to Nations on Occupational Fraud & Abuse 2016). The cash clerk withdraws money from the drawer and posts a fake voucher for conveyance expenses. Without audit and supervision, this

fraud can go on forever. Anyone accessing the accounting system can use it for their benefit (Brennan & Hennessey 2001, p. 61). The legitimacy of accounting records is one of the crucial requirements for clean accounting (Albrecht 2008). The legitimacy of accounting records can be checked through audit trails of each transaction. Each transaction requires certain paperwork. For example, need recognition, purchase orders, delivery challans, and verification from the user department constitute the audit trail, which can be audited each time a payment to a vendor is made.

Accounting fraud is typically perpetrated by employees against an entity (Guy & Pany 1997). Accounting fraud is the deliberate and significant falsification of financial statements or accounting records that materially affects financial statements or financial disclosures (Beasley et al. 2011). According to Young (2000), instead of being motivated by pressure from the organization, a fraudster instead can be motivated by dishonesty and personal benefit. It might begin modestly (KPMG What Boards Need to Know About Financial Statement Fraud 2004) in areas where there are ambiguities in the accounting system or where there are alternative ways to document organizational operations. Most accounting fraud schemes revolve around "earnings management," which does not always include blatant violations of accounting standards. Most frequently, entities manage earnings by selecting accounting policies that meet earnings targets.

Beasley et al. (2010) thoroughly examined the instances of accounting fraud that the US SEC looked into between January 1998 and December 2007. According to that survey, 89 percent of fraud cases involved the chief executive officer (CEO) and/or chief financial officer (CFO). According to Black (2005), CEOs are in a unique position to influence the internal and external controls of their organizations. They can effectively "control the controllers," i.e., internal auditors, external auditors, the board of directors, etc. They frequently perpetrate fraud schemes to reduce the possibility of being caught

(Bloomfield 1997; Newman, Rhoades & Smith 1996; Wilks & Zimbelman 2004). In such situations, fraud is very challenging to spot, especially for auditors and outside stakeholders such as audit committees, investors, and regulators. Black (2005) also asserts that "control frauds" can be perceived as a subset of accounting fraud. Control frauds are the circumstances where employees view the organizations as a tool to swindle management, creditors, shareholders, contributors, or the broader public. According to Black (2005), accounting fraud is an "ideal strategy" for many white-collar crimes since it simultaneously generates personal benefits.

Accounting fraud occurs when the accounting system is fabricated or accounting standards are improperly applied and willfully misinterpreted (Rezaee 2002; Spathis, Doumplos & Zopounidis 2002). Most of the time, auditing also fails to detect the intentional accounting fraud perpetrated by the employees as employees are in charge of the accounting system, and they understand the complete accounting system better than auditors (Albrecht, Albrecht & Dunn 2001; Loebbecke, Eining & Willingham 1989). Therefore, it is crucial that auditors and other interested parties understand the relative frequency of different types of fraud (Nelson, Elliot & Tarpley 2003; Bonner, Palmrose, & Young 1998; Smith & Kida 1991; Heiman 1990; Libby & Frederick 1990). Auditors, forensics, regulators, investors, and academics can better understand the perpetration and concealment process of accounting fraud with knowledge of the frequencies and patterns of fraud schemes. Gao and Srivastava (2008) examined fraud cases reported by the US SEC published between 1997 and 2002 and compiled statistics on the prevalence of accounting fraud schemes. The term "accounting schemes" refers to accounting practices that affect how account balances are manipulated. When employees use a scheme to fabricate or conceal evidence to hide accounting fraud, the scheme is referred to as an "evidence scheme." The most common evidence-covering schemes used by employees to

hide fraud include falsifying or altering documentation, collusion with external parties, altering internal documents, and concealing documents.

### **5.7 Lack Of Independent Checks And Control Of Accounts In The System**

According to research by Clark & Hollinger, 1983, employee theft rates were found to be greater when independent or supervisory checks on employees were missing. Organizational efficiency is achieved by the division of work among employees while being governed by hierarchical performance checks and comprehensive rules and regulations (Dugan & Gibbs 2009). However, more in-depth supervision of employee performance may aggravate the instances of employee theft and sabotage, motivated by professional insults to one's dignity and self-respect (Altheide et al. 1978; Mars 2006).

Fraud occurs when there is insufficient oversight, monitoring, or an absence of an independent review of employees' work, which offers the management or agent an opportunity to engage in fraudulent behavior. A strong oversight structure can reduce fraud (Skousen et al. 2008). Various findings reveal that fraudsters are knowledgeable and skilled at taking advantage of internal control flaws and making the most of their position, function, or authorized access (Abdullahi & Mansor 2015b). Many of the biggest frauds are carried out by smart, experienced, creative people with a strong understanding of controls and vulnerabilities, which affects the individual's concern about authorized access to systems or assets (Wolfe & Hermanson 2004, p. 40).

There are two kinds of checks on employees' actions, reactions, and performance in their day-to-day professional activities. The most prominent manifestation of formal checks or supervision is auditing. The possibility of detection is increased by the presence of an internal or concurrent auditor, decreasing the opportunity for fraud. However, it is improbable that enough auditors could ever be engaged to keep a check on every

conceivable criminal circumstance (Clarke & Hough 1980). Therefore, one tactic has been to concentrate auditor oversight on specific contexts where criminality is most likely to occur.

There are still alternative ways to prevent fraud, even in the absence of formal checks. According to Sturman (1980), the proactive role of management supervision directly contributes to preventing fraud. According to Walsh (1994), the presence of management or a suitable representative reduces the levels of fraud.

Management involvement in accounting is a crucial anti-fraud measure (Hogan et al. 2008; Murphy & Dacin 2011; Trompeter et al. 2013). To increase the perception of detection, it is essential that the owner takes on specific obligations and that employees comprehend the owner's active involvement in the company's financial records (American Institute of Certified Public Accountants [AICPA] 2002). This supervision should involve monthly unopened bank statements being sent directly to the owner so that he can check them for any suspicious transactions. Cheques should be checked for any modifications or shady endorsements. To identify any unexpected tendencies, the owner should be thoroughly aware of the business's revenues and costs. Vendors should be regularly screened to ensure they are reliable; this may be done by checking to see if they are listed in the vendor master. When reviewing financial data, it is best to do so unexpectedly. Management should be looking for anything suspicious, such as missing paperwork, void transactions, documents, or payments. Finally, consider employing a specialist to examine the internal control structure explicitly.

Numerous studies demonstrate how weak supervision of employee performance and absent fraud prevention measures lead to creating accessible opportunities (Hogan et al. 2008; Trompeter et al. 2013). Opportunities are frequently created when autonomy and authority are delegated, especially when oversight and monitoring are minimal

(Cohen et al. 2011; Murphy 2012). For instance, any expense claim made by the employee must be approved by the employee's supervisor. Spending or financial approval requests should be sent to the next or higher level of authority for approval in the absence of the supervisor. Nevertheless, other research (Argyris 1964; Enzle & Anderson 1993) contends that formal checks may adversely impact employees' trustworthiness.

In 2016, Murphy and Free surveyed fraud offenders who were in prison, fraud investigators, and employees who had witnessed fraud in organizations. They looked at the possibility of instrumental climate, described as an environment in which staff members make dishonest decisions to further their interests. Their findings reveal that the instrumental climate was crucial when the fraud was committed. In their 2016 study, Zakaria et al. looked into how fraud occurs due to flaws in internal controls. Using a mixed approach that included document analysis and interviews, they discovered that internal control flaws were a significant contributor to fraud. Additionally, they discovered numerous employees had conspired to commit fraud, taking advantage of weaknesses, including ineffective supervision and flawed document control procedures.

Independent performance checks are one approach to evaluate if transactions are being performed correctly (Friedrichs 2002). These checks could consist of surprise account audits, record reconciliation, cash drawer counts, and physical inventory counts (Willison & Backhouse 2006). These kinds of checks need to be carried out by someone other than the people responsible for keeping the assets, records, or accounts in order to have some degree of independence. For instance, the person in charge of the warehouse or the person in charge of keeping the inventory records should not perform test counts of the inventory. Instead, they should be performed by a person independent of those functions and has no apparent reason to tamper with any of the counts. An internal

auditor or an accounting clerk who exclusively deals with accounts receivable could be assigned for such independent checks.

Access to computers, facilities, storage spaces, and the accounting system should be monitored by management (Bolton & Hand 2002; Huang et al. 2008). In this era of information technology, it is essential to keep a check on aspects like email usage, password-cracking attempts, and account updates or modifications (Rezaee 2005; Zahra et al. 2005).

### **5.8 Poor Control Of Signed Cheques**

The above are merely two examples of poor management of signed cheques. The authority signing the cheques or approving the payments was not reviewing the complete documentation and supporting in order to avoid such fraud instances. Another mode to conduct cheque forgery may be an employee accessing the cheque register and writing a signed blank cheque in his name (Albrecht 2012). In a few cases, the contents of the cheque can be carefully altered without altering the signatures. The laxity on the part of management gives opportunity to such fraud instances (Kranacher 2008).

One cannot forge a company cheque unless they first possess one. Most forgery schemes are carried out by accounts payable clerks, office managers, bookkeepers, or other personnel whose responsibilities include the preparation of business cheques (Wolfe & Hermanson 2004). These are people who have regular access to the corporate chequebook and are thus in the best opportune position to steal blank cheques.

If the fraudster does not have access to the corporate chequebook as part of his job, he must find another way to misappropriate a cheque. How a cheque is stolen is heavily influenced by how the chequebook is handled within a particular organization (Albrecht 2012). In some instances, the chequebook is not adequately secured and is kept



in unguarded areas where anyone can access it. In other companies, where blank cheques are secured in a restricted area, the fraudster may have gained a key or combination to this area secretly. An accomplice may furnish the perpetrator with blank cheques in exchange for a percentage of the stolen funds. There are various ways to steal a cheque, depending on how an organization safeguards its blank cheques. In some cases, employees have gone so far as to create fraudulent cheques (Wells 2001).

After obtaining a blank cheque, the offender selects to whom it should be made payable. Falsified cheques are made payable to the fraudster so they can be easily converted to cash. If the fraudster has a business or has set up a shell company, he will typically write fraudulent cheques to these companies rather than himself. These cheques do not appear to be as fraudulent as cheques made payable to a company. If a fraudster is working in collusion with an accomplice, the falsified cheque can be made payable to that accomplice. Another advantage of hiring an accomplice is that a canceled cheque made payable to a third-party accomplice is less likely to raise suspicion than a cheque made payable to an employee. The perpetrator may also write cheques payable to "cash" to avoid identifying himself as the payee. To liquidate the cheque, the perpetrator must sign his own name or forge the identity of another. Cheques payable to "cash" are typically treated with greater skepticism than cheques payable to individuals or businesses (Kranacher, Riley, & Wells 2011). A fraudster may also use falsified cheque schemes to obtain products or services for personal gain by making them payable to third-party merchants not involved in the scheme. For example, an employee may counterfeit a business cheque to purchase a computer for his house. The computer vendor is not at all involved in the fraud. Furthermore, if the victim organization regularly does business with this vendor, the individual who reconciles the company's finances may believe that the cheque was used for a legitimate business transaction.

In case of a blank cheque, the employee must falsify an authorized signature in order to convert the cheque. When physically signing the cheque in the name of the authorized signatory, the fraudster faces an issue in making a reasonable facsimile of the actual signature. If the fake signature looks genuine, the employee will certainly be able to cash the cheque. On the other hand, a poorly forged signature is a glaring red flag of fraud. During the reconciliation process, the maker's signature on cheques should be checked for forgeries. Hence, in most cases, the fraudster obtains the photocopies of authorized signatures to ensure an accurate forgery. An authorized signatory's signature is duplicated from a document, which is then put over a blank cheque. As a result, the cheque has the perfect signature of an authorized signatory.

Companies that issue a large volume of cheques may use automatic cheque-signing mechanisms such as signature stamps. Obviously, an employee with access to the signature stamp faces no issues forging the signatures of authorized signatories (Kranacher et al. 2011). The most basic control is to restrict access to these mechanisms. Forged endorsements are cheque tampering techniques in which an employee intercepts a corporate cheque intended to pay a third party and converts it by endorsing it in the name of the third party. The major problem for a fraudster in a falsified endorsement scheme is acquiring access to a cheque after it has been legitimately signed. The fraudster must either steal the cheque between the time it is signed and the time it is delivered or reroute it so that it is delivered to a location where he can reclaim it. The method utilized to steal a cheque is heavily influenced by how the organization manages outgoing disbursements (Abagnale 2016). Employees handling and distributing signed cheques are best positioned to intercept them (Abagnale 2016). Due to poor internal control procedures, employees frequently get the opportunity to intercept signed cheques (Albrecht, Howe, & Romney 2008). Many employees, for example, discover signed cheques left unattended

in the work areas of the people who signed them. Clerks who write cheques for their superiors to sign are frequently in charge of delivering them (Albrecht 2014). It is relatively easier for those employees to write a fake cheque and collect a signature. This technique exemplifies the primary issue with business fraud: trust. Cheques mailed outside can subsequently be returned to the company for various reasons, such as an incorrect payee address being frequently targeted for theft by fraudsters. Employees with access to incoming mail can intercept these returned cheques and convert them by forging the intended payee's endorsement. After intercepting a cheque, the fraudster might cash it by falsifying the signature (Kranacher et al. 2011).

Cheque tempering schemes involve using the company to pay personal expenses straight from company funds. Instead of paying personal bills, the fraudster writes cheques to himself, friends, or family. These schemes easily occur since no one pays attention to accounting and due to a lack of sound internal controls to prevent fraud. Some employees who write cheques to themselves or purchase products for themselves simply reconcile the cheques to expenditure accounts in the absence of scrutiny (ACFE Report to Nations on Occupational Fraud & Abuse 2004, 2008, 2016, 2020).

In a financial institution, one person who collects the cheque on behalf of the client must get it authorized by one or more senior officials. Further, cheque washing is when someone steals a cheque while it is in transit between the person who wrote it and the recipient. Chemicals are used to remove the ink from all parts of the cheque except for the signature. The fraudster then fills in the blanks to their advantage. There are three ways to make a forged cheque: 1) Counterfeit. The cheque made on non-bank paper to look genuine. 2) Forged signature. The cheque is genuine, but the signature does not belong to the account holder. 3) Fraudulently altered. In this case, a genuine customer

writes a cheque, but the fraudster alters it, for example, changing the name of the recipient or adding words and/or numbers to make the amount bigger.

## **5.9 Poor Procurement Policies**

Fraudulent practices are widespread in the procurement department of an organization (Murray 2014). Public procurement is a crucial area for fraud due to the volume and complexity of procurement activities, the ambiguity of the market value for specific commodities, and the interdependence between business actors (Hawkins et al. 2011; Rose-Ackerman & Palifka 2016). Due to a lack of monitoring and control mechanisms, transparency and accountability, and professionalization, procurement processes also carry a higher risk of employee fraud (Kolstad & Wiig 2009; Neupane et al. 2012). It is evident that fraudsters have historically targeted the procurement function (Plavsic 2004).

While several studies have looked at related elements of procurement, there is essentially no scholarly literature on procurement fraud (Murray 2014). The hazards of bribery, fraud, and corruption as a limitation are rarely mentioned in procurement literature (Murray 2014; Tanaka & Hayashi 2016). Procurement fraud is a complex problem that can occur at any stage of the procurement of goods or services. Every year, there is a surge in procurement fraud, which has now overtaken money laundering to become the second most frequently reported global economic crime (Kroll 2013; PwC 2014). According to KPMG's forensic division, the company's procurement function is the second most targeted area by fraudsters (Plavsic 2004). Internal procurement staff, including an individual employee or group of employees working in collusion, are capable of engaging in procurement fraud by colluding with an external vendor to defraud the employer in exchange for rewards such as kickbacks, bribes, gifts, or other benefits

(Tan 2013). The pre-contract award phase involves a need recognition scheme, irregularities in the solicitation process, and bid rigging. The post-contract award phase involves falsifying invoices to support claims of goods and services that are either not provided or do not adhere to the specification of the contract (Tan 2013).

The three fundamental procurement methods are 1) competitive bidding, 2) competitive negotiation, and 3) simplified acquisition procedure. In each of these methods, a contracting officer is in charge and has the authority to spend a certain sum of money. However, such authority must always be restricted to a specific limit. The Federal Acquisition Regulation (FAR) is a set of guidelines that specifies the principles and practices that executive agencies must adhere to during the procurement process (Federal Acquisition Regulation 2016).

The procurement function always confronts a larger risk of fraud because this is how many businesses spend money (Plavsic 2004, p. 1). According to E&Y, the most prevalent type of procurement fraud is collusion between an organization's procurement department and its vendors (Tyler 1997, p. 18). Fraudsters target procurement functions across the globe, which could result in millions worth of financial and other economic damage.

Procurement fraud frequently goes unnoticed, uninvestigated, and unpublicized. Because collusion frequently occurs between employees or between employees and suppliers, procurement fraud typically goes unnoticed. Because the organizations perceive that losses may not be recovered, it goes uninvestigated. It remains unpublicized because management is embarrassed that fraud occurred and thus keeps quiet. A common target for procurement fraudsters is the provision of services, where it is challenging to determine what has been supplied and what it is really worth. Poor internal controls further ease procurement fraud.

Due to the fact that the payment or kickback from the supplier to the employee occurs outside of the place of employment, it is frequently challenging to prove that fraud has occurred. Many times, the payments are also non-cash, such as paid holidays. Even though payments and kickbacks are difficult to spot, one or more of the following red flags are associated:

- Contracts that lack any business sense. If a price seems too low, it may indicate that substandard or nonexistent goods or services are being offered. Similarly, if the price seems excessively high, it may indicate that insufficient quotations have been submitted.
- Contracts for which bids have not been tendered. A common defense in these situations is that there was only one supplier with the resources to complete the work, and that supplier was chosen without comparative quotations or the use of formal tender procedures.
- Suppliers who are awarded contracts that are too disproportionate to their size. A business contract is awarded to a supplier who will be able to complete the work on time and to the best value for the contract price.
- Tenders that have been allowed to pass even though they were received late. This includes the release of confidential bids to one particular supplier in order for them to award the final contract.
- Firms that have been requested for quotation but have not responded. Before the contract is awarded, the non-responder suppliers must be followed up.

Every organization incurs the majority of its operating expense in the "Cost of goods sold" or precisely the manufacturing costs. Hence, the proper procurement policy is a crucial deterrent to prevent widespread procurement fraud.

## **5.10 Poor Payroll Management**

Another method of carrying out an employee fraud scheme is manipulating the payroll system. Ghost employees, falsified hours, inflated pay rates, understated leave and vacation time, and unauthorized bonuses and commissions are a few examples of payroll fraud schemes (Wells 2005). Payroll fraud intends to compel the victim organization to make payments or grant benefits to which the beneficiary is not entitled (Moyes & Hasan 1996).

Since it is committed by an employee of an organization, payroll fraud is considered internal fraud. According to Singleton & Singleton (2010), payroll fraud is a scheme in which employees defraud their employer by submitting a fake remuneration claim. According to Coenen (2008), payroll fraud is a process used to cause the organization to pay money or provide benefits that are not actually owed to the beneficiary employee. According to Albrecht et al. (2012), Payroll fraud is a scheme where an employee causes their employer to give them money by drawing up false compensation claims. According to the Association of Certified Fraud Examiners (2010), Payroll fraud occurs when an employee submits a false claim for remuneration or manipulates the payroll system to obtain remuneration to which they are not legally entitled. Payroll fraud involves excessive income to an employee through deception. According to Gbegi & Okoye (2013), payroll fraud includes misrepresenting remuneration, falsifying overtime, and placing a ghost employee on the payroll. According to Hendrik (2012), the number of ghost employees on payroll is the primary indicator of payroll fraud. According to the Association of Certified Fraud Examiners (2014), a payroll fraud scheme involves making fraudulent claims, typically when a fraudster falsifies payroll records, timekeeping records, or other documents pertaining to the payroll. According to Albrecht et al. (2012), there are four main types of payroll fraud schemes: ghost employees, falsified hours, salary commission schemes, and false worker

compensation claims. They claimed that ghost employee schemes typically result in the most losses out of all payroll fraud schemes. Association of Certified Fraud Examiners (2010, 2012, 2016, 2020) states that the average loss per instance is exceptionally significant and can be highly expensive for an organization. Ghost employee fraud refers to adding someone to the payroll who does not actually work for the victim's business. According to Wells (2017), there are various methods for detecting payroll fraud, including payroll audits, surprise audits, periodic reviews of payroll reports, job rotation for payroll staff, mandated leave for payroll employees, supervisor approval for time sheets and overtime, internal payroll tax audits, the separation of payroll jobs and responsibilities, and bank statement checks for payroll staff and employees (Hall et al. 2017).

These schemes can take many forms, e.g. when employees falsify their timekeeping or add ghost or nonexistent employees to the payroll (Husnin et al. 2016; Knechel et al. 2013; Goodwin-Stewart & Kent 2006). The business issues a paycheck to the dummy worker, which in turn is cashed by the fraudster. The perpetrator of payroll schemes often falsifies a timecard or changes data in the payroll records. Payroll fraud involves payments to employees rather than third parties, which is a crucial distinction between payroll schemes and other fraud schemes (Schoenfeld 2017; Jaafar et al. 2014; Hashim et al. 2014; Eng & Mak 2003). Ghost employee schemes, falsified hours and salary schemes, and commission schemes are the most typical types of payroll fraud (Chen et al. 2016; Suhaimi et al. 2016; Doyle et al. 2007).

One of the most prevalent methods of payroll fraud is the overpayment of wages (Nelson et al. 2003). The number of hours worked, and the rate of wages are the two factors determining the size of a worker's pay cheque (Hall et al. 2017). Therefore, in order to draw excess wages, the employee has two options, either to falsify the wage rate



or inflate the hours worked. Since salaried workers are not paid according to their hours worked, they frequently inflate their pay rates to generate fictitious wages (Zakaria et al. 2016).

There are three common ways to keep track of an employee's time (Dorminey et al. 2012). An employee's start and end times can be recorded using time clocks. The time is recorded on the card that the employees enter into the clock at the start and end of their shifts. Manual timecards are created by the employee and approved by his management. When hours are manually recorded, an employee normally fills out his timecard to reflect the number of hours worked, then submits it to his supervisor for approval. The supervisor checks the timecard for accuracy, signs it to express his approval, and then submits it to the payroll department so that a pay cheque can be issued. It is easier to inflate the number of hours worked when an employee fills up his own timecard (Reinikka & Svensson 2006). He just enters fake information, indicating that he arrived earlier or left later than he actually did. The challenge is not in fabricating the timecard but in getting the false card accepted by the employee's supervisor. Sometimes, such authorization can be obtained by forging the signature of the supervisor or by collusion with the supervisor (Schertzer & Schertzer 2013).

Failure to keep proper control over timecards is a common type of control breakdown. Timecards authorized by management should be forwarded immediately to the payroll department. Those who create the timecards should not have access to them once approved. If this separation of duties is not followed, the individual who prepared the timecard may change it after his supervisor approves it and before it is delivered to payroll (McKay 2012). For example, the employee could fill out his timecard in erasable ink, get his supervisor's signature, and then modify the hours reflected on it to

overcompensate himself. Another method of falsifying hours is the misreporting of leaves and vacations.

An employee can increase his salary by adjusting his pay rate. The rate of pay of an employee is shown in his payroll records. If an employee has access to these documents or has an accomplice who does, he can change them to receive a higher pay-cheque. The lack of payroll checks provides ample opportunities for fraudsters to perpetrate a crime against the organization (Olken & Pande 2012).

### **5.11 Lack of Physical and digital access controls**

Access control to data, information, and financial records is one area that needs to be supported by an organization's culture. Conolly (2000) believes that organizations need to have a culture that makes it clear that access control is essential. Verton (2000) states that businesses will have reasonable access security control if their corporate culture is correct. Nosworthy (2000) states that an organization's culture strongly influences organizational data access security, as it may 'hinder change' and ascertain appropriate changes according to critical business processes. Borck (2000) states that adequate data access security must involve the corporate culture. Many researchers contend that information access security in an organization is essential (Sizer & Clark 1989; Schwarzwald 1999; Breidenbach 2000; von Solms 2000; Andress & Fonseca 2000; Clark-Dickson 2001; Beynon 2001). However, there has been limited research on how to evaluate an organization's access control culture.

While speaking about access controls, there are two types of threats to organizational data and information: insider and outsider. Since this research highlights the occupational fraud committed by employees, the insider threat is crucial to understand. A person with authorized access to information, people, hazardous or

priceless materials, facilities, and equipment can be anyone working for an organization at any level. A malicious insider has the potential to cause more damage to the organization and has many advantages over an outsider. Insider employees have legitimate access to resources and information, special privileges, knowledge of the organization and its operations, and the locations of important or valuable assets. Insiders will be aware of the best times, places, and ways to attack while avoiding detection. Insiders can target the information to be accessed directly and avoid most of the obstacles that an outsider may face. However, far less investment is put into controls to protect against unauthorized access threats from employees. Research shows that 70% of fraud is committed by employees, albeit 90% of security controls and monitoring are aimed at outsiders (McCue 2008). Even if there are technical access controls for employees, they should not be considered a thorough deterrent (Jones & Colwill 2008).

The entity and SOX legislation depend most heavily on security and access control to data, information, passwords, and locations (Cappelli et al. 2008; Cummings et al. 2012; Randazzo et al. 2004). Security and access are meant by permitting employees access to the requisite information they need to perform their tasks, as well as only the information they specifically require (Costa et al. 2016; Liang et al. 2016; Magklaras & Furnell 2001, 2005; Shaw et al. 1998). There is a higher fraud risk if an employee has access privileges above what is necessary to perform their assigned task (Kranacher et al. 2011).

Often, access controls are used to keep assets from being stolen through fraud or other means. By making it hard for people to get to assets, access controls like vaults, safes, fences, locks, keys, and system passwords minimize the opportunity for fraud (Band et al. 2006; Bishop et al. 2010; Maybury et al. 2005; Moore et al. 2008a; Nurse et al. 2014; Schultz 2002; Shaw et al. 1998). For example, money locked in a vault cannot

be stolen unless someone gets in without permission or if someone with permission violates the trust. Access controls are often used to protect valuable data and assets from theft or embezzlement (Gheyas & Abdallah 2016).

The opportunity to commit fraud includes having unrestricted access to resources, people, data, and computer systems that allow one to not only perpetrate but also cover up the crime (Cram et al. 2018; Teodor et al. 2014). In order to carry out their assigned tasks, employees are given a variety of access rights to resources and records, and this access is one of the essential elements of fraud (Jones & Colwill 2008). It is crucial to grant access to the resources, systems, and information only to those employees who actually need it to perform their tasks (Mohamed 2013).

For a few employees, it is easier to commit employee fraud due to increasing access to resources and data as well as enhanced influence over certain functional areas of businesses (Shaw et al. 1999). Employees' access to information, assets, data, and resources typically increases as they advance in their hierarchal positions; thus, fraudulent opportunities are created in the system. Employee fraud can be largely prevented by maintaining the physical and digital access security of the organization's premises and its assets. It directly prevents the theft and misappropriation of tangible assets. Access controls convey to staff how management secures the overall business functions (Jones & Colwill 2008).

Access controls are dedicated to physical access and digital access. It is crucial to safeguard computer systems so that users may only access the data they actually require. Access to unnecessary data and resources can lead to fraudulent activity and provide an opportunity for cover-up (Crane 2005; Hunter 2002). In the current information age, it is crucial to restrict access to digital resources (Fitzpatrick 2000; Schweizer 1993).

Customer information must be carefully protected because computerized data is susceptible to hackers and disgruntled staff.

The opportunity to commit fraud can take many different forms. Access control becomes insufficient with weaknesses in other system controls, such as accounting controls that allow authorized people to engage in fraudulent behavior. Perhaps the simplest internal control is restricting physical access to assets, data, and information. Locking desks, doors, and files seem logical, but since co-workers frequently trust each other at the office, these fundamental access control measures become weak (Im & Baskerville 2005; Stanton et al. 2005; Willison 2006; Willison & Backhouse 2006). The assumption is that control exists in measures like employee I.D.s, access control cards, electronic surveillance equipment, etc. Physical access is typically only given to people who need it to perform their assigned duties. Such controls have a deterrent effect as they make it clear to everyone involved that controls are taken seriously. Unfortunately, ineffective physical controls or restrictions also send a message that the organization is not serious about upholding adequate internal controls. There are likely additional holes in the control framework that fraudsters might exploit (Ernst & Young 2008). Effective firewalls, intrusion detection systems, and access control lists on routers can all be used to limit access over networks. Biometric authentication can be added to user authentication. Digital certificates or cryptographic handshakes can be used for authentication to other computers. Authentication codes and network traffic encryption can prevent fraudsters from entering the system undetected. Network traffic monitoring can be a valuable investigative tool for spotting odd communication patterns or sources.

## **5.12 Absence Of Cash Reconciliation And Surprise Checks On Cash**

Cash can be misappropriated in a variety of ways. Most accounting entries are on cash; hence, cash is the most commonly targeted asset. The ACFE reported in its 2002 report that the misuse or theft of non-cash assets represented 10.60% of asset misappropriations, while the misuse or theft of cash represented 89.40% of asset misappropriations with the median cost of cash schemes at \$80,000 (ACFE Report to Nations on Occupational Fraud & Abuse 2002).

Depending on the place of theft, these schemes can either be on-book or off-book frauds. Skimming and larceny are the two subcategories of cash theft fraud (Albrecht 2008). The act of skimming involves stealing money from a victim entity before it is recorded in the accounting system. Skimming schemes are referred to as "off-book" fraud since the money is taken before it is reflected in the records of the victim organization (Kranacher et al. 2004). Because of this characteristic, skimming schemes do not leave an audit trail. The victim organization might not be aware that the money was ever received because the stolen money is never recorded. As a result, it could be incredibly challenging to identify that the money has been stolen.

Skimming is one of the most prevalent types of employee fraud involving cash (Albrecht 2002). Any employee working with the cash receipt may be able to skim money. This scheme includes salespeople, tellers, and other employees as fraudsters who take direct cash payments from clients. Of course, those who interact with clients directly or handle customer payments are the most potential candidates for cash skimming.

Skimming, one of the most common types of employee fraud can occur at every moment when cash enters a business. Many skimming schemes are carried out by staff, including collecting and logging customer payments by mail. Instead of forwarding cheques to the appropriate revenue or receivables accounts, fraudsters slip them out of the incoming mail. Those dealing directly with clients or handling customer payments are the

most likely to steal cash. Examples of skimming include unrecorded sales, understated sales & receivables, theft of cheques through the mail, and short-term skimming. Unrecorded sales involve sales register alteration, skimming during non-business hours, skimming off-site sales, and poor collection procedures. The most basic skimming scheme is unrecorded sales or services. This fraud occurs when goods or services are sold, and the perpetrator collects payment but does not record the sale (Wells 2011). A second method to skim unrecorded sales is to make sales during non-business hours. The fraudster opens the store on weekends or after business hours without the owner's knowledge. The employee is then able to pocket all the proceeds from these sales. The third method of skimming unrecorded sales entails skimming at off-site locations, e.g., the apartment manager collecting the payments from tenants removes a few payments from the books and keeps them to himself. The fourth method to skim unrecorded sales or receivables involves the fraudster's taking advantage of poor collection procedures. For example, if daily receipts are not reconciled, the fraudster can skim them. Also, if numbered receipts are not used, the dishonest employee is given another opportunity to skim payments (Wells 2011). Understated sales and receivables are another form of skimming that involves recording the sale or service at a lower amount than the amount collected from the customer (Albrecht 2012). One method to perpetrate this theft would be for the dishonest employee to give the customer a receipt but remove the carbon. The salesperson could then create a company copy that reflects a lower amount and skim the difference. Another means to understate sales and receivables is to record the sale of fewer items than are actually sold. Understated sales and receivables may also occur through the use of false discounts when employees have the authority to extend discounts. When payment is made, the salesperson accepts full payment but records the transaction as though a discount was given (Wells 2011).

A third form of skimming occurs when fraudsters target cheques received through the mail. This type of theft occurs when a single employee opens the mail and records the receipt of the payments. In this situation, the employee does not record the receipt and takes the cheque (Wells, 2011).

The intentional stealing of an employer's cash (which includes both cash and cheques) without the knowledge or consent and against the will of the employer is known as cash larceny (Wells 2011). Any situation where an employee can access cash can lead to a cash larceny scheme. All businesses that receive, deposit, and distribute cash are at risk of cash larceny. Most larceny schemes include the theft of incoming cash, cash in hand or cash box, etc. Since the cash is typically kept in the drawer over the counter, a high percentage of cash larceny methods occur at cash counters.

Additionally, the cash counter witnesses a lot of activities and transactions on a daily basis, and hence this might be used as a front to steal money. An employee can frequently steal money from the counter and put it in his pocket undetected in a flurry of activity while cash is being moved back and forth between the client and staff. The easiest way to steal money is to just open the counter and take cash. The theft is frequently carried out in conjunction with a sale so as to look to be a part of the deal. In other cases, the offender waits for a quiet moment when nobody will see him opening the cash drawer.

In a larceny scheme, the amounts stolen have already been reflected in the Journal ledger. As a result, an imbalance arises between the book cash and the actual cash (Kranacher 2012). A journal is balanced by comparing the transactions on the journal to the quantity of cash in hand. However, if the books show that there should be more cash than the present, the difference could be due to larceny. In a few cases, the larceny is concealed by posting reversal transactions, which forces the journal to reconcile to the



amount of cash in hand after the theft. An employee can lower the cash balance displayed on the journal by processing fake refunds. Sometimes, an employee might manually change the existing journal vouchers instead of reversing journal entries. Again, the objective of this activity is to force a balance between cash in hand and actual cash received. Changing the cash counts is another strategy for hiding cash larceny. When cash from a ledger is totaled and prepared for the deposit, an employee simply records the incorrect amount so that the cash in hand balances with the journal's total (Wells 2004).

Concealment techniques of larceny include the fraudster's taking cash from a register assigned to another employee or using another employee's access code on a shared register. In both instances, the other employee becomes the prime suspect when the theft is discovered. Another way to avoid detection is to steal small amounts over an extended period. The missing amounts are assumed to be errors rather than fraud. Cash larceny can also be concealed by reversing entries in the accounting records, making a false refund or reducing the cash amount on the register, manually altering the register, destroying the register, or destroying all records that could implicate the fraudster (Wells 2011).

However, not all receipts go through the cash register. A common method to commit cash larceny is to take a remittance received in the mail. The dishonest employee posts the amount to the customer's account, then pockets the cash or cheque. This fraud is easily concealed if the employee has access to deposits and ledgers (Wells 2011).

Another cash larceny scheme involves stealing from the bank deposit. Where one employee is responsible for totaling the receipts, preparing a list of payments, and filling in the bank deposit slip, and another employee is responsible for making the deposit, the deposit slip should then be compared to the list. Stealing from the bank deposit is very easy when one individual has all the responsibilities mentioned above. Lapping is another

method to commit cash larceny fraud. Lapping involves an employee stealing the deposit from one day and replacing it with the next day's deposit. The second day's deposit is replaced with the third day's deposit, and so on. Another concealment method is to list the deposit as being in transit (Wells 2011). Cash is a fast-moving asset, changing hands frequently. If not appropriately monitored, Cash could easily be embezzled without anybody in the system notice.

### **5.13 Hiring Without Background Checks**

Organizations prefer applicants with no criminal record over ex-offenders. Additionally, federal or state laws also prohibit employers from hiring ex-offenders. In many countries, the law mandates criminal background checks to reduce the likelihood that an ex-offender will be hired by an organization (Stoll & Bushway 2008). Numerous studies demonstrate that an employer's decision to hire employees depends upon the criminal backgrounds of job applicants (Holzer, Raphael, & Stoll 2004; Pager 2003).

Companies prefer to hire other workers over ex-offenders because they believe the latter will be less productive or more disruptive. A person's criminal history is likely viewed by many employers as a significant indicator of their talents, work ethic, and reliability. It is a red flag indicating the individual is more likely to commit fraud at work, for instance, stealing from the employer. Employers also believe that a violent offender could endanger the safety of clients or co-workers. This could lead to claims against the company for negligence in not checking the background information of the employee. According to Uggen, Manza, and Thompson (2006:290), conducting background checks on employees is a crucial hiring step. One justification for conducting criminal background checks of prospective employees is that employers recognize a high correlation between past and future criminal offenses. Extensive research has confirmed

that criminal behavior is incessant (Blumstein Farrington, & Moitra 1988; Brame, Bushway, & Paternoster 2003; Farrington 1987; Piquero Farrington, & Blumstein, 2000). However, one body of research contends that changes in an offender's life circumstances have an impact on the likelihood that they would again engage in criminal acts (Sampson & Laub 1993; Sampson, Laub, & Wimer 2006; Uggen 1999; Wallman & Blumstein 2006; Warr 1998). Additionally, aging is one of the most potent causes of resistance to criminal conduct (Farrington 1986; Hirschi & Gottfredson 1983; Sampson & Laub 1993, 2003). However, studies on recidivism repeatedly show that people who have committed crimes in the past have the highest likelihood of doing so again within a few years of conviction, and that likelihood then gradually decreases (Maltz 1984; Schmidt & Witte 1988; Visher, Lattimore, & Linster 1991).

The accounting department is more prone to financial fraud and embezzlement as the employees have access to records and information (Winning 1996, p.1). In such a sensitive environment, if an accountant with prior embezzlement history intends to utilize the opportunities to defraud, it can be disastrous for the organization (Odom 1995). Any organization can prevent fraud by ensuring that no one with a questionable background gets employed in the first place (Kinard & Renas 1991). Nearly thirty-eight percent of organizations worldwide are unable to address fraud concerns (ACFE Report to nations on occupational fraud & abuse 2020). The employer is responsible for conducting adequate background checks on potential employees, especially for those who would have access to cash collections and disbursements. Through background checks, employers can determine whether a candidate is reliable and honest in the information they provide on their job application and in the initial interview (Clark et al. 1994). Background checks are the most efficient method for keeping people away from the company who have been accused or convicted of financial crimes (Furman 1995).

Approximately 50% of organizations in the USA revealed that they conduct criminal background checks on prospective employees (Holzer, Raphael, & Stoll 2004). Another survey recorded that 80% of large organizations in the USA conduct criminal background checks on potential hires (Society for Human Resources Management 2004). A background check is a procedure intended to validate someone's identity and guarantee reliability (Greengard 1995; Lane 1996). Depending on the person's history of fraud, delinquency, criminal activity, or credit score, one can assess their level of trustworthiness (Perry 1991; Munchus 1992). Background checks and KYC verification appear similar in numerous ways. The main distinction is that the former is utilized to confirm the candidates' identities, while the latter is implemented for consumers, vendors, and clients.

The depth of the background check increases with the candidate's hierarchal position in the company. For a CEO, CFO, or controller, deeper background checks must be required rather than for the positions of an accounting assistant or a receptionist (Albright & Denq 1996; Atkinson, Fenster, & Blumberg 1976; Holzer 1996). According to statistics, most embezzlers are "first-time" offenders (from a criminal conviction perspective). Many have simply not been discovered; others may have been discovered, but their previous employers decided not to pursue legal action, leaving no trace (Legal Action Center 2004).

Larger organizations have the resources to implement internal controls to prevent and detect fraud that may not be cost-effective for smaller organizations, such as having an internal audit department or conducting proper background checks before hiring. However, it is crucial to prescreen job applicants. Informing the applicant of the screening procedure is vital because it deters the fraudsters from applying for the job (SEARCH Group 2003). However, many people do not seek jobs with the aim of

defrauding companies (KPMG 2011). Fraudsters are frequently laid off from their jobs quietly, which gives them the opportunity to move on to another organization where they can commit fraud. If an embezzler is fired without being prosecuted, further background checks on criminal activity will not reveal anything fraudulent (Clark 2004; May 1995). Former employers could be hesitant to disclose specific details when contacted for a reference if the offender was not punished.

Although background checks have limitations, they are essential instruments in the due diligence process (Mukamal & Samuels 2003). Since financial pressure is one of the reasons why an employee commits fraud, conducting a credit check on employees having access to money or the power to circumvent internal controls is another crucial deterrent (Andrews & Bonta 2001).

Even the best controls cannot prevent fraud when dishonest people are hired. In a bank, for example, tellers, managers, loan officers, and others have access to cash every day and can steal. Since it is impossible to stop all bank fraud, banks believe that personal integrity, preventive and detective controls, and the fear of getting caught will keep people from stealing. If a company does not carefully screen job applicants and hires people who are not honest, it will have fraud incidents no matter how good its other controls are.

#### **5.14 Size Of Organization**

Though fraud occurs equally in large and small organizations, however, large organizations are more likely to suffer from fraud due to poor controls and supervision of employees (Thomas & Gibson 2003; PWC 2003). The average per-case amount of fraud perpetrated in small organizations was \$98,000, compared to \$105,500 for large

organizations (ACFE Report to Nations on Occupational Fraud & Abuse 2004).

According to ACFE, a "large business" is one that has more than 100 employees.

The size of the organization determines whether a firm is to be classified as small or large (Mutia, Zuraida, & Andriani 2011). The size of the company can be seen from its equity value, sales value, or asset value (Dang & Li 2015). The ease with which a company can get external and internal funding depends on its size. Due to their access to more parties or the confidence of having assets worth more than small businesses, large organizations typically find it easier to acquire loans from third parties.

The employment environment, including features like the size of the firm, may be the most significant determinant affecting the type and degree of employee fraud. Smigel (1970) discovered that his respondents were more willing to steal from large firms than from smaller ones. First, stealing from a large company could be rationalized more easily on the grounds that these companies are particularly exploitative and do not experience measurable damage from conventional levels of fraud. Second, the likelihood of being discovered decreases as the size of the organization increases.

Studies show that a more complex, impersonal, and decentralized nature of large companies is linked to their greater involvement with illegal activity (Coleman 1992; Shover & Bryant 1993; Simpson 1993). Major corporate breakdowns and associated patterns of corporate fraud may be attributed to excessive risk-taking, competition, and the large size and growing complexity of organizations (Skeel 2005).

The size and organizational makeup of enterprises vary widely, and as a result, so do the people who may be aware of criminal activities within those organizations. Compared to smaller businesses, larger ones are more likely to be segmented into specialized areas, which makes it easier to conceal fraudulent activity from managers and workers in other areas. Comparatively, smaller businesses are likelier to have a "flat"

management structure (Barlow 1993; Makkai & Braithwaite 1994). Top supervisors are more likely to be aware of fraudulent behavior with such a management structure. However, legally top management is accountable for fraudulent conduct that they should have known about but did not (Cohen 1998).

The kind of victimization an organization experiences is influenced by its size. The study by Kristy Holtgreter asserts a crucial connection between the size of an organizational structure and the potential for employee fraud. Regarding organizational traits, including size and internal control procedures, three types of fraud exist. For instance, she discovered that while corruption and fraudulent financial reporting occurred more frequently in larger organizations, asset misappropriation was more common in smaller organizations. Paul Jesilow and his associates (Jesilow, Geis, & O'Brien 1985) surveyed 313 auto shops throughout California to judge the impact of the size of shops on fraudulent behavior. Researchers discovered that honesty varied by size, with smaller shops showing greater honesty than larger retailers.

Tillman and Pontell (1995) found that larger, rapidly expanding firms with complicated ownership structures are more likely to engage in fraud. Other academics have also asserted that corporate fraud is influenced by size and complexity (Punch 2008). Large organizations are more prone to fraud because they are more resilient to the stigma associated with wrongdoing, and larger companies view penalties as a necessary cost of doing business (Yeager 1986). The growing size and complexity of businesses create a risk for fraud (Cooper et al. 2013). The control mechanisms at larger organizations are generally poorer than those at smaller organizations. This gives an opportunity to the fraudsters to commit their crime and escape.

However, there are arguments that fraud is more likely to occur in smaller organizations for several reasons. The Sarbanes-Oxley Act of 2002, generally known as

SOX, was created as a result of Enron and several other accounting scandals that occurred in the early 2000s (Hays & Ariail 2013). However, the Sarbanes-Oxley Act only applies to publicly traded companies (Hrncir & Metts 2012). Private and many small-size organizations with less than 100 employees are exempt from anti-fraud rules and restrictions of the SOX act (Hrncir & Metts 2012). Consequently, small businesses are frequently more vulnerable to occupational fraud due to their propensity to have little or no internal controls designed to prevent fraud (Gagliardi 2014).

Fraud prevention measures such as robust internal controls make it more difficult for small organizations to defend themselves against fraudulent actions (Singleton & Atkinson 2011). Small organizations are frequently not financially equipped to implement an appropriate internal control system, making them susceptible to employee fraud (Kapp & Heslop 2011). In many cases, small businesses only have one person in charge of all of the organization's financial functions; hence, the lack of segregation of duties creates a possibility for occupational fraud (Hrncir & Metts 2012). According to a survey of 1,483 cases conducted by the Association of Certified Fraud Examiners, Organizations with less than 100 employees had the highest incidence of occupational fraud (Bhasin 2013). Experts estimate that 30 and 50 percent of all business failures are due to occupational fraud (Hrncir & Metts 2012).

### **5.15 Organizational structure weakness**

Organizational structure, according to Mintzberg (1972), is the framework of relationships between tasks, systems, operating procedures, individuals, and groups working to accomplish objectives. An organization's structure is a collection of procedures for allocating tasks to specific functions and coordinating them. One of the services that the structure of the organization provides is aiding the information flow



(Monavarian, Asgari, & Ashena 2007). The organization's structure helps to fulfill its function in the environment (Nelson & Quick 2011). Hence, the term organizational structure refers to the formal marshalling between individuals and groups regarding the authority, responsibilities, and allocation of tasks, within the organization (Galbraith 1987; Greenberg 2011).

Numerous ways in which organizational structure and procedures influence an individual's deviant behavior have been found by criminological analyses of corporate and occupational fraud. Researchers have looked at how structural processes in organizations may produce fraudulent behavior (Kelman & Hamilton 1989; Gioia 1992), while others have examined how socialization processes in organizations can result in the normalization of fraud (Vandivier 1972; Kelman & Hamilton; Gioia) (Skolnick & Fyfe 1993; Hochstetler & Copes 2003; Crelinsten 2003). Additionally, Jackall (1988) and Pearce (2001) concentrated on the connection between formal control structures in organizations and fraud, while Vaughan (1982) investigated how the sheer structural complexity of organizations may foster deviance in organizations.

The relationship between fraudulent behaviors of employees and strategically designed organization structures exposes the fraudulent behavior of employees. Weaknesses in organizational structure arise when the organizations, as well as their leaders and managers, fail to monitor, prevent, punish, or respond to the fraudulent behavior of employees. Studies (Vaughan 1982, 1997; Meyer & Rowan 1977; DiMaggio & Powell 1983, 1991; Scott 2001) reveal that organizations significantly contribute to the employee fraud that occurs within them through elements of their formal structure.

In studies of occupational fraud, the organization structure is considered to influence ethical decision-making and employee conduct, typically at lower and mid-levels of such organizations. The embedded environment of the organization and the

prospect that fraud may occur, go hand in hand. Studies of occupational fraud start with the legal fiction of the corporation as a "person" and aim to justify the fraudulent behavior as it had human impulses and the ability to act (Cressey 1988). Hence, both the construction of the organizational structure and employee fraud result from human agency. Glasberg and Skidmore have noticed a concentration on the organization's structure in organizational deviance studies (1998: 426). Therefore, requests for definitional clarity in the study of occupational fraud (e.g., Braithwaite 1985) have led to some fragmentation across levels of analysis.

The organizational structure helps decision-making, appropriate environmental response, and inter-unit conflict resolution. The responsibilities of organizational structure include the interaction between fundamental organizational principles, coordination of its actions, and internal organizational relations in terms of reporting and receiving reports (Daft, Translated by Parsayian & Arabi 1998). Soltani (2014) identified a few potential causes of organizational wrongdoings as Ineffective boards, ineffective corporate governance and control mechanisms, distorted incentive schemes, irregular accounting practices, auditory failures, domineering CEOs, dysfunctional management practices, and a lack of a strong ethical tone at the top (Abid & Ahmed 2014).

A clear organizational structure is crucial to deter employees from committing fraud (Albrecht 2004). Fraud is less likely to happen when everyone in an organization knows precisely who is in charge of each business activity. With a clearly defined organizational structure, it is easier to find assets that have gone missing and harder to steal without getting caught (Albrecht 2012). A good control environment needs strict accountability for how a job is performed.

The organizational structure outlines the manner in which an organization operates (Jo. hatch, translated by Danayifard 2014). Weak organizational structure

denotes the conditions when there is a lack of managerial hierarchy, supervision, and communication (Rabbinz, translated by Parsian & Arabi 2012). Entrusting a whole series of tasks to one person without being supervised by another is another example of a weak organizational structure since it denotes the absence of hierarchy within the system. One fundamental principle of sound organizational structure is that different departments must function under different supervision (Tafreshi, Yusefi, & Khadivi 2002). For example, suppose an employee independently manages the procurement function and also has the authority to independently approve the payment against those procurements. In that case, the organizational structure becomes weak, and the opportunity for fraudulent conduct arises.

Corporate culture is an essential and embedded feature of organizational structure as it influences and directs the behavior of members of the organization. Both organizational structure and Corporate culture affect all three sides of the fraud triangle, according to a study on preventing and detecting financial fraud by the Centre for Audit Control (2010). A robust ethical culture within the organizational structure fosters an expectation that employees would act morally, reducing the temptation to excuse fraudulent behavior. Additionally, it enables efficient controls and minimizes fraudulent opportunities, which increases the possibility that fraud will be swiftly discovered and lowers the pressure and incentives to conduct fraud.

Organizational structure creates the culture by defining the beliefs, values, attitudes, and behaviors displayed inside a company and its operations. It thus represents an organization's core values and how both internal and external stakeholders perceive them. Hence organizational structure is an organization's personality, including its hierarchy, common views, values, habits, methods of doing things, and explicit and tacit standards (Bouwman 2013). Organizational structure is always formal and visible (Weiss

2009). According to KPMG (2017), the organizational structure is the written standards that guide the thousands of decisions that employees make on a daily basis across the whole organization (p.4).

A sound organizational structure can resolve numerous organizational issues and challenges (Warrick 2017). In other words, a strong a sound organizational structure helps create a sustainable culture. According to Graham et al. (2015), a robust organizational structure affects performance through better execution, lines of authority and responsibility, and the empowerment of employees to make consistent decisions in challenging situations. They further stated that organizational structure has an impact on profitability, the value of the company, productivity, and innovation (Schmidt & Rosenberg 2014; Edwards 2012).

The prevalence of these fifteen sub-elements across the studied cases underlines their significance as core components that create opportunities for employee fraud. The findings of this research emphasize the need for organizations to critically assess and strengthen their internal controls, policies, and procedures. By addressing these key areas of vulnerability, organizations can significantly reduce the risk of fraud and safeguard their assets and reputation.

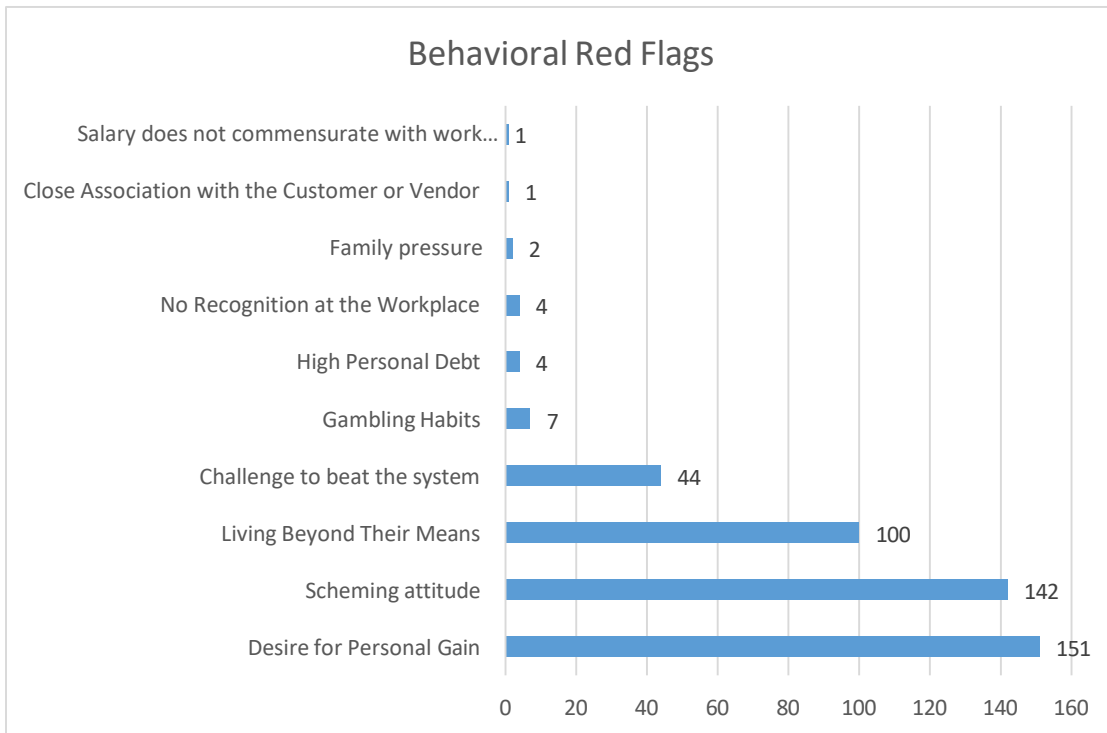
## CHAPTER 6: RED FLAGS AS A DETECTION TOOL FOR FRAUD

Through an exhaustive analysis of both behavioral and organizational red flags, this research attempts to provide organizations with pragmatic recommendations aimed at reducing the prevalence of employee fraud. This objective is instrumental in addressing the overarching research question by explaining best practices in fraud prevention that organizations may implement to fortify their defenses against employee fraud.

### **6.1 Behavioral Red Flags**

Among the behavioral red flags identified, certain patterns were consistently observed, indicating their critical role in predicting and preventing fraudulent activities. These red flags include living beyond one's means, a desire for personal gain, a scheming attitude, the challenge to beat the system, and gambling habits. These behaviors often manifest as early warning signs of potentially fraudulent activities, underscoring their importance in fraud detection and prevention strategies.

However, it is noteworthy that other red flags, such as high personal debt, close association with customers or vendors, salary disparities, family pressure, and lack of workplace recognition, were less ascertainable. This could be attributed to their inherently personal nature, which makes them less visible in a professional setting or harder to quantify.



*Figure 6 - Findings On Behavioral Red Flags As A Detection Tool For Fraud*

These findings highlight the complexity of detecting and preventing occupational fraud. They emphasize the need for organizations to adopt a comprehensive approach that combines vigilant monitoring of behavioral red flags with robust internal controls and auditing practices. Additionally, the research emphasizes the importance of fostering a culture of integrity and ethical behavior within organizations. By addressing underlying issues such as employee dissatisfaction, financial pressures, and inadequate recognition, companies can mitigate the risk of fraud. This proactive approach, coupled with effective training and awareness programs, can enhance an organization's ability to combat Employee fraud.

### **6.1.1 A desire for personal Gain**

A desire for personal gain is a significant behavioral red flag in the context of occupational or employee fraud. This motive is often driven by individual greed and the

pursuit of personal enrichment, sometimes at the expense of ethical standards and organizational loyalty. Employees harboring this desire may rationalize fraudulent behavior as a means to achieve their financial or materialistic objectives. Research in the field of fraud examination has repeatedly highlighted the critical role of personal gain as a motivator for fraudulent behavior. Even in the current research, more than 95% of the cases revealed a “Desire for personal gain” as the fraud motivator. Cressey's Fraud Triangle theory posits that one of the key elements driving an individual to commit fraud is "motivation" or "pressure," which, in many cases, is the desire for personal financial gain (Cressey 1953). This is supported by empirical studies, such as the one conducted by the Association of Certified Fraud Examiners (ACFE), which identifies personal gain as a common factor in cases of occupational fraud (ACFE Report to Nations on Occupational Fraud & Abuse 2020).

Organizations must recognize this red flag as one of the effective approaches to foster a strong ethical culture that emphasizes integrity and transparency. This can be achieved through regular ethics training, clear communication of ethical standards, and a zero-tolerance policy towards unethical behavior (Albrecht, W. S., Albrecht, C. O., & Albrecht, C. C. 2012). Additionally, implementing robust internal controls, such as segregation of duties and regular audits, can reduce opportunities for individuals to pursue personal gain through fraudulent means (Singleton, T. W., & Singleton, A. J. 2010).

### **6.1.2 Scheming Attitude**

The presence of a scheming attitude among employees is a significant behavioral red flag which is characterized by a consistent inclination towards deceptive behavior, manipulation, or circumventing established procedures for personal gain. Employees

displaying a scheming attitude are often adept at identifying and exploiting vulnerabilities within organizational systems and processes. Research in organizational behavior and psychology highlights that individuals with a scheming attitude may possess traits aligned with the 'Dark Triad' personality traits – Machiavellianism, narcissism, and psychopathy (Paulhus & Williams 2002). These traits predispose individuals to engage in manipulative behavior, a lack of empathy, and a focus on personal benefit over collective good. In an organizational context, such attitudes can manifest in various forms of misconduct, including fraud, embezzlement, or collusion with external parties to the detriment of the organization (Jones & Paulhus 2011).

From a fraud prevention perspective, implementing strong internal controls and a robust ethical framework is fundamental (Cressey 1953). Additionally, fostering a transparent and open culture where unethical behavior is neither tolerated nor rewarded is essential in mitigating the risks posed by such attitudes (Murphy & Dacin 2011). Regular training programs on ethics and compliance, along with rigorous hiring practices that include personality assessments, can also help in identifying and managing individuals prone to such behavior (Blickle et al. 2006). Organizations must be vigilant in monitoring for signs of a scheming attitude and take proactive steps to address it. This includes establishing clear channels for reporting unethical behavior and ensuring that all employees, regardless of position, are held accountable for their actions (ACFE Report to Nations on Occupational Fraud & Abuse 2020).

### **6.1.3 Living Beyond One's Means**

Living beyond one's means as a behavioral red flag in the context of employee fraud refers to situations where an employee's lifestyle appears inconsistent with their known income. This discrepancy raises suspicions about the source of additional funds,



which can be indicative of fraudulent activity. Academic research highlights this red flag as a critical indicator in detecting fraud within organizations (Singleton & Singleton 2010). Employees who display signs of living beyond their means may engage in extravagant spending, purchase luxury items, or maintain a standard of living that seems disproportionate to their salary. This behavior can be driven by various factors, including personal financial strain or a desire for materialistic validation. According to the Association of Certified Fraud Examiners (ACFE Report to Nations on Occupational Fraud & Abuse 2020), such employees might rationalize fraudulent actions as a means to sustain their lifestyle or address their financial pressures.

Organizations should be vigilant in identifying such discrepancies. Regular financial background checks and lifestyle audits can be effective tools in detecting potential fraud risks. However, it's essential to balance these measures with respect for employee privacy and legal considerations. Organizations can also foster an environment where employees feel comfortable discussing financial challenges, potentially averting the need for fraudulent actions (Wells 2017). Addressing the root causes, such as financial literacy and support for employees in financial distress, can be as crucial as implementing stringent controls.

#### **6.1.4 Challenge To Beat The System**

The behavioral red flag of a "challenge to beat the system" reflects an employee's inclination towards outsmarting or circumventing established rules and protocols. This mindset is sometimes seen as a harmless trait of a competitive or innovative individual; however, it can be a precursor to fraudulent activities, especially in positions that grant access to sensitive information or control over financial transactions. Employees exhibiting this red flag often view policies and procedures as obstacles to be overcome

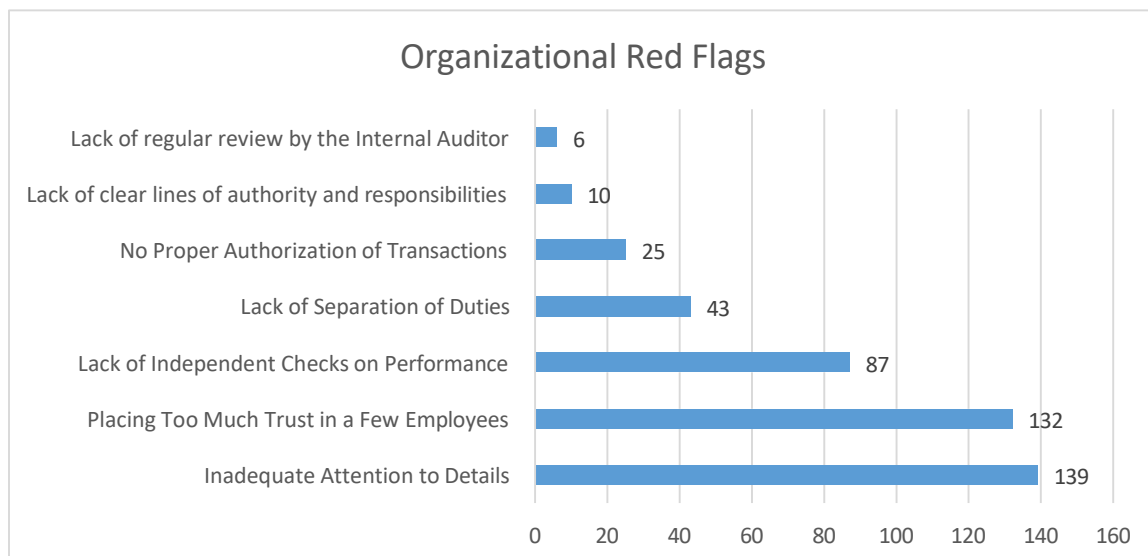
rather than safeguards to be respected. They may take pride in finding loopholes or exploiting system weaknesses, rationalizing their actions as a display of cleverness or efficiency. However, this behavior can escalate into more serious transgressions, including embezzlement, data manipulation, or other forms of fraud, as these individuals become more confident in their ability to deceive without detection.

Organizations can mitigate this risk by fostering a culture of ethical compliance and transparency. Regular training sessions emphasizing the importance of adhering to company policies and ethical standards can help inculcate a sense of responsibility and deter rule-breaking behavior. Additionally, implementing strong internal controls, such as segregation of duties, periodic audits, and robust monitoring systems, can serve as effective deterrents. These measures not only detect and prevent fraudulent activities but also discourage employees from attempting to manipulate the system in the first place. It's crucial for organizations to establish clear channels for reporting unethical behavior or system weaknesses. Encouraging open communication and providing reassurance against retaliation for whistleblowers can uncover potential risks before they manifest into fraudulent actions. By addressing the challenge to beat the system head-on, organizations can create a more secure and integrity-based work environment.

## **6.2 Organizational Red Flags**

The organizational red flags identified by ACFE include excessive trust in select employees, absence of proper transaction authorization, non-disclosure of personal investments and incomes, lack of independent performance checks, insufficient attention to details, absence of duty segregation, unclear authority lines, and infrequent reviews by internal auditors.

After examining the fraud cases, it was found that only a subset of these red flags was recurrently highlighted by the expert panel. Specifically, placing too much trust in a few employees, lack of transaction authorization, inadequate attention to detail, and irregular internal audits were commonly observed. This finding is consistent with the research of Cressey (1953), who posited that trust violation is a critical element in fraudulent activities. Moreover, it aligns with the work of Wolfe and Hermanson (2004), who emphasized the importance of internal controls in mitigating fraud risks.



*Figure 7 - Findings On Organizational Red Flags As A Detection Tool For Employee Fraud*

The less frequent occurrence of other red flags could be attributed to their more personal and less observable nature. This observation echoes the insights of Trompeter et al. (2013), who argued that personal behavioral indicators are often subtler and more challenging to detect within an organizational context. The analysis underscores the importance of comprehensive internal controls and a vigilant oversight mechanism in organizations. Regular audits, clear authorization processes, and balanced employee trust are fundamental in mitigating the risk of occupational or employee fraud.

### **6.2.1 Inadequate Attention To Details**

Inadequate attention to detail is an organizational red flag that exhibits a lack of meticulousness or thoroughness in business processes, record-keeping, and transaction monitoring. Scholarly research emphasizes that such negligence can create vulnerabilities that fraudsters exploit (Singleton & Singleton 2010). Organizations often fall prey to fraud when they overlook minor discrepancies or irregularities in financial statements, transaction records, or operational procedures. According to the Association of Certified Fraud Examiners (ACFE Report to Nations on Occupational Fraud & Abuse 2020), even small inconsistencies, if ignored, can accumulate over time, leading to substantial financial losses. For instance, inconsistencies in inventory records or unexplained alterations in vendor lists can be initial signs of ongoing fraudulent activities.

Effective fraud prevention requires organizations to instill a culture of attention to detail. This entails regular and comprehensive audits, both internal and external, and rigorous scrutiny of financial and operational records (Wells 2017). Training employees to recognize and report anomalies and encouraging a meticulous approach in their daily tasks are also essential strategies. Additionally, implementing sophisticated data analytics and monitoring tools can aid in detecting subtle signs of fraud. These tools can analyze patterns in large datasets, identifying irregularities that might go unnoticed by the human eye (Albrecht, Albrecht, & Albrecht 2012).

### **6.2.2 Placing Too Much Trust In A Few Employees**

Placing excessive trust in a few employees is an organizational red flag that can lead to significant fraud exposure within a company. This issue is particularly prevalent in smaller or closely-knit organizations where long-term employees are often given

unchecked autonomy over critical business operations. The consequences of over-reliance on a small group of employees are well-documented in fraud literature. As noted by Wells (2017) and the Association of Certified Fraud Examiners (ACFE Report to Nations on Occupational Fraud & Abuse 2020), an over-concentration of responsibilities can create opportunities for fraud, especially when there is a lack of appropriate checks and balances. Employees with unchecked control over key processes, such as financial transactions or inventory management, can easily manipulate records or misappropriate assets without detection. The concept of "trust but verify," emphasized by scholars like Singleton and Singleton (2010), underlines the importance of establishing robust oversight mechanisms, even in environments where trust is high.

Organizations must focus on implementing strong internal controls, including segregation of duties, regular audits, and transparent reporting systems. These measures help in mitigating the risks associated with placing too much trust in a few employees. Additionally, cultivating a culture of ethical behavior and transparency can discourage fraudulent activities. Training programs and clear communication of policies regarding fraud and ethical behavior can reinforce the message that while trust is valued, accountability and oversight are non-negotiable aspects of the organizational culture. While trust in employees is fundamental to a positive workplace environment, an over-reliance on a small number of employees without adequate oversight can open the door to fraudulent activities. Organizations must balance trust with effective control mechanisms to safeguard against potential fraud risks.

### **6.2.3 Lack Of Independent Checks On Performance**

The lack of independent checks on performance in an organization is a significant organizational red flag for potential fraud. This scenario often arises when there is an

absence of a system to independently review and verify the accuracy and integrity of employees' work, particularly in areas related to financial transactions and record-keeping. The importance of independent checks is emphasized in numerous studies and fraud prevention literature (Singleton & Singleton 2010; ACFE Report to Nations on Occupational Fraud & Abuse 2020). When independent reviews are not conducted, employees may have unchecked opportunities to manipulate records or engage in unauthorized activities without detection. This lack of oversight can lead to significant financial losses and damage to the organization's reputation. As per the fraud triangle theory proposed by Cressey (1953), when individuals perceive an opportunity to commit fraud without being caught – a scenario made more likely in the absence of independent checks – the likelihood of fraudulent behavior increases.

Organizations can address this red flag by implementing a robust system of internal controls, including regular audits and reviews by independent parties. This could involve periodic checks by an internal audit department or engaging external auditors to provide an objective assessment of the organization's financial and operational activities (Wells 2017). Such practices not only help in identifying discrepancies and irregularities but also serve as a deterrent to potential fraudsters. Additionally, technological solutions like automated auditing tools and data analytics can enhance the effectiveness of these independent checks by identifying patterns and anomalies that might indicate fraudulent activities (ACFE Report to Nations on Occupational Fraud & Abuse 2020).

#### **6.2.4 Lack Of Separation Of Duties**

The concept of lack of separation of duties as an organizational red flag is pivotal in understanding and preventing employee fraud. This principle, rooted in basic internal control systems, dictates that no single individual should have control over all aspects of

a financial transaction to minimize the risk of erroneous or fraudulent activities (Arens, Elder, & Beasley 2019). When duties are not adequately separated, it creates an environment prone to fraud. For example, the same person should not be responsible for authorizing transactions, recording them, and maintaining custody of the related assets. This lack of separation can lead to unchecked power, enabling employees to perpetrate fraud without detection. The Association of Certified Fraud Examiners (ACFE Report to Nations on Occupational Fraud & Abuse 2020) emphasizes that separation of duties is a critical deterrent to fraud, as it not only prevents fraudulent activities but also helps in their detection.

Organizations can mitigate this risk by implementing a system where responsibilities are distributed among different individuals or departments. For instance, the person who approves invoices should not be the same person who writes checks or reconciles bank statements (Singleton & Singleton 2010). Regular internal audits and reviews can also help in identifying any breakdown in the separation of duties. The challenge, particularly for smaller organizations, lies in limited staff, which can make it difficult to separate duties fully. In such cases, compensating controls, such as stringent oversight and periodic independent reviews, become vital (Wells 2017).

## CHAPTER 7: DISCUSSIONS AND CONCLUSION

The comprehensive analysis undertaken in this research interprets the complex dynamics of occupational fraud, presenting a holistic perspective on the mechanisms through which organizations can fortify their defenses against occupational fraud. By exploring the essence of occupational fraud, including its definition, costs, and the evaluation of established fraud theories—such as the Fraud Triangle, Fraud Diamond, Fraud Scale, MICE Model, and the SCORE Model, the study critically assessed their applicability in the contemporary organizational context.

This assessment revealed a significant gap in the existing theoretical frameworks, which fail to capture the overall nature of modern occupational fraud. Drawing from the existing literature, this research selects six pivotal elements that reinforce the phenomenon of fraud: financial pressure, opportunity, rationalization, capability, ego, and coercion, with a particular focus on the overwhelming significance of opportunity in facilitating fraudulent activities (Cressey 1953; Wolfe & Hermanson 2004).

### **7.1 Integrated Fraud Model - IFM**

As a conclusion, this study conceptualizes a comprehensive model wherein Pressure, Money, Ideology, Ego, and Coercion emerge as primary motivators propelling employees toward fraudulent behavior. These motivators, individually or in combination, precipitate the process of Rationalization, serving as a mediator that facilitates the transition towards the enactment of fraud, herein identified as the dependent variable.



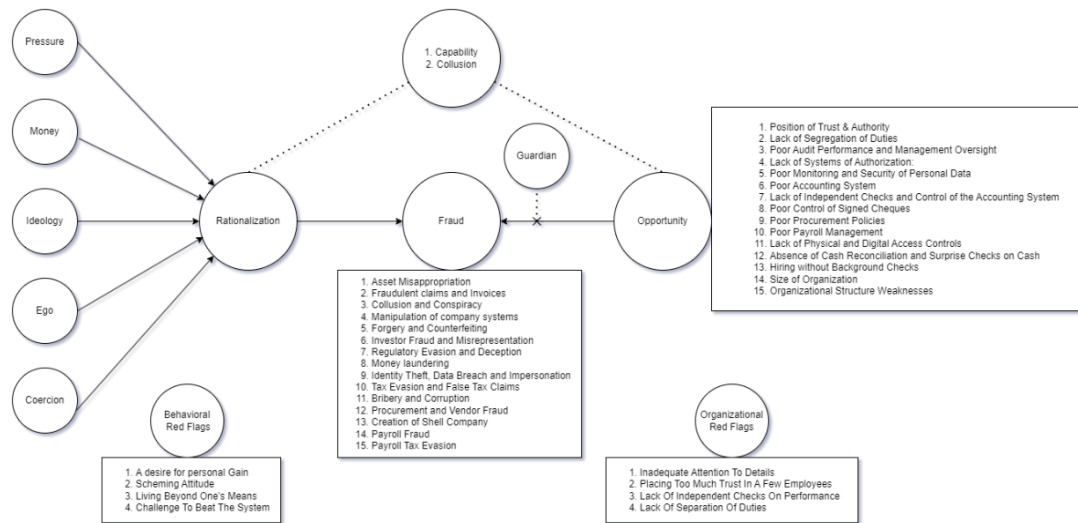


Figure 8 - First Look At The Integrated Fraud Model (IFM)

Central to the occurrence of fraud, however, is the necessity of an additional independent variable: Opportunity. This study posits Opportunity as a pivotal element without which the potential for fraud significantly diminishes. The conditions for fraud become optimal within the confluence of motivated offenders and the presence of opportunity.

Further refining the model, Capability, and Collusion are introduced as moderators that amplify the likelihood of fraud. These elements function by either augmenting the process of rationalization or by facilitating the creation of opportunities for fraud. The presence of Capability and Collusion, therefore, does not only heighten the probability of fraud but also influences the degree and severity of fraudulent activities within an organization. Importantly, while these moderators significantly contribute to the complexity of fraud occurrence, they are not deemed mandatory for its manifestation.

Additionally, the study highlights the role of Red Flags as critical indicators of potential fraud. Red flags may manifest in various forms and degrees of visibility,

presenting a challenge for organizational detection and identification. The presence of red flags, while indicative of possible fraudulent activities, does not guarantee their recognition by organizations due to their often subtle or intangible nature. Therefore, it is imperative for organizations to cultivate a heightened awareness and understanding of these red flags as part of a comprehensive fraud prevention strategy. By doing so, organizations can proactively address vulnerabilities and mitigate the risk of fraud from its inception. This understanding of the interplay between motivators, rationalization, opportunity, moderators, and red flags provides a robust theoretical framework for examining and addressing the complex dynamics of fraud within organizational settings.

## **7.2 Interplay Of IFM Elements With Central Focus On Opportunity**

As far as opportunity is concerned, fraud literature can be understood in two ways. One is the "available opportunity" that attracts a person to commit fraud (accidental fraudster) subject to their moral ethics, and another is the "creation of opportunity," which is mainly used by seasoned perpetrators (predators). Available opportunity comes with poor internal controls, management oversight, lack of supervision, etc. On the other hand, a fraudster can create the opportunity using his position of trust in the organization, coercion, collusion, etc. The fact that all fraud theories contend that opportunity is a necessary (although not sufficient) condition of fraud is one reason why the study concentrates on it. Fraud opportunity is frequently left undefined, even though it is primarily believed to be a crucial part of any explanation of crime. Crime is supposed to arise from opportunity (among other things), but systematic conceptualizations and theorizing about the opportunity as such are usually absent. This is how the idea of criminal opportunity operates. It seems fair to construct a conceptual

framework with criminal opportunity as its primary emphasis, given that opportunity is an assumed necessary condition for the crime.

On the basis of research conducted, the study explores that all crimes require that the perpetrators have some opportunity to commit a crime and that various crimes have various "opportunity structures." Since it is so apparent, the notion that opportunity must exist for crime to occur holds reasonably good (Albrecht et al. 2015; Dorminey et al. 2015, 2012, 2010; Rodgers et al. 2015). Of course, motivation is crucial, but not all (Dorminey et al. 2012, 2010). However, the seemingly straightforward concept of opportunity turns out to be more complicated. This has several significant ramifications for the comprehension of the origins of fraud and the challenge of managing it.

Although there has been much research on fraud in recent years, the role of opportunity has not been clearly defined in fraud occurrence (AICPA 2016; Dorminey et al. 2012, 2010; Tipgos 2002). The opportunities to perpetrate fraud are unequal across society (Felson & Clarke 1998). Fraud opportunities are more accessible to some people than to others. The opportunity angle makes us aware that, on occasion, organizations may be able to stop or, at the very least, lessen specific types of fraud. Instead, there are occasions when we can prevent crimes by changing a part of the opportunity structure. One more thing to comprehend is that motivation and rationalization are the innate attributes of a fraudster, while the opportunity is beyond their control to some extent (Albrecht et al. 2015; Friedrichs 2010; Holtfreter 2005). Opportunity comes with poor policies, weaker safeguard measures, management oversight, and poor internal controls (Farrell et al. 1995; Farrell & Pease 2007). It is more challenging to prevent fraudsters from creating an opportunity to perpetrate fraud. If a determined fraudulent mind has decided to create a fraud opportunity, it is more likely that fraud will be perpetrated (Albrecht 2012).

It is essential to focus on both the perpetrator of fraud and the conditions in which fraud is committed in order to comprehend why a specific fraud occurs at a specific time and location. Understanding a fraudster's intentions or justifications for committing a crime is crucial. Moreover, even if the criminal has a compelling reason, say, hunger, the desire for money does not explain why he picks one specific victim over the other. The answer is the presence and absence of opportunity among victims. Opportunities for crime are generally acknowledged as a significant contributor to all crime (Felson 2002). A crime does not seem to occur if there is no opportunity.

In accordance with routine activity theory, a criminal opportunity consists of three components: a motivated offender, a suitable target, and the absence of a capable guardian (Cohen & Felson 1979). According to Felson, individuals with good resources target people with weaker resources (Felson 1996). The absence of capable guardians is the other element of a criminal opportunity. Capable guardian means any measure that can either stop the fraudster from committing a crime or persuade him that it would be too risky to pursue (Felson 1998). The two basic types of guardianship are access restrictions and surveillance. Fraudsters may be discouraged from pursuing an opportunity if they believe doing so would be too risky. Riskiness refers to the possibility that the perpetrator will be seen or otherwise caught while doing the act or later on (Tedeschi & Felson 1994).

The perceived opportunity enables fraud since internal controls and governance are weak. Conditions are ideal for an employee to commit fraud once they believe there is a chance to do so, such as when there is a lack of segregation of duties, poor internal controls, or irregular audits. When one of the other elements, such as pressure, incentive, or rationalization, is present, the consequences are amplified. The perpetrator's

impression of opportunity is comparable to their perception of perceived pressure (Wells 2011).

Although the idea of criminal opportunity has received relatively little theoretical attention, two major theoretical traditions, i.e., routine activity and social control theory, have examined the inner workings of opportunity. Since this research aims to develop opportunity as a significant study of fraud for future research, analysis of these two major theories on which criminal opportunity theory is based is crucial. The author examines the background and fundamental features of criminal opportunity theory and proposes how a modified method can assist in studying fraud.

Every crime results from the interaction of two variables: the motivation of the offender to commit a crime and the availability of the opportunity to do so in a specific circumstance (Felson & Clarke 1998). The first factor, the motivation or propensity to commit an offense, has been the main emphasis of traditional criminology. As a result, theories of crime are frequently considered the theories of motivations that have, if not neglected, put less emphasis on the element of opportunity. Thus, the significance of situational opportunity has historically been neglected in literature and seen as not being particularly important (Clarke & Felson 2011). Situational opportunity theories are frequently referred to as environmental criminology because they emphasize how the physical and social environment impacts the availability of criminal opportunities (Bottoms 1994).

Routine Activity Theory (Cohen & Felson 1979) has been the subject of considerable research over the last four decades (Bennett 1991; Reynald 2010; Hollis-Peel et al. 2011). Cohen and Felson (1979) found that for a crime to happen, three elements must be present at the same time and in the same place: a motivated offender who intends to commit a crime, suitable targets available to the offender, and a lack of

capable guardian whose presence would otherwise have prevented the likelihood of crime.

According to Lawrence Cohen and Marcus Felson (1979), some people in society will be driven to commit crimes and look to take advantage of available opportunities. If a determined offender identifies a suitable target (potential victim), the issue is whether he can actually carry out his plan and commit the crime. Suitable targets can come in various forms, depending on the specific objective of the offender, the nature of the crime, and the surrounding circumstances, i.e., the available opportunities. The suitability of the target depends upon the opportunity available at the time of the offense (Tilley 1993; Laycock & Tilley 1995).

The last element of Routine Activity Theory, capable guardianship, can deter or prevent crime even in the presence of a suitable target and motivated offender (Cohen & Felson 1979). Capable guardianship essentially means the limiting of opportunity available for the crime (Reynald 2009, 2010). The concept of capable guardianship is broad, and researchers interpret and explore it in numerous ways. Formal forms of guardianship, like police officers and other law enforcement, stand for a widely accepted method of defense against crime, fraud, and victimization (Mayhew et al. 1976). Despite having the desire to commit a crime, many potential offenders would be reluctant to perpetrate the act in the presence of a guardian (Eck 1994; Felson & Boba 2010; Sampson et al. 2010; Tillyer & Eck 2010)

Hence, it can be inferred that the absence of a capable guardian gives rise to the opportunity for crime (Miethe & Meier 1994, p. 32). Guardianship is not just confined to individuals, e.g., law enforcement, police departments, or communities; it may also result from tangibles or environmental factors (Cohen & Felson 1979; Cohen et al. 1981). An offender may be deterred from committing a crime by a nearby security camera or a

house burglary alarm. Similarly, house fencing may impede the physical access of an offender. A wide range of environmental factors can also deter offenders, e.g., neighborhood and economic conditions (Felson & Boba 2010). According to Cohen and Felson (1979), specific social conditions impact the opportunity available for criminal conduct. Any deviation from regular and routine activities is likely to give an opportunity to the offender (Felson 2002; Tompson & Bowers 2013).

The existence or absence of guardianship has been studied for more than fifty years in the theory of literature. Guardianship is fundamental to the opportunity because they both have a negative relationship (Eck 1994). The existence of guardianship lessens the opportunity (Sampson et al., 2010 p. 39). Over the years, there have been numerous interpretations and developments of the concept of guardianship. Guardianship is an objective control that also benefits from illusion (Rengert & Wasilchick 1985). If a perpetrator believes that a CCTV camera is installed and functioning in the accounting room, he may not enter it to steal the cash. The camera's functioning can be an illusion to him; even if the camera is non-functional, the perpetrator will have to think twice before committing the theft. Even if guardians are present, though incapable, the opportunity to commit the crime lessens. An accountant believes that there are audit procedures to track any abnormal transactions. It is sufficient that auditors are present even though they may not be able to trace a fraudulent accounting journal in books. The accountant will still be deterred from posting a fraudulent voucher by the mere existence of auditors.

The original guardianship concept was further divided by Felson (1995) and others (Eck 1994; Felson & Boba 2010; Sampson et al. 2010) into three categories of controllers: handlers, managers, and guardians. Someone who oversees potential offenders and with whom offenders have emotional connections are known as handlers (Sampson et al. 2010). This group comprises people like parents, employers, and

educators. Supervisors of locations or situations where criminal conduct could occur are considered managers. Hence, managers are people whose presence and vigilance prohibit crime from occurring (Felson & Boba 2010). Managers are defined as the owners of places or the owner's representatives at the place who ensure the smooth operation of the place (Sampson et al. 2010). Guardians are those who have the objective of protecting targets (Sampson et al. 2010). Tilley (2009) further asserted that guardian capability might be less significant than guardianship credibility. Based on the above discussion, employers, owners, and shareholders can be referred to as handlers in an organization. Auditors and supervisors play the vital role of managers and sound corporate governance; audit committees and internal controls perceive the role of guardians.

In an organizational set-up, there are various instances of "absence of guardianship," e.g., poor Internal Controls, lack of segregation of duties, poor digital and physical access control, management override, too much trust in key personnel, poor human resource policies, poor audit, and supervision, absence of ethics, etc. (Locker & Godfrey 2006). However, the absence of capable guardians is only one attribute of criminal opportunity. In the absence of audit procedures or supervision, opportunities to commit fraud increase drastically.

Many scholars have conceived the importance of opportunity. For example, Green (1990) defines occupational crime or "fraud at the workplace" as any act punishable by law committed through opportunity created in the course of a legitimate occupation. Fraudsters have a stronger ability to identify the opportunity and the capacity to recognize circumstances surrounding them than other types of criminals (Benson & Simpson 2009), albeit not everyone will take advantage of the available opportunities. Shover and Hochstetler (2006: 5) assert that opportunity is in the eye of the beholder. They contend that the presence of a "lure" is the primary factor tempting people to such



opportunities. Money, ease of exploitation, or other alluring opportunities could be a lure. Shover and Hochstetler point out that not everyone reacts the same way to lure and that some people may not even notice it when it is present (ibid: 28).

Therefore, the question of why some people participate in crime when opportunities arise and others, in a similar scenario, do not still persists. According to Becker's (1968, 1976) economic theory of crime, everyone acting rationally will commit crimes if net benefits outweigh net costs. Coleman (1987), however, believes that there is a difference in how individuals estimate the risks and penalties associated with following an opportunity. One of the opportunities leading to fraud that offenders most frequently cite is weaknesses in organizational systems. Organizations allow something to occur deliberately or in ignorance because there are insufficient or no checks on their overall control environment. Therefore, an effective internal control system should reduce criminal opportunities and offer sound security management, including countermeasures for employee fraud (Bamfield 2006; Hayes 2007; 2008).

Self-control theory, as coined by Gottfredson and Hirschi (1990), specifies the role of opportunity. This idea explains the straightforward fact that illegal activity or fraud only takes place when opportunities are available. The authors of the self-control theory give a clear definition of the term "self-control"; however, they do not go into enough detail about the term "opportunity." Additionally, they lack precision in their beliefs regarding the connection between the principles of opportunity and self-control, which is why numerous authors have expanded on this connection (cf. Longshore 1998; Longshore & Turner 1998).

Self-control theory is a broad theory of deviant behavior. The theory conceptualizes criminal behavior as an action taken to maximize benefit. It states that when a person lacks self-control and is presented with an excellent opportunity to commit

a crime, deviant behavior is likely to occur (Grasmick et al. 1993). Although the authors of self-control theory assert that the theory may be applied to white-collar crime or employee fraud, other authors have cast doubt on that assertion (cf. Reed & Yeager 1996; Yeager & Reed 1998). One aspect of self-control, particularly risk-taking, was found to be relevant in terms of opportunity (Farrington 1995; Piquero & Rosay 1998).

Since the authors of self-control theory have sometimes been contradictory (Gottfredson & Hirschi 1990), the conceptualization of opportunities in employee fraud is unclear. Hence, four interpretations have been proposed based on the justifications provided in the pertinent literature: First, some authors believe that the variable of opportunity is either low (Lamnek 1994) or has no significance in crime (Fetchenhauer & Simon 1998). The second perspective holds that deviant behavior is influenced by opportunities independently (Brownfield & Sorenson 1993). Third, self-control and situational conditions interact statistically and can induce a person to utilize the opportunity (Eifler 1998, 1999, 2002; Grasmick et al. 1993; Longshore 1998; Longshore & Turner 1998; Seipel 1999a, 1999b, 2000). Fourth, the perspective proposed by Hirschi and Gottfredson (1993) is that there can be countless opportunities to commit a crime, and self-control and opportunities can sometimes interact. Otherwise, opportunity and self-control are frequently interdependent (p. 50). In the social sciences, the idea is that agent characteristics and situational factors both influence human behavior. Situational factors give rise to available opportunities, such as poor internal controls, absence of effective audits, management oversight, etc.

Identifying fraud opportunity elements, corresponding fraudulent actions, and red flags offers a comprehensive framework through which organizations can enhance their fraud prevention strategies. By systematically addressing each opportunity element, organizations can significantly reduce the vulnerabilities through which fraudsters

commit fraudulent actions. Below is an analysis of how these opportunity elements can be mitigated, referencing the associated fraudulent actions and red flags:

### **7.2.1 Position Of Trust And Authority**

Employees occupying positions of trust and authority are better positioned to exploit their roles for fraudulent purposes due to their access to sensitive information and control over organizational processes. Misusing such positions can lead to various fraudulent acts. These acts result in financial losses and erode the integrity and reputation of the organization.

Occupational fraud, committed by those in positions of trust, involves stealing or misusing an organization's assets. Employees in authoritative roles can manipulate financial records or transactions to divert organizational resources for personal gain. Similarly, these employees might engage in bribery and corruption, leveraging their authority to influence decisions or transactions in exchange for personal benefits. Employees in trusted positions can also falsify earnings or financial conditions to meet targets or manipulate stock prices.

The study of behavioral and organizational red flags plays a critical role in reducing the opportunity for such fraudulent activities. Recognizing signs such as living beyond means, a close association with vendors or customers, or a lack of regular review by internal auditors can alert organizations to potential fraud. For instance, an employee living significantly beyond their means might indicate misuse of organizational assets, while an unusually close relationship with a vendor could suggest procurement fraud or kickbacks. Similarly, the absence of regular audits and checks on performance, especially in areas under the control of a single authoritative figure, increases the risk of undetected fraud.

Employees in positions of trust and authority have the potential to commit a range of fraudulent acts due to their access and control within the organization. However, by understanding and responding to red flags, organizations can significantly reduce the opportunity for such fraud. Implementing a comprehensive approach that includes strong internal controls, regular monitoring, and a culture of ethical integrity is essential for mitigating occupational fraud risk, thereby protecting the organization's assets and reputation.

### **7.2.2 Lack Of Segregation Of Duties**

The lack of segregation of duties within an organizational structure creates a fertile ground for various fraudulent activities. This fundamental weakness in internal control allows employee fraudsters to exploit their positions by bypassing the natural checks and balances that a well-segregated system would provide. For instance, without segregation of duties, an employee could initiate, approve, and reconcile transactions without oversight, thereby facilitating the unauthorized diversion of assets or the manipulation of financial records to conceal theft or unauthorized use of organizational resources (Singleton et al. 2006).

Occupational fraud occurs when employees exploit their control over assets for personal gain. This could manifest in the theft of cash or inventory or the misdirection of funds through fraudulent disbursements. Similarly, in environments lacking segregation of duties, employees might create fictitious vendors or inflate invoices, subsequently approving these for payment, thus diverting organizational funds for personal benefit (COSO 2013). Further, the risks associated with concentrated control allow employees to alter financial data or transactions in a way that benefits them personally, potentially

leading to financial statement fraud or the concealment of other fraudulent activities (Moeller 2009).

The study and recognition of behavioral and organizational red flags can significantly mitigate these opportunities for fraud by creating awareness and prompting preemptive action. Behavioral red flags such as living beyond one's means, a close association with a customer or vendor, or a scheming attitude can indicate potential fraud risk, particularly in environments where duties are not adequately segregated. Organizational red flags like inadequate attention to detail, lack of independent checks on performance, and the absence of regular reviews by the internal auditor further highlight systemic vulnerabilities that opportunistic employees may exploit (ACFE Report to Nations on Occupational Fraud & Abuse 2020).

Organizations can reduce these opportunities for fraud by instituting rigorous controls and fostering a vigilant organizational culture. Implementing robust segregation of duties ensures that no single individual controls all aspects of any financial transaction, which is a primary defense against fraud (Treviño et al. 2003). Organizations can significantly diminish these opportunities by recognizing and responding to the associated behavioral and organizational red flags, enhancing their overall fraud prevention strategies. Establishing a culture of ethical behavior, transparency, and accountability, supported by strong internal controls, is essential in safeguarding against the risks posed by inadequate segregation of duties.

### **7.2.3 Poor Audit Performance And Management Oversight**

Poor audit performance and management oversight represent significant organizational vulnerabilities, creating prolific grounds for various forms of occupational fraud. These shortcomings in oversight mechanisms can inadvertently allow employees

to engage in fraudulent activities. The causal relationship between these opportunity elements and fraudulent actions highlights the critical importance of robust audit practices and diligent management oversight in fraud prevention.

Occupational fraud thrives in environments lacking audit performance or management oversight. In such settings, employees may find it easier to divert company assets for personal gain, as the usual checks and balances that should catch discrepancies in asset records are weakened or entirely absent. Similarly, fraud can occur when employees exploit poor oversight to establish fictitious vendors or approve inflated invoices, diverting organizational funds through collusion with external parties. In the absence of stringent review processes, employees with financial reporting responsibilities might alter records to meet targets or hide the organization's true financial health, misleading stakeholders and potentially causing significant financial damage.

The study and recognition of behavioral and organizational red flags can significantly reduce the opportunity for such fraud. Behavioral red flags such as a sudden change in lifestyle, which may indicate living beyond means, or a scheming attitude, can alert management to potential issues. Organizational red flags, such as the lack of regular reviews by internal auditors or inadequate attention to detail in financial reports, point to systemic issues that need addressing to fortify the organization against fraud.

Organizations can address these vulnerabilities by implementing stronger audit practices and enhancing management oversight. Regular, comprehensive audits, both internal and external, serve as a critical deterrent to fraudulent behavior, as they increase the likelihood of detection. Enhanced management oversight through continuous monitoring of financial activities ensures that deviations from standard operating procedures are quickly identified and addressed. Occupational fraud can be mitigated through improved audit practices, diligent oversight, and the cultivation of an

organizational culture attuned to the signs of fraud. By recognizing and acting upon both behavioral and organizational red flags, organizations can significantly reduce the incidence of fraud, protecting their assets and ensuring their long-term integrity and financial health.

#### **7.2.4 Lack Of Systems Of Authorization**

The absence of robust systems of authorization within an organization creates a significant vulnerability that employees can exploit to commit various forms of fraudulent activities. Without clear authorization protocols, the oversight over financial transactions and access to sensitive information is markedly reduced, providing an opportunity for unscrupulous employees to engage in fraudulent acts.

Where authorization controls are weak or nonexistent, there are stronger opportunities to commit fraud by the employees. In such settings, employees may find it easier to divert company assets for personal use, manipulate expense reports, or embezzle funds without detection. Similarly, it allows employees to submit or approve false expenses or payments to non-existent suppliers. The overstatement of assets or underreporting of liabilities is another fraudulent activity that can be perpetrated under the guise of insufficient authorization systems. Employees with access to financial reporting processes can manipulate data or create fictitious transactions that enhance the company's financial position, misleading stakeholders and potentially causing significant financial and reputational damage to the organization.

The study of behavioral and organizational red flags plays a crucial role in identifying and mitigating the risk of fraud in organizations lacking strong systems of authorization. Behavioral red flags such as living beyond one's means, a sudden display of wealth, or a scheming attitude among employees can indicate potential fraud.

Organizational red flags, including the absence of regular reviews by internal auditors or the concentration of multiple financial responsibilities in a single individual, further signal the potential for fraud. By recognizing and addressing these red flags, organizations can take proactive steps to strengthen their systems of authorization and oversight. Implementing dual controls, where transactions require approval from multiple individuals, and establishing clear thresholds for authorization levels can significantly reduce fraudulent activity opportunities.

### **7.2.5 Poor Monitoring And Security Of Personal Data**

The inadequate monitoring and security of personal data represents a significant vulnerability that fraudsters can exploit to commit various fraudulent acts. This lack of stringent data protection measures provides an opportunity for fraudsters to access sensitive information, which can be used in executing acts such as identity theft, data breach, and impersonation, and even facilitating more complex schemes like money laundering. Exploiting weak data security measures highlights the importance of robust monitoring and safeguarding of personal and organizational data to prevent these types of fraud.

Poor data monitoring and security directly facilitate identity theft and data breaches. Fraudsters within an organization can exploit this vulnerability to access confidential information such as social security numbers, bank account details, and personal identification information. This information can then be used to impersonate individuals, apply for credit, or conduct unauthorized transactions in their name. Such actions result in financial losses for the individuals and damage trust and integrity within the organizational ecosystem. Moreover, the inadequate security of personal data can serve as a foundation for more complex fraudulent activities like money laundering. By



accessing and manipulating personal and financial information, fraudsters can create elaborate schemes to disguise the origins of illegally obtained money, making it appear as though it derives from legitimate sources. It weakens the financial system and exposes the organization to significant legal and reputational risks.

The study of behavioral and organizational red flags plays a crucial role in reducing the opportunity for such fraud. Recognizing signs such as a scheming attitude, a challenge to beat the system, or a close association with the customer or vendor can alert organizations to potential internal threats. Behavioral red flags like living beyond means or high personal debt may indicate that an employee could be tempted to exploit vulnerabilities for personal gain. Organizational red flags, including inadequate attention to details or lack of independent checks on performance, highlight systemic weaknesses that could be exploited for fraud. Organizations must adopt a proactive approach to identify and address both behavioral and organizational red flags to mitigate the risks associated with poor data security. Implementing regular training sessions to educate employees about the importance of data security, recognizing the signs of potential fraud, and encouraging a culture of transparency and accountability are vital steps. Additionally, enhancing data protection measures through technological solutions like encryption, regular audits, and access controls can significantly reduce the vulnerability to fraud.

#### **7.2.6 Poor Accounting System**

A poor accounting system presents a significant opportunity for employee fraudsters to engage in various fraudulent activities. The inadequacy of an accounting system may stem from outdated software, insufficient recording procedures, or a lack of proper reconciliation processes, all of which create an environment where discrepancies

can go unnoticed and manipulative actions can be hidden amidst the system's inefficiencies.

Occupational fraud, one of the most direct consequences of a poor accounting system, occurs when employees exploit weaknesses in the system to divert company assets for personal use. This could be exhibited through the creation of fictitious vendors and invoices, enabling the embezzlement of funds, or through the unauthorized use of company credit cards due to inadequate tracking and approval processes within the accounting system. Further, the employees can manipulate records and transactions, leading to overstated assets or liabilities and misleading stakeholders about the organization's financial health. Employees can also take advantage of the system's incapacity to accurately track and report financial activities and submit fraudulent claims to tax authorities to benefit personally or to enhance the company's financial appearance.

The study and recognition of behavioral and organizational red flags are essential in reducing the opportunity for such fraud. Behavioral red flags, such as living beyond one's means or demonstrating a scheming attitude, can indicate potential fraudulent behavior. For instance, an employee displaying signs of significant personal wealth that are incongruous with their salary might be exploiting vulnerabilities in the accounting system to misappropriate assets. Similarly, organizational red flags like inadequate attention to details and a lack of regular review by the internal auditor highlight systemic issues that facilitate fraud. An organization that fails to implement thorough checks and balances, including regular audits and independent reviews, is at heightened risk of fraud, as the oversight necessary to detect and prevent manipulation of financial records is insufficient.

Addressing these red flags involves a comprehensive approach to strengthening the accounting system and organizational practices. Implementing more sophisticated

accounting software with automated checks, real-time monitoring, and detailed reporting can significantly reduce the risk of asset misappropriation and financial statement fraud. By enhancing the accounting system and fostering an organizational culture that prioritizes ethical behavior and rigorous oversight, organizations can significantly reduce the opportunity for employee fraudsters to commit these acts.

### **7.2.7 Absence Of Independent Checks And Control Within The Accounting System**

The absence of independent checks and control within the accounting system presents a significant vulnerability that employees can exploit to commit various forms of fraud. This opportunity arises from the lack of oversight and accountability mechanisms that would otherwise serve to detect and prevent unauthorized or fraudulent activities. Independent checks, including regular audits and reviews by external parties, are crucial for maintaining the integrity of the accounting system and ensuring that transactions are recorded accurately and comply with established policies and standards.

Occupational fraud resulting from this vulnerability involves the theft or misuse of an organization's assets by an employee who exploits the lack of controls within the accounting system. Without independent verification of transactions and balances, employees can easily divert funds, misappropriate assets, or engage in unauthorized transactions without detection (Singleton et al. 2006). Similarly, fraud can occur when employees manipulate accounting records and financial reports to present a false picture of the company's financial health, often to meet targets or hide poor performance. The manipulation of company systems further facilitates these fraudulent activities, enabling employees to alter or delete information within the accounting system to conceal their actions.

The study of behavioral and organizational red flags can significantly reduce the opportunity for such fraud by highlighting indicators of potential misconduct and prompting timely investigation and intervention. Behavioral red flags such as living beyond one's means, high personal debt, and a scheming attitude may indicate an employee's motivation or inclination to commit fraud. Organizational red flags, including inadequate attention to details and the lack of separation of duties, point to systemic weaknesses that create opportunities for fraud (ACFE Report to Nations on Occupational Fraud & Abuse 2020). By addressing these red flags, organizations can implement targeted controls and corrective measures to mitigate the risk of fraud. For example, introducing regular independent audits and reviews can help identify discrepancies and irregularities in accounting records. Strengthening the internal control environment by enforcing separation of duties, implementing robust authorization processes, and enhancing the monitoring and security of the accounting system are critical steps in preventing the manipulation of financial information and unauthorized access to assets.

### **7.2.8 Poor Control of Signed Cheques**

Employee fraudsters can utilize poor control of signed cheques as a significant opportunity to commit various fraudulent acts. The absence of stringent controls over cheque issuance and signing processes allows employees to exploit this vulnerability, diverting organizational funds for personal gain or creating unauthorized financial obligations on behalf of the organization. For instance, an employee could forge signatures on company cheques to misappropriate funds or create counterfeit cheques to indirectly siphon off company assets. Such acts result in financial losses and compromise the integrity of the organization's financial management system.

The study of behavioral and organizational red flags plays a crucial role in reducing these opportunities for fraud. Behavioral red flags, such as living beyond one's means or a scheming attitude, could indicate an increased risk of engaging in fraudulent activities, including misusing signed cheques. For example, an employee displaying a significant and unexplained increase in personal wealth may be utilizing organizational resources, such as signed cheques, to finance their lifestyle. Similarly, organizational red flags, like inadequate attention to details or the lack of separation of duties, create an environment conducive to fraud. The absence of detailed scrutiny of financial documents and the concentration of financial responsibilities in the hands of a few individuals can make it easier for fraudsters to manipulate cheque controls without detection. Addressing these red flags necessitates a comprehensive approach to strengthen internal controls and vigilance within the organization. Implementing dual controls on cheque signing, where two or more authorized signatories are required for all cheques, significantly reduces the risk of forgery and misappropriation. Moreover, regular audits and reviews of cheque issuance procedures can help identify and rectify procedural weaknesses, thereby preventing the creation of counterfeit cheques.

### **7.2.9 Poor Procurement Policies**

Poor procurement policies provide rich ground for various fraudulent activities within organizations, particularly in the domain of procurement and vendor fraud. These types of fraud exploit weaknesses in procurement processes, such as inadequate vendor vetting, lack of competitive bidding, and insufficient oversight of procurement transactions. When organizations fail to implement robust procurement policies, it creates opportunities for employee fraudsters to manipulate the system for personal gain. Procurement and vendor fraud, for instance, can occur when employees collude with

external vendors to inflate invoices or create phantom vendors, siphoning off funds from the organization. The absence of stringent procurement policies makes it easier for such fraudulent schemes to go undetected. Similarly, fraud can manifest through the misdirection of company funds or the theft of company assets facilitated by the lack of controls within the procurement process. Collusion among employees or between employees and external parties can further exacerbate these issues, leading to significant financial losses and undermining the integrity of the organization's procurement functions.

The study and recognition of behavioral and organizational red flags can be crucial in reducing the opportunity for such fraudulent activities. Behavioral red flags such as living beyond one's means, a close association with a customer or vendor, or a scheming attitude may indicate an increased risk of involvement in procurement fraud. Organizational red flags, including inadequate attention to details, lack of independent checks on performance, and placing too much trust in a few employees, point toward systemic vulnerabilities that could be exploited for fraud. Organizations should undertake comprehensive reviews of their procurement policies and practices to mitigate these risks. Instituting competitive bidding processes, conducting thorough background checks on vendors, and implementing regular audits of procurement activities can help identify and address vulnerabilities. Moreover, establishing a clear separation of duties within the procurement process ensures that no single individual controls all aspects of a transaction, thereby reducing the opportunity for fraud.

#### **7.2.10 Poor Payroll Management**

Poor payroll management is a significant fraud vulnerability within organizations. By inadequately managing payroll systems, organizations inadvertently open the door to

frauds such as Payroll Fraud and Payroll Tax Evasion. These fraudulent activities lead to direct financial losses and damage the organization's reputation and trustworthiness. Payroll fraud typically involves employees manipulating the payroll system to receive compensation for hours not worked, inflating their wages, or creating ghost employees whose paychecks are diverted to fraudulent accounts. In the absence of stringent payroll management practices, such as regular audits and verifications, detecting these fraudulent activities can be challenging. Similarly, Payroll Tax Evasion occurs when individuals exploit poor payroll management to underreport wages, evade paying payroll taxes, or misclassify employees to reduce tax liabilities. This impacts the organization's financial health due to penalties back taxes and compliance with tax laws. Additionally, fraudsters may manipulate payroll figures to inflate expenses and reduce reported profits, thereby misleading investors and stakeholders about the organization's financial health. This manipulation can have far-reaching consequences, affecting investor confidence and the organization's market value.

The study and recognition of behavioral and organizational red flags play a crucial role in reducing the opportunity for such fraudulent activities. Behavioral red flags such as living beyond means, high personal debt, or a scheming attitude among employees can indicate potential fraudulent intent. Organizational red flags, including inadequate attention to details, lack of separation of duties, and the absence of regular reviews by the internal auditor, highlight systemic vulnerabilities that could facilitate payroll-related fraud. To mitigate these risks, organizations must implement robust payroll management systems, including regular and surprise audits, thorough verification processes and cross-checks to ensure accuracy and integrity in payroll transactions. Ensuring proper authorization of transactions and fostering an environment that

encourages disclosure of personal investments and incomes can further enhance transparency and accountability within the payroll process.

#### **7.2.11 Lack Of Physical And Digital Access Controls**

The absence of robust physical and digital access controls within an organization creates a substantial vulnerability that employee fraudsters can exploit to commit a variety of fraudulent acts. These acts of fraud capitalize on the ease of access to sensitive information and systems that stringent access controls should otherwise safeguard. This vulnerability highlights the necessity for organizations to diligently study and respond to both behavioral and organizational red flags as a means to mitigate such opportunities for fraud. Identity theft, data breach, and impersonation are particularly egregious consequences of inadequate access controls. Fraudsters within an organization may exploit weak digital security measures to access customer's or employee's confidential personal and financial information. This information can then be used for various malicious purposes, including opening unauthorized accounts, making fraudulent transactions, or selling the information to third parties engaged in illegal activities. They can also manipulate the company systems, allowing unauthorized employees to alter or falsify information in their records for personal gain or to cover up other fraudulent activities (Singleton et al. 2006).

The study and recognition of behavioral red flags can play a critical role in reducing these opportunities for fraud. For instance, an employee living beyond their means or desiring personal gain may be more inclined to exploit weak access controls to commit fraud. Similarly, a scheming attitude or a challenge to beat the system mentality among employees can indicate a higher risk of engaging in such deceptive practices. Organizations that are vigilant in identifying and investigating such behavioral indicators



can preemptively address potential security vulnerabilities before they are exploited (ACFE Report to Nations on Occupational Fraud & Abuse 2020). Organizational red flags, such as the lack of independent checks on performance or inadequate attention to details, also contribute to an environment where fraud can grow. The absence of a rigorous review mechanism for access control procedures and the failure to enforce policies around the authorization of transactions can facilitate unauthorized access and misuse of company assets. By strengthening organizational oversight and ensuring that roles and responsibilities are clearly defined and segregated, companies can significantly diminish the likelihood of fraud occurring through these channels. Implementing regular reviews of physical and digital access controls, coupled with ongoing monitoring of employee behaviors and the organization's adherence to internal control practices, are essential steps in fortifying defenses against fraud. This includes adopting advanced security technologies, conducting background checks, and fostering a culture of integrity and transparency within the workplace. By doing so, organizations can reduce the opportunity for fraud and build a resilient framework that deters potential fraudsters and protects the organization's assets and reputation.

#### **7.2.12 Absence Of Cash Reconciliation And Surprise Checks On Cash**

The absence of cash reconciliation and the lack of surprise checks on cash within an organization can create a significant opportunity for employee fraudsters to commit various fraudulent acts. These fraudulent activities leverage the gaps in cash management and oversight, exploiting the organization's vulnerabilities to divert funds for personal gain. As one of the most direct consequences of inadequate cash controls, occupational fraud occurs when employees embezzle company funds by exploiting the absence of regular cash reconciliation. Without this critical control measure, discrepancies in cash

balances can go unnoticed, allowing fraudsters to siphon off assets over time without detection. Employees may draw from the company's cash reserves. By underreporting cash receipts or inflating cash expenses, employees can reduce the organization's taxable income, engaging in tax evasion that impacts the organization's financial integrity and exposes it to legal penalties.

The study and recognition of behavioral and organizational red flags can significantly reduce these opportunities for fraud. Behavioral red flags, such as living beyond one's means or displaying a scheming attitude, can indicate potential fraud risks when combined with weak cash management practices. Organizational red flags, such as inadequate attention to details and the lack of independent checks on performance, further emphasize the systemic vulnerabilities that facilitate these fraudulent acts. Organizations can mitigate these risks by implementing robust cash management controls, including regular cash reconciliation processes and surprise cash checks. These practices ensure discrepancies are identified and addressed promptly, reducing the window of opportunity for asset misappropriation. Enhancing oversight mechanisms, such as instituting dual control over cash handling and conducting periodic audits, can deter fraud by introducing accountability and transparency into the process.

### **7.2.13 Hiring Without Background Checks**

The practice of hiring without conducting thorough background checks presents a significant vulnerability within organizations, creating an opportunity for potential fraudsters to infiltrate the workforce. By neglecting to vet the backgrounds of prospective employees, organizations risk employing individuals with a history of fraudulent behavior or those predisposed to commit such acts due to past experiences or affiliations. Occupational fraud can be facilitated by employees who, due to a lack of background

checks, are placed in positions where they have access to company assets without the necessary scrutiny of their integrity and past conduct. Such employees may exploit this oversight to misappropriate funds or assets for personal gain. Similarly, identity theft, data breach, and impersonation can occur when employees with a propensity for or a history of engaging in these activities are given access to sensitive information without adequate vetting. These employees might use their positions to access the personal data of customers or employees, leading to significant breaches of privacy and financial loss. Moreover, employees with a history of circumventing regulations, whether in financial reporting, safety standards, or compliance with industry-specific guidelines, can bring these deceptive practices into the organization, jeopardizing its legal standing and integrity.

The study and recognition of behavioral and organizational red flags can play a crucial role in reducing the opportunity for fraud within organizations, particularly in mitigating risks associated with inadequate hiring practices. Behavioral red flags such as a history of living beyond means, a desire for personal gain, high personal debt, or a scheming attitude can indicate a higher risk of fraudulent behavior. When these red flags are considered during hiring, organizations can take proactive steps to prevent potential fraudsters from joining the workforce. Organizational red flags, such as placing too much trust in a few employees or the lack of proper authorization of transactions, underscore the importance of implementing robust internal controls and oversight mechanisms. By instituting policies that require thorough background checks as a standard part of the hiring process, organizations can significantly reduce the risk of hiring employees who are likely to commit fraud. This approach should be complemented by ongoing monitoring and transparency within the workplace. Additionally, regular reviews by internal auditors and establishing clear lines of authority and responsibilities can ensure

that any discrepancies or suspicious behaviors are promptly identified and addressed. This vigilance can deter potential fraudsters and identify vulnerabilities within the organization's processes, thereby minimizing fraud opportunities.

#### **7.2.14 Size Of The Organization**

The size of an organization significantly influences its vulnerability to various forms of occupational fraud. With their complex structures and numerous transactions, larger organizations may inadvertently provide more opportunities for fraudulent activities to go undetected due to the sheer volume of operations and potential oversight challenges. Conversely, smaller entities might suffer from a lack of resources to implement comprehensive fraud detection and prevention measures, making them susceptible to similar risks. Understanding how the size of an organization can facilitate fraud, particularly in these areas, and recognizing the associated red flags can aid in mitigating these vulnerabilities. The complexity and volume of transactions can obscure fraudulent activities in larger organizations. Employees may exploit the organization's expansive nature to divert assets for personal gain, leveraging the chaotic environment to conceal their actions. Occupational fraud can thrive in large entities where the manipulation of records or omission of crucial financial data might be lost in the vast array of financial information processed and reported. The creation of shell companies for procurement and vendor fraud is another fraudulent activity that can be facilitated by the size of an organization. Employees may establish fictitious vendors to channel payments from the organization to themselves, exploiting the lack of visibility and control inherent in larger operations.

The study of behavioral and organizational red flags is instrumental in reducing the opportunity for such fraudulent acts. Behavioral red flags like living beyond means or

a sudden lifestyle change can indicate asset misappropriation, while a scheming attitude or a desire for personal gain might hint at an employee's inclination towards financial statement fraud or the establishment of shell companies. Organizational red flags pertinent to larger entities include inadequate attention to details and lack of separation of duties, which directly contribute to an environment where fraud can succeed. Organizations can mitigate these risks by implementing robust internal controls tailored to their size and complexity. For larger organizations, enhancing transparency and oversight, such as through regular audits and the implementation of sophisticated fraud detection software, can help identify discrepancies indicative of fraud. Focusing on cultivating an ethical organizational culture and implementing basic but effective controls, like regular reviews by internal or external auditors, can be significantly beneficial for smaller entities.

#### **7.2.15 Organizational Structure Weaknesses**

Organizational structure weaknesses present a significant vulnerability that can be exploited by employee fraudsters to commit various fraudulent acts. These structural weaknesses often result from unclear lines of authority, inadequate segregation of duties, and a lack of effective oversight mechanisms. By understanding how these weaknesses facilitate fraud, organizations can implement strategies to strengthen their structures and reduce opportunities for fraudulent behavior. Occupational fraud arises from organizational structure weaknesses. Employees may exploit unclear lines of authority and responsibilities to misappropriate company assets without detection. For instance, without clear oversight, an employee could manipulate expense reports or siphon off company funds for personal use. Additionally, fraud can occur when there is insufficient oversight over financial reporting processes. Employees might overstate revenues or

understate expenses to meet financial targets, taking advantage of the lack of clear authority and oversight within the organizational structure. In situations where policies are poorly defined or enforced, employees may collude with other employees to inflate invoices or create fictitious vendors, skimming funds off the top for personal gain. The absence of stringent controls and oversight in the process enables such fraudulent activities, highlighting the critical role of organizational structure in preventing fraud.

The study and recognition of behavioral and organizational red flags are instrumental in mitigating these risks. For example, a sudden and unexplained increase in an employee's lifestyle may indicate asset misappropriation, while inconsistencies in financial reports could hint at financial statement fraud. On the organizational side, red flags such as inadequate attention to detail, lack of separation of duties, and the absence of regular reviews by internal auditors signal structural weaknesses that could be exploited for fraud. By being vigilant and responsive to these red flags, organizations can take proactive steps to address vulnerabilities in their structures. Implementing robust internal controls, such as regular audits, clear authorization protocols, and effective monitoring systems, can help in identifying and addressing organizational weaknesses. Moreover, fostering a culture of transparency and accountability, where employees feel empowered to report suspicious activities, can enhance the detection of fraud. Training programs that educate employees about the signs of fraud and the importance of ethical behavior can also play a crucial role in preventing fraudulent activities.

### **7.3 Guidance For Industry**

Organizations can adopt the following measures to reduce fraudulent opportunities toward their fraud minimization objective:

### **7.3.1 Show That Ethics Are Essential**

Morality is significant, and most businesses are managed by decent individuals. According to research, moral dilemmas always exist in the workplace. Employees are often unaware of the moral ramifications of their actions. There are numerous things organizations may do to demonstrate that ethics are essential. A leader should always explicitly explain the need to achieve targets and efficiency through moral means. Organizations must demonstrate the importance of ethics by creating and promoting a code of conduct that aligns with their mission and vision policies. Effective standards of conduct discourage not only wrongdoing but also encourage moral leadership. Organizations can take their codes a step further by applying these concepts to their relationships with their suppliers as well. The corporation can prevent fraud by weeding out employees and business partners who ignore ethical behavior.

### **7.3.2 Facilitation Of Reporting**

Every organization must have an ethics hotline. Facilitating the reporting of witnessed wrongdoing is the most effective technique to uncover fraud (ACFE Report to Nations on Occupational Fraud & Abuse 2020). According to the Association of Certified Fraud Examiners (2014), insider tips have uncovered 43% of all frauds, which is more than all other means of detection combined, including audits. Employing a third-party hotline provider is recommended since it grants anonymity to the reporter, which boosts both the quantity and quality of reporting. For the benefit of organizations, third-party hotline providers also offer case management and investigation support. However, organizations can take interim measures to offer efficient reporting if the cost of a third-party hotline provider is too high. Organizations must make clear to the employees where

to report and that it is everyone's responsibility to report any questionable activity. In addition, leaders might take the initiative and inquire about prospective issues.

### **7.3.3 Trust But Verify**

Long-term trusted employees perpetrate the majority of fraud in organizations since it is easier for them to steal from their employer and hide their trails. Additionally, the majority of fraudsters have no history of criminal activity or fraudulent behavior. When under extreme pressure in their personal lives, such as the prospect of bankruptcy, divorce, or abuse of drugs or alcohol, good people often find themselves rationalizing fraudulent decisions. Organizations have several options for protecting themselves against employee-related fraud risks. Easier internal control measures, such as the segregation of duties and mandatory vacations, can help avoid employee theft and spot existing fraudulent schemes. With the segregation of duties, different employees are given responsibilities of asset custody, record keeping, approvals, and reviews. Similarly, different employees should be in charge of authorizing and documenting transactions. It is possible to avoid common fraud techniques like authorizing payments to a shell company or creating a ghost employee by properly segregating the duties. Organizations may monitor staff with the help of affordable technology. Even the perception of detection can be a strong deterrent to employee fraud. The "trust but verify" principle can also help lower the risk of outsider fraud, particularly phishing scams on the Internet. Employees should be obliged to always obtain permission before disclosing proprietary information to anyone. Refunds, returns, and warranty requests should all adhere to a strict procedure closely scrutinized for abuse.

### **7.3.4 Beware Of The Slippery Slope**



Organizations can further lower their risk of fraud by enforcing the company code of conduct with a strict “no exceptions” policy. Leaders frequently turn a blind eye to minor transgressions like abusing sick leaves, applying the company's assets for personal use, or inflating expense reimbursement requests. However, minor offenses that go unpunished open the door for major delinquencies subsequently if employees observe that the organization is not willing to prosecute employees accountable for violating company policies. This discourages honest employees from following the policies. Permitting the employees shortcuts to achieve performance targets and placing profits above ethics also raises the likelihood of fraud. In conclusion, regardless of who commits it or how small it might be, every offense should be thoroughly investigated and appropriately handled.

### **7.3.5 Keep An Eye Out For Odd Patterns**

Organizations can boost their opportunities of spotting fraud by keeping an eye on suspicious trends and unexpected transactions. The red flags of fraudulent conduct, such as transactions posted on holidays, rounded-off amounts, payments made to vendors at employee's addresses, or employees being paid even after their departure, can be detected using straightforward accounting checks. Using Benford's law, fraud can also be found via examination of a population of transactions. Looking through the file drawers, missing or altered documentation may be a red flag of fraud. Suspicious transaction patterns, not necessarily financial, can be behavioral red flags of fraud. According to the Association of Certified Fraud Examiners (2014), 44% of employee fraudsters live beyond their means hence paying attention to unexpected lifestyle changes among employees is of utmost importance. Other red flags of fraud include defensiveness, control concerns, and abrupt personality changes.

### **7.3.6 Good Results Do Not Justify Poor Decisions**

Organizations prefer good results over risky choices. This propensity, which psychologists refer to as "outcome bias," is a frequent cause of fraud risk in organizations. According to a recent poll by KPMG (2019), a "whatever it takes" attitude is the most frequent cause of unethical behavior among employees. Organizations can take steps to reduce outcome bias. Organizations must pay closer attention to how choices are made within them.

### **7.3.7 Provide Resources So Workers Can Achieve Their Objectives**

Giving staff the tools and resources they need to succeed can lower the risk of fraud. Without the appropriate resources to meet a stated target, employees may resent being held to what they perceive to be an unreasonable standard and rationalize cheating or fraud as a necessary evil to reach the goal. The single most prevalent rationalization for fraudulent action is when an organization sets its sales targets or efficiency goals too high, giving employees tacit license to do whatever it takes to meet them. Instead, organizations should carefully consider developing targets that challenge employees to give their full without betraying their sense of fairness. According to research, financial incentives are effective at promoting good performance. However, they tend to cause employees to focus more narrowly, lowering creative and cognitive performance.

The perception of opportunity is an essential pre-requisite for fraud to occur. An employee can conduct fraud when a control or governance system is ineffective and provides the opportunity. This is referred to as internal control vulnerabilities in accounting. The idea of perceived opportunity implies that people utilize most of their circumstances (Kelly & Hartley 2010). Perceived opportunity is similar to perceived

pressure in nature. The potential for opportunity is in the perpetrator's vision and conviction. Most of the time, fraud is more likely to occur with a lesser risk of being discovered (Cressey 1953). The potential to engage in fraudulent behavior exists in an organization due to many variables, including policy violations committed by employees and a lack of disciplinary action (Sausser 2007). Wilson (2004) defines "opportunity" as the power to circumvent fraud safeguards. Rae and Subramanian (2008) contend that opportunity refers to an employee's capacity and authority to recognize flaws in the organizational system and exploit them to commit fraud.

Additionally, according to Srivastava, Mock, Turner (2005), and Hooper et al. (2010), financial fraud is impossible to commit without an opportunity, even under conditions of tremendous pressure. An opportunity has two components: the organization's innate propensity for manipulation and the organizational conditions that might allow fraud to occur. The employee will be more likely to commit fraud if there is poor job segregation, poor internal control, irregular auditing, etc. According to Moyes et al. (2005), the existence of related party transactions is the most common opportunity they encounter. Related-party transactions were ranked third among the most frequent opportunities for fraud in a study by Wilks and Zimbelman from 2004.

Similarly, related party transactions were also conceived as crucial by Ming and Wong (2003) to assess the opportunity. According to Vance (1983), inadequate monitoring is another indicator of opportunity. Kenyon and Tilton (2006) assert that poor internal controls, a lack of monitoring & supervision, and a lack of segregation of duties may present fraud opportunities. According to Lindquist & Singleton (2006), the Association of Certified Fraud Examiners found that lack of job rotation helps employees and management take advantage of organizational failure to commit fraud successfully, fearlessly, and stress-free (Ewa & Udoayang 2012).

## **7.4 Conclusion**

This study provides a detailed insight into the relationship among fraud opportunity elements, fraudulent actions, and red flags. It emphasizes how they are all interconnected in cases of occupational fraud. This study has thoroughly analyzed the complicated dynamics that enable fraud to take place within organizations, showing that the combination of these factors creates an environment conducive to fraudulent behavior. It is crucial for organizations to take a comprehensive and unified approach to preventing and detecting fraud, carefully examining the various aspects of fraud risk factors and indicators.

Based on the findings from the analysis, the study suggests creating an Integrated Fraud Model based on a thorough analysis of fraud opportunity elements, the range of fraudulent actions that take advantage of these opportunities, and the warning signs that indicate the possibility or the actual happening of fraud. By capturing these components, the Integrated Fraud Model provides organizations with a strategic framework to proactively identify vulnerabilities, implement specific controls to reduce fraud risk and improve the detection of fraudulent activities by closely monitoring behavioral and organizational indicators.

The importance of the Integrated Fraud Model is its ability to provide organizations with a detailed perspective to understand the obscure world of occupational fraud. Highlighting the importance of staying alert and well-informed in addressing fraud risk management and promoting flexible strategies that can adapt to the changing environment of fraud threats. In addition, the model highlights the crucial importance of organizational culture, controls, and governance in creating an environment that naturally deters fraud.

## **7.5 Future Research**

This study sets the stage for further investigations into the field of preventing and detecting occupational fraud. This encourages academics and professionals to investigate the Integrated Fraud Model further, examining how it can be applied in various organizational settings and its impact on reducing fraud.

Future studies may delve deeper into the core principles of the model, exploring how well it can grow and adjust to new fraud patterns and technological progress.

Additionally, conducting empirical studies to evaluate the model's influence on fraud prevention outcomes could provide valuable insights into its practical effectiveness.

## **7.6 Closing Statement**

This dissertation stands as a valuable addition to the occupational fraud field, providing a fresh outlook on the relationship between fraud risk factors and suggesting a strategic framework for risk reduction. The Integrated Fraud Model exemplifies the study's thorough investigation of occupational fraud and captures the importance of preventing and detecting fraud in a dynamic organizational environment.

APPENDIX A:  
LIST OF CASES ANALYZED IN THIS STUDY

| S. No | Press release No. | Date of hearing | Case title   | Case Source   |
|-------|-------------------|-----------------|--|---|
| 1     | 23-333            | 24-03-2023      | CEO of Titanium Blockchain Sentenced for \$21M Cryptocurrency Fraud Scheme                   | <a href="https://www.justice.gov/opa/pr/ceo-titanium-blockchain-sentenced-21m-cryptocurrency-fraud-scheme">https://www.justice.gov/opa/pr/ceo-titanium-blockchain-sentenced-21m-cryptocurrency-fraud-scheme</a>   |
| 2     | 23-324            | 23-03-2023      | Former Puerto Rico Mayor Convicted of Accepting Bribes                                       | <a href="https://www.justice.gov/opa/pr/former-puerto-rico-mayor-convicted-accepting-bribes">https://www.justice.gov/opa/pr/former-puerto-rico-mayor-convicted-accepting-bribes</a>   |
| 3     | N/A               | 14-03-2023      | Former CFO Sentenced to 3 Years and 5 Months in Prison for Embezzling over \$1.9 Million     | <a href="https://www.justice.gov/usao-edca/pr/former-cfo-sentenced-3-years-and-5-months-prison-embezzling-over-19-million">https://www.justice.gov/usao-edca/pr/former-cfo-sentenced-3-years-and-5-months-prison-embezzling-over-19-million</a>                 |
| 4     | 23-98             | 10-03-2023      | Former Finance Director Of Non-Profit Trade Association Charged With Embezzlement Scheme     | <a href="https://www.justice.gov/usao-sdny/pr/former-finance-director-non-profit-trade-association-charged-embezzlement-scheme">https://www.justice.gov/usao-sdny/pr/former-finance-director-non-profit-trade-association-charged-embezzlement-scheme</a>       |
| 5     | N/A               | 09-03-2023      | Two North Louisiana Men Plead Guilty to Defrauding Their Employer out of Millions of Dollars | <a href="https://www.justice.gov/usao-wdla/pr/two-north-louisiana-men-plead-guilty-defrauding-their-employer-out-millions-dollars">https://www.justice.gov/usao-wdla/pr/two-north-louisiana-men-plead-guilty-defrauding-their-employer-out-millions-dollars</a> |

|    |        |            |   |   |
|----|--------|------------|---|---|
| 6  | N/A    | 09-03-2023 | Martin Woman Indicted for Larceny and Embezzlement  | <a href="https://www.justice.gov/usao-sd/pr/martin-woman-indicted-larceny-and-embezzlement">https://www.justice.gov/usao-sd/pr/martin-woman-indicted-larceny-and-embezzlement</a>   |
| 7  | 23-16  | 06-03-2023 | Former Accountant Providing Financial Services to Utah Charter Schools Indicted for \$2.5M Fraud Scheme                               | <a href="https://www.justice.gov/usao-ut/pr/former-accountant-providing-financial-services-utah-charter-schools-indicted-25m-fraud">https://www.justice.gov/usao-ut/pr/former-accountant-providing-financial-services-utah-charter-schools-indicted-25m-fraud</a> |
| 8  | N/A    | 06-03-2023 | Surgeon Convicted of Federal Charges for Accepting Over \$300,000 in Illicit Payments to Perform Spinal Surgeries at Corrupt Hospital | <a href="https://www.justice.gov/usao-cdca/pr/surgeon-convicted-federal-charges-accepting-over-300000-illicit-payments-perform">https://www.justice.gov/usao-cdca/pr/surgeon-convicted-federal-charges-accepting-over-300000-illicit-payments-perform</a>         |
| 9  | N/A    | 06-03-2023 | United Bank Senior Vice President Pleads Guilty To Embezzlement And Tax Evasion   | <a href="https://www.justice.gov/usao-wdmi/pr/2023_0306_Figg">https://www.justice.gov/usao-wdmi/pr/2023_0306_Figg</a>   |
| 10 | N/A    | 01-03-2023 | Illinois Woman Admits Stealing \$439,000 From Bank  | <a href="https://www.justice.gov/usao-edmo/pr/illinois-woman-admits-stealing-439000-bank">https://www.justice.gov/usao-edmo/pr/illinois-woman-admits-stealing-439000-bank</a>   |
| 11 | N/A    | 01-03-2023 | Tewksbury Woman Pleads Guilty to Embezzlement, Unemployment Fraud and Tax Crimes  | <a href="https://www.justice.gov/usao-ma/pr/tewksbury-woman-pleads-guilty-embezzlement-unemployment-fraud-and-tax-crimes">https://www.justice.gov/usao-ma/pr/tewksbury-woman-pleads-guilty-embezzlement-unemployment-fraud-and-tax-crimes</a>                     |
| 12 | 23-217 | 24-02-2023 | Former Insurance Executive Indicted for \$2B Fraud Scheme   | <a href="https://www.justice.gov/opa/pr/former-insurance-executive-indicted-2b-fraud-scheme">https://www.justice.gov/opa/pr/former-insurance-executive-indicted-2b-fraud-scheme</a>   |
| 13 | N/A    | 23-02-2023 | Barnstead Woman Pleads Guilty to Stealing Over \$130,000 from Barnstead and Hampton School Districts                                  | <a href="https://www.justice.gov/usao-nh/pr/barnstead-woman-pleads-guilty">https://www.justice.gov/usao-nh/pr/barnstead-woman-pleads-guilty</a>   |

|    |        |            |  |   |
|----|--------|------------|--|---|
|    |        |            |  | <a href="#">stealing-over-130000-barnstead-and-hampton-school-districts</a>   |
| 14 | N/A    | 22-02-2023 | Foley Woman Sentenced to Five Years in Prison for Embezzling Church Funds  | <a href="https://www.justice.gov/usao-sdal/pr/foley-woman-sentenced-five-years-prison-embezzling-church-funds">https://www.justice.gov/usao-sdal/pr/foley-woman-sentenced-five-years-prison-embezzling-church-funds</a>   |
| 15 | N/A    | 17-02-2023 | Former NBA Players Keyon Dooling And Alan Anderson Sentenced To 30 And 24 Months In Prison For Defrauding NBA Players' Health And Welfare Benefit Plan | <a href="https://www.justice.gov/usao-sdny/pr/former-nba-players-keyon-dooling-and-alan-anderson-sentenced-30-and-24-months-prison">https://www.justice.gov/usao-sdny/pr/former-nba-players-keyon-dooling-and-alan-anderson-sentenced-30-and-24-months-prison</a> |
| 16 | N/A    | 16-02-2023 | Amery Woman Sentenced to 18 Months for Stealing More Than \$500,000 from Special Needs Trust   | <a href="https://www.justice.gov/usao-wdwi/pr/amery-woman-sentenced-18-months-stealing-over-500000-special-needs-trust">https://www.justice.gov/usao-wdwi/pr/amery-woman-sentenced-18-months-stealing-over-500000-special-needs-trust</a>                         |
| 17 | N/A    | 15-02-2023 | Former VP and Chief Operating Officer of Chicago Area Hospital Indicted for Fraud  | <a href="https://www.justice.gov/usao-ndil/pr/former-vp-and-chief-operating-officer-chicago-area-hospital-indicted-fraud">https://www.justice.gov/usao-ndil/pr/former-vp-and-chief-operating-officer-chicago-area-hospital-indicted-fraud</a>                     |
| 18 | 23-059 | 14-02-2023 | Defendant Convicted In Scheme To Steal Nearly \$1 Million From Tech Company  | <a href="https://www.justice.gov/usao-sdny/pr/defendant-convicted-scheme-steal-nearly-1-million-tech-company">https://www.justice.gov/usao-sdny/pr/defendant-convicted-scheme-steal-nearly-1-million-tech-company</a>   |
| 19 | N/A    | 13-02-2023 | Woman Sentenced to 2 Years in Federal Prison for 13 Year-Long Scheme to Embezzle Nearly \$600,000 from Catholic Church and School                      | <a href="https://www.justice.gov/usao-sdin/pr/woman-sentenced-2-years-federal-prison-13-year-long-scheme-embezzle-nearly-600000">https://www.justice.gov/usao-sdin/pr/woman-sentenced-2-years-federal-prison-13-year-long-scheme-embezzle-nearly-600000</a>       |



|    |        |            |  |   |
|----|--------|------------|--|---|
| 20 | 23-059 | 10-02-2023 | CEO Of Cryptocurrency And Forex Trading Platform Pleads Guilty To Over \$240 Million Scheme To Defraud Investors | <a href="https://www.justice.gov/usao-sdny/pr/ceo-cryptocurrency-and-forex-trading-platform-pleads-guilty-over-240-million-scheme">https://www.justice.gov/usao-sdny/pr/ceo-cryptocurrency-and-forex-trading-platform-pleads-guilty-over-240-million-scheme</a> |
| 21 | N/A    | 10-02-2023 | Ashton J. Ryan, Jr. Found Guilty of Fraud Resulting In Failure of First NBC Bank                                 | <a href="https://www.justice.gov/usao-edla/pr/ashton-j-ryan-jr-found-guilty-fraud-resulting-failure-first-nbc-bank">https://www.justice.gov/usao-edla/pr/ashton-j-ryan-jr-found-guilty-fraud-resulting-failure-first-nbc-bank</a>                               |
| 22 | N/A    | 10-02-2023 | Fort Wayne Woman Sentenced To 30 Months In Prison  | <a href="https://www.justice.gov/usao-ndin/pr/fort-wayne-woman-sentenced-30-months-prison">https://www.justice.gov/usao-ndin/pr/fort-wayne-woman-sentenced-30-months-prison</a>   |
| 23 | N/A    | 07-02-2023 | Woman Sentenced to 6+ Years in Prison for Embezzling \$800,000 from IT Company                                   | <a href="https://www.justice.gov/usao-ndtx/pr/woman-sentenced-6-years-prison-embezzling-800000-it-company">https://www.justice.gov/usao-ndtx/pr/woman-sentenced-6-years-prison-embezzling-800000-it-company</a>   |
| 24 | N/A    | 06-02-2023 | Former City Clerk Admits Stealing \$487,673 from Small North St. Louis County Municipality                       | <a href="https://www.justice.gov/usao-edmo/pr/former-city-clerk-admits-stealing-487673-small-north-st-louis-county-municipality">https://www.justice.gov/usao-edmo/pr/former-city-clerk-admits-stealing-487673-small-north-st-louis-county-municipality</a>     |
| 25 | N/A    | 03-02-2023 | Former Bank Teller Sentenced for Federal Fraud Charges   | <a href="https://www.justice.gov/usao-edla/pr/former-bank-teller-sentenced-federal-fraud-charges">https://www.justice.gov/usao-edla/pr/former-bank-teller-sentenced-federal-fraud-charges</a>   |
| 26 | N/A    | 03-02-2023 | Union County Investment Advisor Admits Stealing Client Money   | <a href="https://www.justice.gov/usao-nj/pr/union-county-investment-advisor-admits-stealing-client-money">https://www.justice.gov/usao-nj/pr/union-county-investment-advisor-admits-stealing-client-money</a>   |

|    |        |            |   |   |
|----|--------|------------|---|---|
| 27 | 23-037 | 02-02-2023 | Former Employee Of Technology Company Pleads Guilty To Stealing Confidential Data And Extorting Company For Ransom  | <a href="https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-pleads-guilty-stealing-confidential-data-and">https://www.justice.gov/usao-sdny/pr/former-employee-technology-company-pleads-guilty-stealing-confidential-data-and</a> |
| 28 | N/A    | 02-02-2023 | Accountant Pleads Guilty to Misappropriating Funds from New Orleans Band  | <a href="https://www.justice.gov/usao-edla/pr/accountant-pleads-guilty-misappropriating-funds-new-orleans-band">https://www.justice.gov/usao-edla/pr/accountant-pleads-guilty-misappropriating-funds-new-orleans-band</a>                               |
| 29 | N/A    | 01-02-2023 | Grand Jury Charges Disbarred Plaintiffs' Lawyer Tom Girardi with Wire Fraud for Allegedly Embezzling Over \$15 Million in Client Money                                | <a href="https://www.justice.gov/usao-cdca/pr/grand-jury-charges-disbarred-plaintiffs-lawyer-tom-girardi-wire-fraud-allegedly">https://www.justice.gov/usao-cdca/pr/grand-jury-charges-disbarred-plaintiffs-lawyer-tom-girardi-wire-fraud-allegedly</a> |
| 30 | 23-119 | 31-01-2023 | Former Florida CEO Sentenced to Prison for Tax Evasion  | <a href="https://www.justice.gov/opa/pr/former-florida-ceo-sentenced-prison-tax-evasion">https://www.justice.gov/opa/pr/former-florida-ceo-sentenced-prison-tax-evasion</a>   |
| 31 | N/A    | 31-01-2023 | Former Chief Financial Officer Pleads Guilty for Failing to Pay Over \$3.6M in Employee Tax Withholdings and for Pocketing \$130,000 from his Employer's Bank Account | <a href="https://www.justice.gov/usao-ndok/pr/former-chief-financial-officer-pleads-guilty-failing-pay-over-36m-employee-tax">https://www.justice.gov/usao-ndok/pr/former-chief-financial-officer-pleads-guilty-failing-pay-over-36m-employee-tax</a>   |
| 32 | N/A    | 30-01-2023 | Chicago Illinois Man Sentenced To 30 Months In Prison For Conspiracy To Commit Wire Fraud   | <a href="https://www.justice.gov/usao-wdmi/pr/2023_0130_Groom">https://www.justice.gov/usao-wdmi/pr/2023_0130_Groom</a>   |
| 33 | 23-81  | 24-01-2023 | Former Energy Company Executive Sentenced for \$15 Million Investment Fraud   | <a href="https://www.justice.gov/opa/pr/former-energy-company-executive-sentenced-15-million-investment-fraud">https://www.justice.gov/opa/pr/former-energy-company-executive-sentenced-15-million-investment-fraud</a>                                 |

|    |     |            |  |   |
|----|-----|------------|--|---|
| 34 | N/A | 24-01-2023 | Former CEO Of Email Security Company Sentenced To Five Years In Prison   | <a href="https://www.justice.gov/usao-sdny/pr/former-ceo-email-security-company-sentenced-five-years-prison">https://www.justice.gov/usao-sdny/pr/former-ceo-email-security-company-sentenced-five-years-prison</a>   |
| 35 | N/A | 20-01-2023 | Former Operations And Marketing Director At Lifeway Credit Union Sentenced To Federal Prison                                   | <a href="https://www.justice.gov/usao-mdtn/pr/former-operations-and-marketing-director-lifeway-credit-union-sentenced-federal-prison">https://www.justice.gov/usao-mdtn/pr/former-operations-and-marketing-director-lifeway-credit-union-sentenced-federal-prison</a> |
| 36 | N/A | 20-01-2023 | Overland Park Woman Sentenced for Bank Fraud   | <a href="https://www.justice.gov/usao-ks/pr/overland-park-woman-sentenced-bank-fraud">https://www.justice.gov/usao-ks/pr/overland-park-woman-sentenced-bank-fraud</a>   |
| 37 | N/A | 20-01-2023 | Bank Employee Admits Role in Fraud Conspiracy  | <a href="https://www.justice.gov/usao-ri/pr/bank-employee-admits-role-fraud-conspiracy">https://www.justice.gov/usao-ri/pr/bank-employee-admits-role-fraud-conspiracy</a>   |
| 38 | N/A | 17-01-2023 | Military Contractor Pleads Guilty to Bid Rigging   | <a href="https://www.justice.gov/opa/pr/military-contractor-pleads-guilty-bid-rigging">https://www.justice.gov/opa/pr/military-contractor-pleads-guilty-bid-rigging</a>   |
| 39 | N/A | 17-01-2023 | Former CEO of Los Angeles-Based Anti-Poverty Nonprofit Agrees to Plead Guilty to Embezzling and Misusing Funds and Tax Offense | <a href="https://www.justice.gov/usao-cdca/pr/former-ceo-los-angeles-based-anti-poverty-nonprofit-agrees-plead-guilty-embezzling-and">https://www.justice.gov/usao-cdca/pr/former-ceo-los-angeles-based-anti-poverty-nonprofit-agrees-plead-guilty-embezzling-and</a> |
| 40 | N/A | 13-01-2023 | Former Payroll Manager for Chicago Museum Charged With Misappropriating More Than \$2 Million                                  | <a href="https://www.justice.gov/usao-ndil/pr/former-payroll-manager-chicago-museum-charged-misappropriating-more-2-million-0">https://www.justice.gov/usao-ndil/pr/former-payroll-manager-chicago-museum-charged-misappropriating-more-2-million-0</a>               |
| 41 | N/A | 12-01-2023 | Former Executive Director at Bedford Senior Living Center Sentenced to over 2  | <a href="https://www.justice.gov/usao-sdin/pr/former-executive-director-bedford">https://www.justice.gov/usao-sdin/pr/former-executive-director-bedford</a>   |

|    |     |            |   |   |
|----|-----|------------|---|---|
|    |     |            | Years in Federal Prison for Embezzling<br>Over \$419,000 Over Five Years  | <a href="#">senior-living-center-sentenced-over-2-years-federal</a>   |
| 42 | N/A | 11-01-2023 | Former Executive Director of Long Island Charity Sentenced to Over Two Years in Prison for Embezzlement                     | <a href="https://www.justice.gov/usao-edny/pr/former-executive-director-long-island-charity-sentenced-over-two-years-prison">https://www.justice.gov/usao-edny/pr/former-executive-director-long-island-charity-sentenced-over-two-years-prison</a>                   |
| 43 | N/A | 11-01-2023 | Meridian Women Indicted for Embezzling More Than \$1.7 Million From Black Canyon Irrigation District                        | <a href="https://www.justice.gov/usao-id/pr/meridian-women-indicted-embezzling-more-17-million-black-canyon-irrigation-district">https://www.justice.gov/usao-id/pr/meridian-women-indicted-embezzling-more-17-million-black-canyon-irrigation-district</a>           |
| 44 | N/A | 10-01-2023 | Windsor Resident Sentenced to 33 Months in Prison for Defrauding Employer and its Lender of More than \$700K                | <a href="https://www.justice.gov/usao-ct/pr/windsor-resident-sentenced-33-months-prison-defrauding-employer-and-its-lender-more-700k">https://www.justice.gov/usao-ct/pr/windsor-resident-sentenced-33-months-prison-defrauding-employer-and-its-lender-more-700k</a> |
| 45 | N/A | 09-01-2023 | Former University Official Pleads Guilty To Wire Fraud  | <a href="https://www.justice.gov/usao-mdfl/pr/former-university-official-pleads-guilty-wire-fraud">https://www.justice.gov/usao-mdfl/pr/former-university-official-pleads-guilty-wire-fraud</a>   |
| 46 | N/A | 06-01-2023 | Former Bank Manager in Orange County Pleads Guilty to Bank Fraud for Stealing \$1.2 Million from Elderly Customers' Account | <a href="https://www.justice.gov/usao-cdca/pr/former-bank-manager-orange-county-pleads-guilty-bank-fraud-stealing-12-million-elderly">https://www.justice.gov/usao-cdca/pr/former-bank-manager-orange-county-pleads-guilty-bank-fraud-stealing-12-million-elderly</a> |
| 47 | N/A | 05-01-2023 | Restaurant manager sentenced to prison for embezzling \$300,000 from employer   | <a href="https://www.justice.gov/usao-ndga/pr/restaurant-manager-sentenced-prison-embezzling-300000-employer">https://www.justice.gov/usao-ndga/pr/restaurant-manager-sentenced-prison-embezzling-300000-employer</a>   |

|    |         |                   |   |   |
|----|---------|-------------------|---|---|
| 48 | N/A     | 05-01-2023        | CFO of KC Company Sentenced for \$3 Million Embezzlement Scheme, Filing False Tax Returns                                   | <a href="https://www.justice.gov/usao-wdmo/pr/cfo-kc-company-sentenced-3-million-embezzlement-scheme-filing-false-tax-returns">https://www.justice.gov/usao-wdmo/pr/cfo-kc-company-sentenced-3-million-embezzlement-scheme-filing-false-tax-returns</a>           |
| 49 | N/A     | 04-01-2023        | Franklin County Woman Sentenced to Two More Years in Prison for Committing Pandemic Loan Fraud After \$727,000 Embezzlement | <a href="https://www.justice.gov/usao-edmo/pr/franklin-county-woman-sentenced-two-more-years-prison-committing-pandemic-loan-fraud">https://www.justice.gov/usao-edmo/pr/franklin-county-woman-sentenced-two-more-years-prison-committing-pandemic-loan-fraud</a> |
| 50 | 22-1410 | 29-12-2022        | Bookkeeper Pleads Guilty to Embezzling Over \$29 Million  | <a href="https://www.justice.gov/opa/pr/bookkeeper-pleads-guilty-embezzling-over-29-million">https://www.justice.gov/opa/pr/bookkeeper-pleads-guilty-embezzling-over-29-million</a>   |
| 51 | 22-1389 | 20-12-2022        | Two Biotech CEOs Charged in Securities Fraud Schemes  | <a href="https://www.justice.gov/opa/pr/two-biotech-ceos-charged-securities-fraud-schemes">https://www.justice.gov/opa/pr/two-biotech-ceos-charged-securities-fraud-schemes</a>   |
| 52 | 22-1388 | 19-12-2022        | Texas Accountant Pleads Guilty to Embezzling Funds from Employer and Filing False Tax Return                                | <a href="https://www.justice.gov/opa/pr/texas-accountant-pleads-guilty-embezzling-funds-employer-and-filing-false-tax-return">https://www.justice.gov/opa/pr/texas-accountant-pleads-guilty-embezzling-funds-employer-and-filing-false-tax-return</a>             |
| 53 | N/A     | 16-12-2022        | Former CEO of Subprime Auto Lender Indicted in \$54.5 Million Bank Fraud Scheme   | <a href="https://www.justice.gov/usao-ndil/pr/former-ceo-subprime-auto-lender-indicted-545-million-bank-fraud-scheme">https://www.justice.gov/usao-ndil/pr/former-ceo-subprime-auto-lender-indicted-545-million-bank-fraud-scheme</a>                             |
| 54 | N/A     | December 15, 2022 | Jack Vicars Sentenced To 27 Months For Embezzling Nearly \$350,000  | <a href="#">Eastern District of Tennessee   Jack Vicars Sentenced To 27 Months For Embezzling Nearly \$350,000   United States Department of Justice</a>  |

|    |         |                   |   |   |
|----|---------|-------------------|---|---|
| 55 | N/A     | December 15, 2022 | Long-Time Employee Of Local Construction Firm Sentenced To Prison For Embezzlement  | <a href="https://www.justice.gov/usao-mdfl/pr/long-time-employee-local-construction-firm-sentenced-prison-embezzlement">https://www.justice.gov/usao-mdfl/pr/long-time-employee-local-construction-firm-sentenced-prison-embezzlement</a>             |
| 56 | 22-1363 | 14-12-2022        | Maryland Security Guard Convicted of Tax Evasion  | <a href="https://www.justice.gov/opa/pr/maryland-security-guard-convicted-tax-evasion">https://www.justice.gov/opa/pr/maryland-security-guard-convicted-tax-evasion</a>   |
| 57 | N/A     | 14-12-2022        | Lab Owner Convicted in \$463 Million Genetic Testing Scheme to Defraud Medicare   | <a href="https://www.justice.gov/opa/pr/lab-owner-convicted-463-million-genetic-testing-scheme-defraud-medicare">https://www.justice.gov/opa/pr/lab-owner-convicted-463-million-genetic-testing-scheme-defraud-medicare</a>                           |
| 58 | N/A     | 14-12-2022        | Former Chief Financial Officer Faces Charges for Failing to Pay Over \$3.6M in Employee Tax Withholdings and for Pocketing \$130,000 from his Employer's Bank Account | <a href="https://www.justice.gov/usao-ndok/pr/former-chief-financial-officer-faces-charges-failing-pay-over-36m-employee-tax">https://www.justice.gov/usao-ndok/pr/former-chief-financial-officer-faces-charges-failing-pay-over-36m-employee-tax</a> |
| 59 | 22-1347 | 13-12-2022        | FTX Founder Indicted for Fraud, Money Laundering, and Campaign Finance Offenses   | <a href="https://www.justice.gov/opa/pr/ftx-founder-indicted-fraud-money-laundering-and-campaign-finance-offenses">https://www.justice.gov/opa/pr/ftx-founder-indicted-fraud-money-laundering-and-campaign-finance-offenses</a>                       |
| 60 | N/A     | December 12, 2022 | Cabell County Woman Pleads Guilty to Federal Fraud Crimes   | <a href="https://www.justice.gov/usao-sd-wv/pr/cabell-county-woman-pleads-guilty-to-federal-fraud-crimes">Southern District of West Virginia   Cabell County Woman Pleads Guilty to Federal Fraud Crimes   United States Department of Justice</a>    |
| 61 | N/A     | December 7, 2022  | Former President of Waterbury Credit Union Admits Embezzling \$250K   | <a href="https://www.justice.gov/usao-ct/pr/former-president-waterbury-credit-union-admits-embezzling-250k">https://www.justice.gov/usao-ct/pr/former-president-waterbury-credit-union-admits-embezzling-250k</a>                                     |

|    |     |                  |  |   |
|----|-----|------------------|--|---|
| 62 | N/A | December 7, 2022 | Former IT Director Charged with Fraud, Aggravated Identity Theft                                 | <a href="https://www.justice.gov/usao-ri/pr/former-it-director-charged-fraud-aggravated-identity-theft">https://www.justice.gov/usao-ri/pr/former-it-director-charged-fraud-aggravated-identity-theft</a>   |
| 63 | N/A | December 6, 2022 | Comerica Vault Manager Pleads Guilty to Embezzling At Least \$120,000                            | <a href="https://www.justice.gov/usao-ndtx/pr/comerica-vault-manager-pleads-guilty-embezzling-least-120000">https://www.justice.gov/usao-ndtx/pr/comerica-vault-manager-pleads-guilty-embezzling-least-120000</a>                                     |
| 64 | N/A | 02-12-2022       | Granby Man Sentenced to Prison for Embezzling from Employer                                      | <a href="https://www.justice.gov/usao-ct/pr/granby-man-sentenced-prison-embezzling-employer">https://www.justice.gov/usao-ct/pr/granby-man-sentenced-prison-embezzling-employer</a>   |
| 65 | N/A | 01-12-2022       | Seattle woman who embezzled more than \$2.1 million from health club chain sentenced to prison   | <a href="https://www.justice.gov/usao-wdwa/pr/seattle-woman-who-embezzled-more-21-million-health-club-chain-sentenced-prison">https://www.justice.gov/usao-wdwa/pr/seattle-woman-who-embezzled-more-21-million-health-club-chain-sentenced-prison</a> |
| 66 | N/A | 28-11-2022       | Former CEO Of Iconix Brand Group Convicted At Trial Of Accounting Fraud                          | <a href="https://www.justice.gov/usao-sdny/pr/former-ceo-iconix-brand-group-convicted-trial-accounting-fraud">https://www.justice.gov/usao-sdny/pr/former-ceo-iconix-brand-group-convicted-trial-accounting-fraud</a>                                 |
| 67 | N/A | 22-11-2022       | Belgrade woman sentenced to 16 months in prison for embezzling more than \$800,000 from employer | <a href="https://www.justice.gov/usao-mt/pr/belgrade-woman-sentenced-16-months-prison-embezzling-more-800000-employer">https://www.justice.gov/usao-mt/pr/belgrade-woman-sentenced-16-months-prison-embezzling-more-800000-employer</a>               |
| 68 | N/A | 22-11-2022       | Festus Man Sentenced to 33 Months in Prison for Embezzling \$854,000                             | <a href="https://www.justice.gov/usao-edmo/pr/festus-man-sentenced-33-months-prison-embezzling-854000">https://www.justice.gov/usao-edmo/pr/festus-man-sentenced-33-months-prison-embezzling-854000</a>   |

|    |     |            |   |   |
|----|-----|------------|---|---|
| 69 | N/A | 18-11-2022 | Daycare CEO Pleads Guilty to Financial Fraud Schemes  | <a href="https://www.justice.gov/usao-mdga/pr/daycare-ceo-pleads-guilty-financial-fraud-schemes">https://www.justice.gov/usao-mdga/pr/daycare-ceo-pleads-guilty-financial-fraud-schemes</a>   |
| 70 | N/A | 17-11-2022 | VA Employees Plead Guilty in \$2.9 Million Embezzlement Scheme  | <a href="https://www.justice.gov/usao-ndtx/pr/va-employees-plead-guilty-29-million-embezzlement-scheme">https://www.justice.gov/usao-ndtx/pr/va-employees-plead-guilty-29-million-embezzlement-scheme</a>   |
| 71 | N/A | 15-11-2022 | Kansas Businessman Sentenced to Prison for Falsifying Records   | <a href="#">Kansas Businessman Sentenced to Prison for Falsifying Records   USAO-KS   Department of Justice</a>   |
| 72 | N/A | 14-11-2022 | Former Auditor at Newport Beach Commercial Real Estate Agency Arrested on Complaint Alleging He Stole \$2.5 Million from Employer | <a href="#">Central District of California   Former Auditor at Newport Beach Commercial Real Estate Agency Arrested on Complaint Alleging He Stole \$2.5 Million from Employer   United States Department of Justice</a>  |
| 73 | N/A | 07-11-2022 | Pennsylvania man defrauds Morgantown business of \$3.5 million  | <a href="https://www.justice.gov/usao-ndwv/pr/pennsylvania-man-defrauds-morgantown-business-35-million">https://www.justice.gov/usao-ndwv/pr/pennsylvania-man-defrauds-morgantown-business-35-million</a>   |
| 74 | N/A | 07-11-2022 | Former bank teller sentenced for taking nearly \$100,000 from bank  | <a href="https://www.justice.gov/usao-ndwv/pr/former-bank-teller-sentenced-taking-nearly-100000-bank">https://www.justice.gov/usao-ndwv/pr/former-bank-teller-sentenced-taking-nearly-100000-bank</a>   |
| 75 | N/A | 03-11-2022 | Taylorsville, N.C. Woman Is Sentenced To Eight Years In Prison For Embezzling More Than \$15 Million From Former Employer         | <a href="https://www.justice.gov/usao-wdnc/pr/taylorsville-nc-woman-sentenced-eight-years-prison-embezzling-more-15-million-former">https://www.justice.gov/usao-wdnc/pr/taylorsville-nc-woman-sentenced-eight-years-prison-embezzling-more-15-million-former</a> |



|    |         |            |   |   |
|----|---------|------------|---|---|
| 76 | N/A     | 03-11-2022 | Founder Of Cyberfraud Prevention Company Sentenced To Five Years In Prison For Defrauding Investors Out Of Over \$100 Million | <a href="https://www.justice.gov/usao-sdny/pr/founder-cyberfraud-prevention-company-sentenced-five-years-prison-defrauding-investors">https://www.justice.gov/usao-sdny/pr/founder-cyberfraud-prevention-company-sentenced-five-years-prison-defrauding-investors</a> |
| 77 | 22-1185 | 02-11-2022 | Former Georgia County Commissioner Convicted of Extortion   | <a href="https://www.justice.gov/opa/pr/former-georgia-county-commissioner-convicted-extortion">https://www.justice.gov/opa/pr/former-georgia-county-commissioner-convicted-extortion</a>   |
| 78 | N/A     | 02-11-2022 | Berwick Bank Officer Sentenced To 12 Months' Imprisonment   | <a href="https://www.justice.gov/usao-mdpa/pr/berwick-bank-officer-sentenced-12-months-imprisonment">https://www.justice.gov/usao-mdpa/pr/berwick-bank-officer-sentenced-12-months-imprisonment</a>   |
| 79 | N/A     | 01-11-2022 | Bethany Woman Pleads Guilty to Embezzling More Than \$850,000 From Former Employer  | <a href="https://www.justice.gov/usao-wdok/pr/bethany-woman-pleads-guilty-embezzling-more-850000-former-employer">https://www.justice.gov/usao-wdok/pr/bethany-woman-pleads-guilty-embezzling-more-850000-former-employer</a>   |
| 80 | 22-1160 | 27-10-2022 | Two Former Directors of Public Works Sentenced for Accepting Bribes   | <a href="https://www.justice.gov/opa/pr/two-former-directors-public-works-sentenced-accepting-bribes">https://www.justice.gov/opa/pr/two-former-directors-public-works-sentenced-accepting-bribes</a>   |
| 81 | N/A     | 27-10-2022 | Former Charter School Board President Sentenced to 40 Months in Prison for Embezzlement and Wire Fraud                        | <a href="https://www.justice.gov/usao-sdfl/pr/former-charter-school-board-president-sentenced-40-months-prison-embezzlement-and-wire">https://www.justice.gov/usao-sdfl/pr/former-charter-school-board-president-sentenced-40-months-prison-embezzlement-and-wire</a> |
| 82 | N/A     | 26-10-2022 | Danville Woman Sentenced For Embezzling More Than \$66,000 From Saint Anselm College  | <a href="https://www.justice.gov/usao-nh/pr/danville-woman-sentenced-embezzling-more-66000-saint-anselm-college">https://www.justice.gov/usao-nh/pr/danville-woman-sentenced-embezzling-more-66000-saint-anselm-college</a>   |

|    |         |            |   |   |
|----|---------|------------|---|---|
| 83 | 22-1147 | 25-10-2022 | CEO and President of Hawaii Shipbuilding Company Charged with Securities Fraud                  | <a href="https://www.justice.gov/opa/pr/ceo-and-president-hawaii-shipbuilding-company-charged-securities-fraud">https://www.justice.gov/opa/pr/ceo-and-president-hawaii-shipbuilding-company-charged-securities-fraud</a>   |
| 84 | N/A     | 24-10-2022 | Pittsburgh Woman Embezzled from Two Area Employers  | <a href="https://www.justice.gov/usao-wdpa/pr/pittsburgh-woman-embezzled-two-area-employers">https://www.justice.gov/usao-wdpa/pr/pittsburgh-woman-embezzled-two-area-employers</a>   |
| 85 | N/A     | 24-10-2022 | Husband And Wife Are Sentenced To Prison For Stealing \$200,000 From A High School Booster Club | <a href="https://www.justice.gov/usao-wdnc/pr/husband-and-wife-are-sentenced-prison-stealing-200000-high-school-booster-club">https://www.justice.gov/usao-wdnc/pr/husband-and-wife-are-sentenced-prison-stealing-200000-high-school-booster-club</a>             |
| 86 | N/A     | 20-10-2022 | Southern Ohio woman admits to embezzling \$700k from employer                                   | <a href="https://www.justice.gov/usao-sdoh/pr/southern-ohio-woman-admits-embezzling-700k-employer">https://www.justice.gov/usao-sdoh/pr/southern-ohio-woman-admits-embezzling-700k-employer</a>   |
| 87 | N/A     | 19-10-2022 | California Man Pleads Guilty to Defrauding His Massachusetts Employer Over a 16-Year Period     | <a href="https://www.justice.gov/usao-ma/pr/california-man-pleads-guilty-defrauding-his-massachusetts-employer-over-16-year-period">https://www.justice.gov/usao-ma/pr/california-man-pleads-guilty-defrauding-his-massachusetts-employer-over-16-year-period</a> |
| 88 | N/A     | 17-10-2022 | Burlington County, NJ, Bookkeeper Charged With Stealing From Former Employer                    | <a href="https://www.justice.gov/usao-edpa/pr/burlington-county-nj-bookkeeper-charged-stealing-former-employer-0">https://www.justice.gov/usao-edpa/pr/burlington-county-nj-bookkeeper-charged-stealing-former-employer-0</a>                                     |
| 89 | N/A     | 13-10-2022 | Beverly Farms Man Indicted for Multi-Million-Dollar Payroll Scheme                              | <a href="https://www.justice.gov/usao-ma/pr/beverly-farms-man-indicted-multi-million-dollar-payroll-scheme">https://www.justice.gov/usao-ma/pr/beverly-farms-man-indicted-multi-million-dollar-payroll-scheme</a>   |

|    |     |                  |  |   |
|----|-----|------------------|--|---|
| 90 | N/A | 13-10-2022       | Former Yale Med School Employee Who Stole \$40 Million in Electronics Sentenced to 9 Years in Prison   | <a href="https://www.justice.gov/usao-ct/pr/former-yale-med-school-employee-who-stole-40-million-electronics-sentenced-9-years-prison">https://www.justice.gov/usao-ct/pr/former-yale-med-school-employee-who-stole-40-million-electronics-sentenced-9-years-prison</a> |
| 91 | N/A | October 12, 2022 | Albert Lea Bookkeeper Pleads Guilty to Embezzling More Than \$200,000 in Public Housing Rent Payments  | <a href="https://www.justice.gov/usao-mn/pr/albert-lea-bookkeeper-pleads-guilty-embezzling-more-200000-public-housing-rent-payments">https://www.justice.gov/usao-mn/pr/albert-lea-bookkeeper-pleads-guilty-embezzling-more-200000-public-housing-rent-payments</a>     |
| 92 | N/A | 11-10-2022       | Former Financial Controller Sentenced to Three Years in Prison for Embezzling Over \$1.8 Million From Montgomery County Multinational Technology Company | <a href="https://www.justice.gov/usao-edpa/pr/former-financial-controller-sentenced-three-years-prison-embezzling-over-18-million">https://www.justice.gov/usao-edpa/pr/former-financial-controller-sentenced-three-years-prison-embezzling-over-18-million</a>         |
| 93 | N/A | 11-10-2022       | Anderson Community School Corporation Bookkeeper Charged with Embezzling nearly \$1 Million Over More than Five Years                                    | <a href="https://www.justice.gov/usao-sdin/pr/anderson-community-school-corporation-bookkeeper-charged-embezzling-nearly-1-million">https://www.justice.gov/usao-sdin/pr/anderson-community-school-corporation-bookkeeper-charged-embezzling-nearly-1-million</a>       |
| 94 | N/A | 11-10-2022       | Chicopee Company Controller Sentenced for Stealing \$1.4 Million from Company Finances   | <a href="https://www.justice.gov/usao-ma/pr/chicopee-company-controller-sentenced-stealing-14-million-company-finances">https://www.justice.gov/usao-ma/pr/chicopee-company-controller-sentenced-stealing-14-million-company-finances</a>                               |
| 95 | N/A | 07-10-2022       | Florida Man Charged with Wire Fraud Scheme to Defraud Former Employer in New Jersey  | <a href="https://www.justice.gov/usao-nj/pr/florida-man-charged-wire-fraud-scheme-defraud-former-employer-new-jersey">https://www.justice.gov/usao-nj/pr/florida-man-charged-wire-fraud-scheme-defraud-former-employer-new-jersey</a>                                   |

|     |     |            |  |   |
|-----|-----|------------|--|---|
| 96  | N/A | 06-10-2022 | Aldie Man Pleads Guilty to Multi-Million Dollar Embezzlement Scheme                                    | <a href="https://www.justice.gov/usao-edva/pr/aldie-man-pleads-guilty-multi-million-dollar-embezzlement-scheme">https://www.justice.gov/usao-edva/pr/aldie-man-pleads-guilty-multi-million-dollar-embezzlement-scheme</a>   |
| 97  | N/A | 06-10-2022 | Ralls County Woman Admits Embezzling \$1.2 million   | <a href="https://www.justice.gov/usao-edmo/pr/ralls-county-woman-admits-embezzling-12-million">https://www.justice.gov/usao-edmo/pr/ralls-county-woman-admits-embezzling-12-million</a>   |
| 98  | N/A | 30-09-2022 | CPAP Clinic Employees Found Guilty of Embezzling from Employer   | <a href="https://www.justice.gov/usao-mn/pr/cpap-clinic-employees-found-guilty-embezzling-employer">https://www.justice.gov/usao-mn/pr/cpap-clinic-employees-found-guilty-embezzling-employer</a>   |
| 99  | N/A | 30-09-2022 | Florida Woman Charged With Embezzling \$2 Million From Former Employer                                 | <a href="https://www.justice.gov/usao-mdpa/pr/florida-woman-charged-embezzling-2-million-former-employer">https://www.justice.gov/usao-mdpa/pr/florida-woman-charged-embezzling-2-million-former-employer</a>   |
| 100 | N/A | 28-09-2022 | Former Cargill Employee Is Sentenced To More Than Four Years In Prison For Bribery And Kickback Scheme | <a href="https://www.justice.gov/usao-wdnc/pr/former-cargill-employee-sentenced-more-four-years-prison-bribery-and-kickback-scheme">https://www.justice.gov/usao-wdnc/pr/former-cargill-employee-sentenced-more-four-years-prison-bribery-and-kickback-scheme</a> |
| 101 | N/A | 28-09-2022 | Former Financial Advisor Agrees to Plead Guilty to Aggravated Identity Theft                           | <a href="https://www.justice.gov/usao-edca/pr/former-financial-advisor-agrees-plead-guilty-aggravated-identity-theft">https://www.justice.gov/usao-edca/pr/former-financial-advisor-agrees-plead-guilty-aggravated-identity-theft</a>                             |
| 102 | N/A | 23-09-2022 | Financial Officer Sentenced to Nearly Three Years for Defrauding Sumter County Non-Profit              | <a href="https://www.justice.gov/usao-sc/pr/financial-officer-sentenced-nearly-three-years-defrauding-sumter-county-non-profit">https://www.justice.gov/usao-sc/pr/financial-officer-sentenced-nearly-three-years-defrauding-sumter-county-non-profit</a>         |

|     |     |            |   |   |
|-----|-----|------------|---|---|
| 103 | N/A | 21-09-2022 | Former manager of Prairie View Federal Credit Union indicted on embezzlement charges  | <a href="https://www.justice.gov/usao-sdtx/pr/former-manager-prairie-view-federal-credit-union-indicted-embezzlement-charges">https://www.justice.gov/usao-sdtx/pr/former-manager-prairie-view-federal-credit-union-indicted-embezzlement-charges</a>             |
| 104 | N/A | 20-09-2022 | Engineer Stole Trade Secrets Before His Departure from Broadcom, Then Accessed and Referenced Trade Secrets While Working For PRC-Based Startup Company | <a href="https://www.justice.gov/usao-ndca/pr/former-broadcom-engineer-sentenced-eight-months-prison-theft-trade-secrets">https://www.justice.gov/usao-ndca/pr/former-broadcom-engineer-sentenced-eight-months-prison-theft-trade-secrets</a>                     |
| 105 | N/A | 20-09-2022 | Myrtle Beach Resort Manager Indicted for Fraud Scheme Totaling Nearly \$1 Million   | <a href="https://www.justice.gov/usao-sc/pr/myrtle-beach-resort-manager-indicted-fraud-scheme-totaling-nearly-1-million">https://www.justice.gov/usao-sc/pr/myrtle-beach-resort-manager-indicted-fraud-scheme-totaling-nearly-1-million</a>                       |
| 106 | N/A | 19-09-2022 | North Idaho Woman Sentenced for Embezzling over 3.6 Million Dollars in Wire Fraud Scheme  | <a href="https://www.justice.gov/usao-id/pr/north-idaho-woman-sentenced-embezzling-over-36-million-dollars-wire-fraud-scheme">https://www.justice.gov/usao-id/pr/north-idaho-woman-sentenced-embezzling-over-36-million-dollars-wire-fraud-scheme</a>             |
| 107 | N/A | 19-09-2022 | Littleton Woman Pleads Guilty to Bank Fraud   | <a href="https://www.justice.gov/usao-nh/pr/littleton-woman-pleads-guilty-bank-fraud">https://www.justice.gov/usao-nh/pr/littleton-woman-pleads-guilty-bank-fraud</a>   |
| 108 | N/A | 16-09-2022 | Former Director of Finance Sentenced to 44 Months in Prison for Defrauding Credit Union of More Than \$600,000  | <a href="https://www.justice.gov/usao-dc/pr/former-director-finance-sentenced-44-months-prison-defrauding-credit-union-more-600000">https://www.justice.gov/usao-dc/pr/former-director-finance-sentenced-44-months-prison-defrauding-credit-union-more-600000</a> |
| 109 | N/A | 15-09-2022 | Former Employee Admits Embezzling \$339,000 from St. Louis County Company   | <a href="https://www.justice.gov/usao-edmo/pr/former-employee-admits-embezzling-339000-st-louis-county-company">https://www.justice.gov/usao-edmo/pr/former-employee-admits-embezzling-339000-st-louis-county-company</a>   |

|     |     |            |  |   |
|-----|-----|------------|--|---|
| 110 | N/A | 09-09-2022 | Former New Pilgrim Federal Credit Union Manager Charged with Embezzlement                                    | <a href="https://www.justice.gov/usao-ndal/pr/former-new-pilgrim-federal-credit-union-manager-charged-embezzlement">https://www.justice.gov/usao-ndal/pr/former-new-pilgrim-federal-credit-union-manager-charged-embezzlement</a>                                       |
| 111 | N/A | 08-09-2022 | Maryland Woman Sentenced to Federal Prison for Fraud Schemes Resulting in Losses of More Than \$1.4 Million  | <a href="https://www.justice.gov/usao-md/pr/maryland-woman-sentenced-federal-prison-fraud-schemes-resulting-losses-more-14-million">https://www.justice.gov/usao-md/pr/maryland-woman-sentenced-federal-prison-fraud-schemes-resulting-losses-more-14-million</a>       |
| 112 | N/A | 06-09-2022 | Passaic County Woman Admits Embezzling over \$3.7 Million from Employer as Company's Chief Financial Officer | <a href="https://www.justice.gov/usao-nj/pr/passaic-county-woman-admits-embezzling-over-37-million-employer-company-s-chief-financial">https://www.justice.gov/usao-nj/pr/passaic-county-woman-admits-embezzling-over-37-million-employer-company-s-chief-financial</a> |
| 113 | N/A | 01-09-2022 | Accounting Specialist Charged with Embezzling more than \$270,000 from WFYI Public Media                     | <a href="https://www.justice.gov/usao-sdin/pr/accounting-specialist-charged-embezzling-more-270000-wfyi-public-media">https://www.justice.gov/usao-sdin/pr/accounting-specialist-charged-embezzling-more-270000-wfyi-public-media</a>                                   |
| 114 | N/A | 30-08-2022 | Shelbyville Woman Sentenced to 30 Months in Federal Prison for Embezzlement and Tax Fraud                    | <a href="https://www.justice.gov/usao-wdky/pr/shelbyville-woman-sentenced-30-months-federal-prison-embezzlement-and-tax-fraud">https://www.justice.gov/usao-wdky/pr/shelbyville-woman-sentenced-30-months-federal-prison-embezzlement-and-tax-fraud</a>                 |
| 115 | N/A | 26-08-2022 | Former Hillandale Farms Accountant Pleads Guilty in \$6.8 Million Embezzlement Scheme                        | <a href="https://www.justice.gov/usao-wdpa/pr/former-hillandale-farms-accountant-pleads-guilty-68-million-embezzlement-scheme">https://www.justice.gov/usao-wdpa/pr/former-hillandale-farms-accountant-pleads-guilty-68-million-embezzlement-scheme</a>                 |

|     |        |                 |  |   |
|-----|--------|-----------------|--|---|
| 116 | 22-877 | 16-08-2022      | Former Member of Congress Charged with Multiple Fraud Schemes  | <a href="https://www.justice.gov/opa/pr/former-member-congress-charged-multiple-fraud-schemes">https://www.justice.gov/opa/pr/former-member-congress-charged-multiple-fraud-schemes</a>   |
| 117 | N/A    | August 15, 2022 | Evansville Man Sentenced to 16 Months in Prison for Using his Accounting Position to Embezzle More than \$87,000 from his Gibson County Employer | <a href="https://www.justice.gov/usao-sdin/pr/evansville-man-sentenced-16-months-prison-using-his-accounting-position-embezzle-more">https://www.justice.gov/usao-sdin/pr/evansville-man-sentenced-16-months-prison-using-his-accounting-position-embezzle-more</a>   |
| 118 | 22-864 | 10-08-2022      | Former Twitter Employee Found Guilty of Acting as an Agent of a Foreign Government and Unlawfully Sharing Twitter User Information               | <a href="https://www.justice.gov/opa/pr/former-twitter-employee-found-guilty-acting-agent-foreign-government-and-unlawfully-sharing">https://www.justice.gov/opa/pr/former-twitter-employee-found-guilty-acting-agent-foreign-government-and-unlawfully-sharing</a>   |
| 119 | N/A    | July 8, 2022    | Former Employee of Mechanical Contractor Sentenced to Prison for Inflating Change Orders   | <a href="https://www.justice.gov/usao-ct/pr/former-employee-mechanical-contractor-sentenced-prison-inflating-change-orders">https://www.justice.gov/usao-ct/pr/former-employee-mechanical-contractor-sentenced-prison-inflating-change-orders</a>   |
| 120 | N/A    | June 30, 2022   | Apple's Former Director of Corporate Law Admits Insider Trading  | <a href="https://www.justice.gov/usao-nj/pr/apples-former-director-corporate-law-admits-insider-trading#:~:text=%E2%80%9CGene%20Levoff%20betrayed%20the%20trust.to%20line%20his%20own%20pockets.">https://www.justice.gov/usao-nj/pr/apples-former-director-corporate-law-admits-insider-trading#:~:text=%E2%80%9CGene%20Levoff%20betrayed%20the%20trust.to%20line%20his%20own%20pockets.</a> |
| 121 | 22-682 | 29-06-2022      | Owner of Technology Companies Arrested for Alleged \$45 Million Investment Fraud Scheme Involving Over 10,000 Victims                            | <a href="https://www.justice.gov/opa/pr/owner-technology-companies-arrested-alleged-45-million-investment-fraud-scheme-involving-over">https://www.justice.gov/opa/pr/owner-technology-companies-arrested-alleged-45-million-investment-fraud-scheme-involving-over</a>   |

|     |        |              |  |   |
|-----|--------|--------------|--|---|
| 122 | 22-665 | 24-06-2022   | Serial Fraudster Previously Extradited from Mexico Pleads Guilty to Multiple Investment Fraud Schemes  | <a href="https://www.justice.gov/opa/pr/serial-fraudster-previously-extradited-mexico-pleads-guilty-multiple-investment-fraud-schemes">https://www.justice.gov/opa/pr/serial-fraudster-previously-extradited-mexico-pleads-guilty-multiple-investment-fraud-schemes</a> |
| 123 | 22-631 | 14-06-2022   | Former EarthWater CFO and Others Plead Guilty to Fraud Charges Related to High-Yield Investment Scheme | <a href="https://www.justice.gov/opa/pr/former-earthwater-cfo-and-others-plead-guilty-fraud-charges-related-high-yield-investment">https://www.justice.gov/opa/pr/former-earthwater-cfo-and-others-plead-guilty-fraud-charges-related-high-yield-investment</a>         |
| 124 | 22-629 | 14-06-2022   | Former Chairman and Managing Partner of Energy Company Pleads Guilty to \$15 Million Ponzi Scheme      | <a href="https://www.justice.gov/opa/pr/former-chairman-and-managing-partner-energy-company-pleads-guilty-15-million-ponzi-scheme">https://www.justice.gov/opa/pr/former-chairman-and-managing-partner-energy-company-pleads-guilty-15-million-ponzi-scheme</a>         |
| 125 | N/A    | June 2, 2022 | Former Bank Employee Admits \$8 Million Fraud and Bribery Scheme                                       | <a href="https://www.justice.gov/usao-nj/pr/former-bank-employee-admits-8-million-fraud-and-bribery-scheme">https://www.justice.gov/usao-nj/pr/former-bank-employee-admits-8-million-fraud-and-bribery-scheme</a>   |
| 126 | 22-577 | 31-05-2022   | Former CEO Indicted for Misleading Investors about COVID-19 Rapid Test Kits                            | <a href="https://www.justice.gov/opa/pr/former-ceo-indicted-misleading-investors-about-covid-19-rapid-test-kits">https://www.justice.gov/opa/pr/former-ceo-indicted-misleading-investors-about-covid-19-rapid-test-kits</a>   |
| 127 | 22-115 | 10-02-2022   | California CEO Sentenced to Prison for Employment Tax Crimes   | <a href="https://www.justice.gov/opa/pr/california-ceo-sentenced-prison-employment-tax-crimes">https://www.justice.gov/opa/pr/california-ceo-sentenced-prison-employment-tax-crimes</a>   |
| 128 | 22-93  | 03-02-2022   | Former President of Energy Company Indicted for Commodities Insider Trading and Kickback Schemes       | <a href="https://www.justice.gov/opa/pr/former-president-energy-company-indicted-commodities-insider-trading-and-kickback-schemes">https://www.justice.gov/opa/pr/former-president-energy-company-indicted-commodities-insider-trading-and-kickback-schemes</a>         |



|     |         |              |   |   |
|-----|---------|--------------|---|---|
| 129 | 22-84   | 01-02-2022   | Woman Pleads Guilty to Misappropriating Funds for Care of COVID-19 Patients   | <a href="https://www.justice.gov/opa/pr/woman-pleads-guilty-misappropriating-funds-care-covid-19-patients">https://www.justice.gov/opa/pr/woman-pleads-guilty-misappropriating-funds-care-covid-19-patients</a>   |
| 130 | 21-1152 | 18-11-2021   | Four Executives Plead Guilty to Fraud Scheme that Caused Over \$4.5 Million in Losses to the Small Business Administration  | <a href="https://www.justice.gov/opa/pr/four-executives-plead-guilty-fraud-scheme-caused-over-45-million-losses-small-business">https://www.justice.gov/opa/pr/four-executives-plead-guilty-fraud-scheme-caused-over-45-million-losses-small-business</a>               |
| 131 | 21-1015 | 18-10-2021   | Former Security Services Executives Plead Guilty to Rigging Bids for Department of Defense Security Contracts   | <a href="https://www.justice.gov/opa/pr/former-security-services-executives-plead-guilty-rigging-bids-department-defense-security">https://www.justice.gov/opa/pr/former-security-services-executives-plead-guilty-rigging-bids-department-defense-security</a>         |
| 132 | 21-761  | 10-08-2021   | Telemedicine Company Owner Charged in Superseding Indictment for \$784 Million Health Care Fraud, Illegal Kickback and Tax Evasion Scheme                                 | <a href="https://www.justice.gov/opa/pr/telemedicine-company-owner-charged-superseding-indictment-784-million-health-care-fraud">https://www.justice.gov/opa/pr/telemedicine-company-owner-charged-superseding-indictment-784-million-health-care-fraud</a>             |
| 133 | 21-735  | 04-08-2021   | Executive Arrested and Charged for Bribery and Money-Laundering Scheme  | <a href="https://www.justice.gov/opa/pr/executive-arrested-and-charged-bribery-and-money-laundering-scheme">https://www.justice.gov/opa/pr/executive-arrested-and-charged-bribery-and-money-laundering-scheme</a>   |
| 134 | N/A     | June 4, 2021 | Former Northeast Missouri City Clerk pleads guilty to stealing city money   | <a href="https://www.justice.gov/usao-edmo/pr/former-northeast-missouri-city-clerk-pleads-guilty-stealing-city-money">https://www.justice.gov/usao-edmo/pr/former-northeast-missouri-city-clerk-pleads-guilty-stealing-city-money</a>                                   |
| 135 | 21-485  | 25-05-2021   | Two Bank Executives Charged for Conspiring to Launder Hundreds of Millions of Dollars Through U.S. Financial System in Connection with Odebrecht Bribery and Fraud Scheme | <a href="https://www.justice.gov/opa/pr/two-bank-executives-charged-conspiring-launder-hundreds-millions-dollars-through-us-financial">https://www.justice.gov/opa/pr/two-bank-executives-charged-conspiring-launder-hundreds-millions-dollars-through-us-financial</a> |

|     |        |                |   |  |
|-----|--------|----------------|---|--|
| 136 | 21-481 | 24-05-2021     | Former NGO Procurement Official Sentenced to Prison for Bribery                                       | <a href="https://www.justice.gov/opa/pr/former-ngo-procurement-official-sentenced-prison-bribery">https://www.justice.gov/opa/pr/former-ngo-procurement-official-sentenced-prison-bribery</a>  |
| 137 | 21-463 | 20-05-2021     | Managing Director and Two Former Loan Officers Plead Guilty for Roles in Widespread Bank-Fraud Scheme | <a href="https://www.justice.gov/opa/pr/former-managing-director-and-two-former-loan-officers-plead-guilty-roles-widespread-bank">https://www.justice.gov/opa/pr/former-managing-director-and-two-former-loan-officers-plead-guilty-roles-widespread-bank</a>  |
| 138 | 21-422 | 07-05-2021     | Deputy Campaign Manager Pleads Guilty to Theft of Campaign Funds                                      | <a href="https://www.justice.gov/opa/pr/former-deputy-campaign-manager-pleads-guilty-theft-campaign-funds">https://www.justice.gov/opa/pr/former-deputy-campaign-manager-pleads-guilty-theft-campaign-funds</a>  |
| 139 | N/A    | April 30, 2021 | North Andover Woman Sentenced for Embezzling Employer's Outgoing Vendor Payments                      | <a href="https://www.justice.gov/opa/pr/district-of-massachusetts-north-andover-woman-sentenced-for-embezzling-employer-s-outgoing-vendor-payments">District of Massachusetts   North Andover Woman Sentenced for Embezzling Employer's Outgoing Vendor Payments   United States Department of Justice</a> |
| 140 | 21-351 | 21-04-2021     | Mathematics Professor and University Researcher Indicted for Grant Fraud                              | <a href="https://www.justice.gov/opa/pr/mathematics-professor-and-university-researcher-indicted-grant-fraud">https://www.justice.gov/opa/pr/mathematics-professor-and-university-researcher-indicted-grant-fraud</a>  |
| 141 | 21-329 | 14-04-2021     | Patient Recruiter Sentenced to Prison for \$3.3 Million Cancer Genetic Testing Fraud Scheme           | <a href="https://www.justice.gov/opa/pr/patient-recruiter-sentenced-prison-33-million-cancer-genetic-testing-fraud-scheme">https://www.justice.gov/opa/pr/patient-recruiter-sentenced-prison-33-million-cancer-genetic-testing-fraud-scheme</a>  |
| 142 | 21-303 | 06-04-2021     | Arkansas Businessman Sentenced to Prison for Income Tax Evasion                                       | <a href="https://www.justice.gov/opa/pr/arkansas-businessman-sentenced-prison-income-tax-evasion">https://www.justice.gov/opa/pr/arkansas-businessman-sentenced-prison-income-tax-evasion</a>  |

|     |        |                   |   |   |
|-----|--------|-------------------|---|---|
| 143 | 21-268 | 25-03-2021        | Former Oil Trader Pleads Guilty to Commodities Price Manipulation Conspiracy  | <a href="https://www.justice.gov/opa/pr/former-oil-trader-pleads-guilty-commodities-price-manipulation-conspiracy">https://www.justice.gov/opa/pr/former-oil-trader-pleads-guilty-commodities-price-manipulation-conspiracy</a>                                     |
| 144 | 21-259 | 23-03-2021        | Former Ecuadorian Government Official Sentenced to Prison for Role in Bribery and Money Laundering Scheme             | <a href="https://www.justice.gov/opa/pr/former-ecuadorian-government-official-sentenced-prison-role-bribery-and-money-laundering">https://www.justice.gov/opa/pr/former-ecuadorian-government-official-sentenced-prison-role-bribery-and-money-laundering</a>       |
| 145 | 21-235 | 17-03-2021        | Pharmacist Charged in \$4 Million Health Care Fraud and Kickback Scheme   | <a href="https://www.justice.gov/opa/pr/pharmacist-charged-4-million-health-care-fraud-and-kickback-scheme">https://www.justice.gov/opa/pr/pharmacist-charged-4-million-health-care-fraud-and-kickback-scheme</a>   |
| 146 | 21-196 | 03-03-2021        | CEO Sentenced to Prison in \$150 Million Health Care Fraud, Opioid Distribution, and Money Laundering Scheme          | <a href="https://www.justice.gov/opa/pr/ceo-sentenced-prison-150-million-health-care-fraud-opioid-distribution-and-money-laundering">https://www.justice.gov/opa/pr/ceo-sentenced-prison-150-million-health-care-fraud-opioid-distribution-and-money-laundering</a> |
| 147 | 21-47  | 13-01-2021        | Restaurant Chain Manager Pleads Guilty to Employment Tax Fraud  | <a href="https://www.justice.gov/opa/pr/restaurant-chain-manager-pleads-guilty-employment-tax-fraud">https://www.justice.gov/opa/pr/restaurant-chain-manager-pleads-guilty-employment-tax-fraud</a>   |
| 148 | N/A    | February 24, 2020 | Accounts Payable Clerk Indicted for Fraud   | <a href="https://www.justice.gov/usao-ri/pr/accounts-payable-clerk-indicted-fraud">https://www.justice.gov/usao-ri/pr/accounts-payable-clerk-indicted-fraud</a>   |
| 149 | N/A    | January 9, 2020   | Two Former Employees of Montgomery Doctor Receive Prison Sentences for Unlawful Distribution of Controlled Substances | <a href="#">Middle District of Alabama   Two Former Employees of Montgomery Doctor Receive Prison Sentences for Unlawful Distribution of Controlled Substances   United States Department of Justice</a>  |

|     |        |                   |   |   |
|-----|--------|-------------------|---|---|
| 150 | N/A    | June 21, 2019     | Employee at Mortgage Company Admits Illegally Accessing Computer to Steal \$2 Million   | <a href="https://www.justice.gov/usao-nj/pr/employee-mortgage-company-admits-illegally-accessing-computer-steal-2-million-0">https://www.justice.gov/usao-nj/pr/employee-mortgage-company-admits-illegally-accessing-computer-steal-2-million-0</a>             |
| 151 | 19-316 | April 3, 2019     | Former Chief Financial Officer at Publicly Traded Transportation Company Charged with \$245 Million Securities and Accounting Fraud Scheme; Two Other Defendants Previously Indicted Charged with Additional Offenses | <a href="https://www.justice.gov/opa/pr/former-chief-financial-officer-publicly-traded-transportation-company-charged-245-million">https://www.justice.gov/opa/pr/former-chief-financial-officer-publicly-traded-transportation-company-charged-245-million</a> |
| 152 | N/A    | March 15, 2018    | Former Nashville Judge Indicted on Additional Federal Obstruction and Theft Charges   | <a href="#">Office of Public Affairs   Former Nashville Judge Indicted on Additional Federal Obstruction and Theft Charges   United States Department of Justice</a>  |
| 153 | N/A    | February 28, 2018 | Deloitte & Touché Agrees to Pay \$149.5 Million to Settle Claims Arising From Its Audits of Failed Mortgage Lender Taylor, Bean & Whitaker  | <a href="https://www.justice.gov/opa/pr/deloitte-touche-agrees-pay-1495-million-settle-claims-arising-its-audits-failed-mortgage">https://www.justice.gov/opa/pr/deloitte-touche-agrees-pay-1495-million-settle-claims-arising-its-audits-failed-mortgage</a>   |
| 154 | N/A    | February 14, 2018 | Law Office Manager Forged and Cashed Firm Checks for Personal Use   | <a href="https://www.justice.gov/usao-wdpa/pr/law-office-manager-forged-and-cashed-firm-checks-personal-use">https://www.justice.gov/usao-wdpa/pr/law-office-manager-forged-and-cashed-firm-checks-personal-use</a>   |
| 155 | N/A    | August 17, 2016   | Accountant Sentenced for \$4 Million Embezzlement Scheme  | <a href="https://www.justice.gov/usao-wdmo/pr/accountant-sentenced-4-million-embezzlement-scheme">https://www.justice.gov/usao-wdmo/pr/accountant-sentenced-4-million-embezzlement-scheme</a>   |

|     |        |                          |   |   |
|-----|--------|--------------------------|---|---|
| 156 | 16-160 | June 9,<br>2016          | Former Dea Supervisor And Employee<br>Convicted Of Making False Statements In<br>National Security Forms          | <a href="https://www.justice.gov/usao-sdny/pr/former-dea-supervisor-and-employee-convicted-making-false-statements-national-security">https://www.justice.gov/usao-sdny/pr/former-dea-supervisor-and-employee-convicted-making-false-statements-national-security</a> |
| 157 | N/A    | Novemb<br>er 25,<br>2002 | U.S. announces what is believed the largest<br>Identity Theft case in American history;<br>losses are in millions | <a href="https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/cummingsIndict.htm">https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/cummingsIndict.htm</a>   |

APPENDIX B  
INTERVIEW GUIDE

**Part 1 - Introduction**

- Thank you for agreeing to participate in this interview. Your expertise in fraud is invaluable to our research.
- The purpose of this interview is to gather insights from your experience and knowledge regarding fraud cases you have studied.
- Your input will greatly contribute to our understanding of fraudulent acts, their motivations, prevention, detection, and potential theoretical advancements in fraud management.

**Part 2 - Participant Information**

1. Name:
2. Position/Title:
3. Affiliation/Organization:
4. Years of experience in fraud examination:

**Part 3 - Case Study Background:**

1. How many cases were you assigned to study?
2. Can you briefly describe the types of fraudulent acts observed in these cases?
3. What were the main reasons or motivations behind the occurrence of fraud in these cases?
4. In your opinion, what factors contributed to the success of these fraudulent acts?
5. How do you think these fraudulent activities could have been prevented and detected earlier?

**Part 4 -Integration with Existing Fraud Theories:**

1. How do existing fraud theories explain or relate to the fraudulent acts observed in the cases you studied?
2. Are there any specific fraud elements outlined in existing theories that you found particularly relevant to these cases?
3. Do you perceive any gaps in existing fraud theories when applied to real-world cases? If so, what are they?

**Part 5 - Conceptualizing a New Fraud Model:**

1. If we were to develop a new model for preventing and detecting employee fraud based on the cases you've studied, what key components or principles do you think should be included?
2. Are there any specific strategies or techniques you believe would be effective in mitigating the risk of employee fraud?
3. How would this new model differ from or build upon existing fraud prevention and detection frameworks?

**Part 6 - Organizational Strategies to Minimize Employee Fraud:**

1. From your experience, what organizational policies or practices have proven effective in deterring employee fraud?
2. How important is the role of corporate culture in preventing fraud within an organization?
3. Are there any specific internal controls or oversight mechanisms that you would recommend implementing to minimize the risk of employee fraud?

**Part 7 - Additional Questions (Optional):**

1. Is there any additional information or insights you would like to share regarding the cases you've studied or fraud in general?
2. Are there any emerging trends or challenges in the field of fraud examination that you believe are important to consider?

**Part 8 - Closing:**

- Thank you once again for your valuable input and expertise. Your insights will be instrumental in advancing our understanding of fraud management.
- If you have any further comments or questions, please feel free to share them at this time.



## APPENDIX C:

### ANALYSIS OF FRAUDULENT ACTS

| Case | Analysis Data  |
|------|--|
| 1    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This applies due to the false and misleading statements made to entice investors to purchase the ICO, including falsifying aspects of TBIS’s white papers and making unfounded claims about business relationships and the ICO's profitability prospects. |
|      | Identity Theft, Data Breach and Impersonation: Although not involving traditional identity theft, the creation of fake client testimonials and the false claims of business relationships with reputable entities mimic aspects of impersonation by adopting false identities to create legitimacy.                              |
|      | Money Laundering: The commingling of ICO investors' funds with personal funds and using the proceeds for expenses unrelated to the stated purposes of TBIS suggests elements of money laundering, where the origins of fraudulently obtained money are obscured.   |
|      | Regulatory Evasion and Deception: Stollery’s failure to register the ICO with the U.S. Securities and Exchange Commission (SEC) or to secure a valid exemption constitutes evasion of regulatory requirements and deception of regulatory authorities.   |
| 2    | Bribery and Corruption: Pérez-Otero accepted cash bribes in exchange for favoring a construction company in contract awards and payment processes.   |
|      | Collusion and Conspiracy: Pérez-Otero and the construction company owner conspired to ensure the company received and retained contracts, highlighting their collaboration to commit fraud.  |
| 3    | Asset Misappropriation: Firlle misappropriated over \$1.9 million from the company by using company funds for personal expenses, issuing unauthorized checks to himself, making unauthorized wire transfers, and withdrawing funds without authorization.  |
|      | Fraudulent Claims and Invoices: The use of company credit cards for personal expenses and the issuance of excess bonus payments can be considered under this category as they involve making fraudulent claims for personal benefit.   |
|      | Forgery and Counterfeiting: Issuing unauthorized company checks to himself might involve forgery, especially if it required falsifying signatures or altering check amounts.   |
|      | Manipulation of Company Systems: Firlle's actions to carry out unauthorized transactions, including wire transfers and withdrawals, indicate manipulation of the company's financial systems.  |
|      | Payroll Fraud: Issuing himself excess bonus payments falls directly under payroll fraud, where an employee manipulates the payroll system to receive unearned compensation.  |
| 4    | Asset Misappropriation: Murray misappropriated funds from her employer's bank account, which is a direct example of stealing or misusing the organization's resources.   |

|   |   |
|---|---|
|   | <p>Fraudulent Claims and Invoices: She fabricated recipients and invoice numbers to conceal the embezzlement, which fits the criteria for making fraudulent claims to justify the unauthorized transactions.</p> <p>Forgery and Counterfeiting: The act of fabricating invoice numbers and recipients for the wire transactions can be considered a form of forgery, as she created false documents to support her theft.</p> <p>Manipulation of Company Systems: By altering the employer's general ledger to hide her theft, Murray manipulated company systems to her advantage.</p>   |
| 5 | <p>Asset Misappropriation: Since the scheme involved diverting business and causing financial loss to Raeford Farms through the misuse of company assets (chicken frames), this action is directly applicable.</p> <p>Collusion and Conspiracy: Hickman and Whiteman conspired together to conceal their fraudulent activities from Raeford Farms, fitting the definition of collusion and conspiracy.</p> <p>Fraudulent Claims and Invoices: The use of invoices to facilitate payments for transactions that were part of a fraudulent scheme fits this category.</p> <p>Procurement and Vendor Fraud: The scheme involved manipulating the procurement process and vendor relationships to defraud Raeford Farms.</p>  |
| 6 | <p>Asset Misappropriation: This involves the theft or misuse of an organization's assets, and in this case, Madonna Peterson is accused of stealing more than \$100,000 from her employer, which directly aligns with the definition of asset misappropriation.</p>   |
| 7 | <p>Asset Misappropriation: Arnold misused his position to steal money from the charter schools for personal expenses, which directly falls under the misuse or theft of company's assets.</p> <p>Fraudulent Claims and Invoices: The creation of false invoices, bills, and credit card statements to claim expenses that were not actually incurred by the schools.</p> <p>Manipulation of Company Systems: Arnold created false computer journal entries, which indicates manipulation of the schools' financial systems to facilitate his fraudulent activities.</p> <p>Procurement and Vendor Fraud: By generating payments to credit cards he controlled under the guise of paying for school supplies and other expenses, Arnold engaged in procurement fraud.</p> <p>Money Laundering: Passing fraudulently obtained money through Venmo and a bank account in the name of a business Arnold was associated with, to disguise the origins of the stolen funds.</p> |
| 8 | <p>Bribery and Corruption: The surgeon accepted bribes and kickbacks in exchange for performing surgeries, directly relating to corrupt practices.</p> <p>Collusion and Conspiracy: The involvement of doctors, chiropractors, marketers, and the hospital owner in a coordinated scheme to exchange kickbacks for patient referrals.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: By disguising the bribes as marketing services and fees based on a sham contract, there is a manipulation of financial statements to cover illegal payments.</p>  |

|    |  |
|----|--|
|    | Procurement and Vendor Fraud: This applies due to the referral of patients to a specific hospital for surgeries in exchange for kickbacks, involving manipulation of procurement processes for personal gain.  |
|    | Regulatory Evasion and Deception: The entire operation was structured to evade regulations governing the medical and insurance industries, specifically workers' compensation systems.   |
| 9  | Asset Misappropriation: Figg's embezzlement of funds from United Bank directly involves the theft and misuse of the company's assets.  |
|    | Fraudulent Claims and Invoices: The creation of phony loans in customer names and funneling fees to his own use can be considered under this category, as it involves fabricating financial transactions for personal gain.  |
|    | Tax Evasion and False Tax Claims: Figg concealed his taxable income derived from illegal activities and underreported his income to avoid tax payments.  |
|    | Identity Theft, Data Breach and Impersonation: Obtaining loans in customer names without their knowledge involves the unauthorized use of their identity, which falls under this category.   |
| 10 | Asset Misappropriation: This is the primary type of fraud occurring as the bank manager embezzled money directly from the bank's vault, which is a clear misuse of the company's assets.   |
|    | Collusion and Conspiracy: Given that Cherry admitted to giving the stolen money to her boyfriend, this implies a level of collusion or conspiracy, even though the boyfriend's involvement in the planning or execution of the theft isn't detailed.               |
| 11 | Asset Misappropriation: Dinoto embezzled more than \$1.8 million from her employer by falsely inflating her compensation and using the company's credit card for personal expenses, which directly involves the theft or misuse of company's assets.               |
|    | Forgery and Counterfeiting: The act of forging at least two checks to herself from her employer's account falls under this category.   |
|    | Manipulation of Company Systems: Modifying her employer's accounting records to hide her embezzlement activities fits this description.  |
|    | Tax Evasion and False Tax Claims: Dinoto did not report over \$1 million embezzled from her employer and income received from another company on her federal income tax returns.   |
|    | Identity Theft, Data Breach and Impersonation: Collecting unemployment benefits under her true Social Security number while employed full-time under a fake Social Security number constitutes identity theft and impersonation.                                   |
| 12 | Asset Misappropriation: Lindberg allegedly used insurance company funds for his personal benefit, including the purchase and refinancing of personal real estate and forgiving more than \$125 million in loans to himself.  |
|    | Regulatory Evasion and Deception: The indictment describes actions to deceive the North Carolina Department of Insurance and evade regulatory requirements meant to protect policyholders.   |
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Lindberg is accused of concealing the true financial condition of his insurance companies and engaging in complex financial investments to disguise the financial health of these entities. |

|    |  |
|----|--|
|    | Collusion and Conspiracy: The indictment charges Lindberg with conspiracy to commit crimes in connection with insurance business, highlighting an agreement to defraud various parties.                                      |
|    | Money Laundering: Lindberg is charged with one count of money laundering conspiracy, indicating the alleged process of disguising the proceeds of his fraudulent activities.   |
| 13 | Asset Misappropriation: Since Burley misused the school districts' funds for personal gain, this directly involves the theft or misuse of the organizations' assets.   |
|    | Payroll Fraud: Burley altered her payroll information, which is a direct form of payroll fraud.  |
|    | Fraudulent Claims and Invoices: This could be applicable if Burley fabricated or altered invoices to legitimize the unauthorized payments to her accounts or for personal expenses like the Amazon account.                  |
|    | Manipulation of Company Systems: By altering payroll information and making unauthorized payments, Burley manipulated the school districts' financial and payroll systems.   |
| 14 | Asset Misappropriation: Collins misused and stole the church's assets through unauthorized credit card transactions.   |
|    | Fraudulent Claims and Invoices: This can be inferred from her use of church-issued credit cards for personal expenses, which would require fraudulent justification or claims to avoid detection.                            |
|    | Manipulation of Company Systems: Collins was responsible for managing the church's accounting system and used this position to embezzle funds, indicating manipulation of the system to her advantage.                       |
|    | Regulatory Evasion and Deception: Making false statements to obstruct the investigation and prosecution demonstrates attempts to evade regulatory scrutiny and deceive investigators.  |
| 15 | Fraudulent Claims and Invoices: The scheme involved the submission of false invoices to support fraudulent claims for reimbursement from the NBA Players' Health and Welfare Benefit Plan.                                   |
|    | Collusion and Conspiracy: The participants in the scheme, including KEYON DOOLING and ALAN ANDERSON, orchestrated and engaged in a collaborative effort to defraud the Plan.   |
|    | Forgery and Counterfeiting: The scheme involved the creation of fake invoices and potentially forged letters of medical necessity to substantiate the fraudulent claims.   |
|    | Regulatory Evasion and Deception: By engaging in activities designed to deceive the health and welfare benefit plan, the individuals involved were evading regulatory standards meant to govern the integrity of such plans. |
| 16 | Asset Misappropriation: Tischer misused the special needs trust funds, which were assets meant for the beneficiary, by spending them on personal expenses.   |
|    | Manipulation of company systems: Tischer forged ledger entries to conceal the misappropriation of funds from the trust.  |
|    | Fraudulent Claims and Invoices: By documenting false expenditures in the trust's ledger, Tischer made fraudulent claims about the use of the funds.  |
| 17 | Asset Misappropriation: Spadoni misused hospital funds by directing them to a company he had a financial interest in, for services that were not provided as claimed.  |

|    |   |
|----|---|
|    | <p>Fraudulent Claims and Invoices: By causing the hospital to pay for purported services that were not actually provided by MES, Spadoni engaged in making fraudulent claims and invoicing the hospital for non-existent services.</p> <p>Creation of Shell Company: Spadoni established Medical Education Solutions (MES) which appears to have been used as a conduit for fraud, fitting the definition of a shell company in this context.</p> <p>Money Laundering: The indictment charges Spadoni with money laundering, which involves the process of making large amounts of money generated by a criminal activity, such as fraud, appear to be legally obtained.</p>  |
| 18 | <p>Asset Misappropriation: Suresh Munshani, in conspiracy with his brother, stole nearly \$1 million from the brother's employer, which is a clear case of misusing the company's assets for personal gain.</p> <p>Creation of Shell Company: Munshani formed a fake company to facilitate the fraudulent scheme, indicating the use of a shell company to conceal the origins of the stolen funds.</p> <p>Collusion and Conspiracy: The conspiracy between Suresh Munshani and his brother to commit wire fraud and money laundering involves collusion to defraud the victim company.</p> <p>Money laundering: The act of laundering the stolen money through a Canadian bank account and then transferring the majority back to a bank account controlled by his brother fits the definition of money laundering, where the illegal proceeds were made to appear legitimate.</p> |
| 19 | <p>Asset Misappropriation: Carson transferred funds from the church and school business accounts to her personal accounts, directly misusing the organization's assets for personal gain.</p> <p>Fraudulent Claims and Invoices: By making false entries into the database to track payments, Carson was essentially creating fraudulent records to justify the illegal transfers.</p> <p>Forgery and Counterfeiting: The creation of a phantom account in the church's name and possibly forging documents or signatures to authorize transfers could fall under this category.</p> <p>Manipulation of Company Systems: Carson manipulated the parish's financial tracking system to conceal her embezzlement activities.</p>  |
| 20 | <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: Eddy Alexandre made false representations about the investment returns of his cryptocurrency and forex trading platform, misleading investors about the financial health and potential of the investments.</p> <p>Asset Misappropriation: Alexandre misused investors' funds for personal purchases, such as buying a BMW and making car payments, which were assets meant for investment purposes.</p> <p>Money Laundering: By redirecting investors' funds to his personal bank account and using them for personal expenses, Alexandre engaged in activities that could be classified as laundering the proceeds of his fraudulent scheme.</p>   |
| 21 | <p>Collusion and Conspiracy: Ryan and others conspired to defraud First NBC Bank by disguising the true financial status of borrowers and their troubled loans.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: By concealing the true financial condition of the bank from the Board, auditors, and examiners, Ryan engaged in financial statement fraud.</p>  |

|    |  |
|----|--|
|    | Forgery and Counterfeiting: Making false entries in bank records constitutes forgery, as it involves falsifying documents to conceal the true state of affairs.  |
| 22 | Asset Misappropriation: Downey stole funds from homeowners' association accounts, which is a clear case of misusing company or client assets for personal gain.  |
|    | Fraudulent Claims and Invoices: By submitting false statements to conceal her mishandling of funds, Downey made fraudulent claims about her entitlements and expenditures.   |
| 23 | Asset Misappropriation: Owens-Sharp stole over \$800,000 from her employer by altering checks and depositing them into her own account.  |
|    | Fraudulent Claims and Invoices: By making false entries in the company's records to reflect payroll and expenses for non-existent employees, Owens-Sharp made fraudulent claims.   |
|    | Forgery and Counterfeiting: Altering paper checks by removing the employees' names and replacing them with her own constitutes forgery.  |
|    | Payroll Fraud: Requesting paper paychecks in addition to direct deposit checks for employees and then altering those checks for her own benefit directly involves payroll fraud.   |
|    | Payroll Tax Evasion: The act of causing the company to incur additional payroll taxes due to fraudulently obtained funds can be seen as contributing to payroll tax evasion, although indirectly, as the primary intent was to embezzle funds rather than evade taxes. |
| 24 | Asset Misappropriation: Woodson and Thompson misused city funds for personal expenses, which constitutes the theft or misuse of the organization's assets.   |
|    | Forgery and Counterfeiting: They forged the signature of the mayor and/or the treasurer on the checks, which directly involves creating false documents or altering existing ones to facilitate fraud.   |
|    | Fraudulent Claims and Invoices: By writing checks to themselves without authority, Woodson and Thompson made fraudulent claims for payments that were not legitimate.  |
| 25 | Asset Misappropriation: TIGLER embezzled funds from Client A's account, which is a clear misuse of the client's assets.  |
|    | Forgery and Counterfeiting: TIGLER forged signatures on counter checks to facilitate the embezzlement of funds.  |
|    | Tax Evasion and False Tax Claims: TIGLER failed to report significant amounts of embezzled income on her tax returns, constituting tax evasion.  |
|    | Identity Theft, Data Breach and Impersonation: By using personal information from legitimate banking transactions to create fraudulent counter checks, TIGLER engaged in identity theft and impersonation.   |
| 26 | Asset Misappropriation: Rivero stole clients' funds, which were assets entrusted to him for investment purposes, and used them for personal expenses and gambling.   |
|    | Fraudulent Claims and Invoices: By claiming he would invest the funds on behalf of his clients but instead using them for personal gain, Rivero made fraudulent claims about the use of the funds.   |

|    |  |
|----|--|
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: He also pleaded guilty to securities fraud, which involves deceitful practices in the trading of securities, such as making false representations to investors.   |
| 27 | Asset Misappropriation: SHARP misused his administrative access to steal confidential files from his employer, which constitutes the misuse of company assets.   |
|    | Identity Theft, Data Breach and Impersonation: SHARP committed identity theft and data breach by unauthorized access and download of gigabytes of confidential data. He also impersonated an anonymous attacker in his extortion attempt.  |
|    | Manipulation of Company Systems: SHARP altered log retention policies and other files to conceal his unauthorized activities, directly manipulating the company's computer systems.  |
|    | Regulatory Evasion and Deception: By causing the publication of misleading news articles about the company's handling of the security breach, SHARP engaged in deception that likely aimed to evade regulatory scrutiny and affect the company's compliance with public disclosure requirements. |
| 28 | Asset Misappropriation: CHABAUD misappropriated funds from Band A's bank accounts, which is a clear case of stealing or misusing the company's assets.   |
|    | Identity Theft, Data Breach and Impersonation: By illegally accessing Band A's bank accounts after her termination, CHABAUD assumed unauthorized access, which could be seen as a form of identity theft or impersonation to commit fraud.   |
| 29 | Asset Misappropriation: Girardi is accused of embezzling more than \$15 million from his clients, which directly involves the theft or misuse of assets entrusted to him.  |
|    | Collusion and Conspiracy: The involvement of Christopher Kazuo Kamon, the law firm's controller and CFO, alongside Girardi in the alleged embezzlement scheme suggests collusion and conspiracy to commit the fraud  |
| 30 | Tax Evasion and False Tax Claims: Cory evaded more than \$600,000 in taxes by not reporting income and not filing tax returns as required by law.  |
|    | Creation of Shell Company: Cory used Gambit Matrix LLC, a shell company he controlled, to funnel more than \$1.5 million under false pretenses.  |
|    | Forgery and Counterfeiting: By falsifying emails and IRS Forms W-9, Cory engaged in forgery to support his tax evasion and conceal his fraudulent activities.  |
|    | Fraudulent Claims and Invoices: Cory caused transfers to Gambit Matrix under the false pretense of payments for consulting services that had never been provided, making fraudulent claims to his employer.  |
| 31 | Asset Misappropriation: Bowker embezzled more than \$130,000 from the company, clearly misusing company assets for personal gain.  |
|    | Payroll Tax Evasion: By failing to file quarterly employment tax returns and not paying over the employment taxes owed to the IRS, Bowker engaged in payroll tax evasion.  |
| 32 | Asset Misappropriation: Funds intended for the benefit of the Grand Traverse Band of Ottawa and Chippewa Indians were stolen or misused by Groom and his co-defendant for personal gain.   |

|    |   |
|----|---|
|    | Creation of Shell Company: R.O. Distributors and Evergreen Distributors LLC were shell companies created to facilitate the fraud.   |
|    | Collusion and Conspiracy: Groom, his co-defendant, and others conspired to commit wire fraud, including recruiting an individual to impersonate a corporate official.   |
|    | Fraudulent Claims and Invoices: Misrepresentations were made to the tribe about the investment in R.O. Distributors and the leasing of water coolers with proprietary technology.   |
|    | Identity Theft, Data Breach and Impersonation: Groom recruited a friend to impersonate a corporate official of High Sierra, which involves impersonation to deceive the tribe.  |
| 33 | Asset Misappropriation: Dodson misused investor funds, which were assets meant for investment in Citadel Energy, for his own personal expenses.   |
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Dodson made materially false and misleading representations to investors regarding the use of funds, the status of a potential acquisition, and his own compensation.  |
|    | Collusion and Conspiracy: The scheme involved multiple actions and decisions by Dodson to defraud investors, which could imply collusion or conspiracy to carry out the fraud, although not explicitly mentioned, the orchestration of such a scheme often involves a level of collusion. |
|    | Money Laundering: The act of pooling funds from the limited partnerships and conducting multiple transfers between accounts to divert funds for personal benefit and conceal his actions hints at behavior characteristic of money laundering   |
| 34 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Bernardi orchestrated a scheme involving false and misleading misrepresentations, fabricated bank statements, and audit reports to defraud investors and lenders.  |
|    | Forgery and Counterfeiting: Fabrication of bank statements, audit materials, and a misleading letter purporting to be from GigaTrust's counsel are clear instances of forgery.  |
|    | Identity Theft, Data Breach and Impersonation: Bernardi and his co-defendants impersonated a customer, auditor, and GigaTrust's lawyer, which directly aligns with impersonation fraud.   |
|    | Collusion and Conspiracy: Bernardi, along with Cardak and Chandra, devised and participated in a fraudulent scheme, indicating collusion and conspiracy to defraud  |
| 35 | Asset Misappropriation: Jackson embezzled funds directly from the credit union, including stealing cash from the vault, which is a clear misuse of the company's assets.  |
|    | Identity Theft, Data Breach and Impersonation: By opening lines of credit in the names of family members without their consent, Jackson engaged in identity theft.  |
|    | Fraudulent Claims and Invoices: The fraudulent transfers made to herself from the account of a deceased credit union member fall under making fraudulent claims.  |
|    | Manipulation of Company Systems: Jackson used her administrative authority to lock access to accounts she was misusing, thereby manipulating the credit union's systems to hide her activities.   |
| 36 | Asset Misappropriation: Stites embezzled more than \$712,000 from Norbrook, clearly misusing the company's assets.  |



|    |   |
|----|---|
|    | <p>Fraudulent Claims and Invoices: By creating two fake companies and manipulating invoices to embezzle funds, Stites engaged in making fraudulent claims and invoices.</p> <p>Creation of Shell Company: The establishment of two fake companies to facilitate the embezzlement of funds falls under the creation of a shell company.</p>  |
| 37 | <p>Identity Theft, Data Breach and Impersonation: Briggs stole banking information from individuals, businesses, and a law firm, which directly relates to identity theft and data breach.</p> <p>Forgery and Counterfeiting: The creation of fraudulent personal and business checks from the stolen information aligns with forgery and counterfeiting.</p> <p>Collusion and Conspiracy: Briggs' provision of stolen information to Kobi, who then worked with others to deposit fraudulent checks and withdraw funds, constitutes collusion and conspiracy.</p> <p>Money Laundering: The act of depositing fraudulent checks and then attempting to make rapid withdrawals can be seen as an attempt to launder the proceeds of the fraudulent scheme.</p> |
| 38 | <p>Collusion and Conspiracy: Aaron Stephens conspired with others to rig bids on government contracts, which directly involves collusion among parties to manipulate the bidding process.</p> <p>Regulatory Evasion and Deception: The act of rigging bids to create a false impression of competition involves deceiving regulatory processes designed to ensure fair competition for government contracts.</p>  |
| 39 | <p>Asset Misappropriation: Slingerland embezzled money from the nonprofit for personal benefit, which directly involves the misuse of the company's assets.</p> <p>Fraudulent Claims and Invoices: By causing funds to be spent on unauthorized expenditures and manipulating finances to cover personal expenses, this action is applicable.</p> <p>Tax Evasion and False Tax Claims: By not reporting money he obtained from YPI and underreporting over \$100,000 in income for multiple years, Slingerland engaged in tax evasion.</p> <p>Regulatory Evasion and Deception: Misapplying grant money and lying on tax returns to evade regulatory oversight and legal obligations.</p>   |
| 40 | <p>Asset Misappropriation: Maurello misappropriated more than \$2 million in museum funds, a clear case of stealing or misusing the company's assets.</p> <p>Payroll Fraud: By fraudulently obtaining museum funds through manipulation of the payroll system, designating payments to his personal bank accounts as if they were made to other employees.</p> <p>Forgery and Counterfeiting: Maurello edited and altered a report from the museum's payroll system, including changing employees' names, dates, and dollar amounts, which constitutes forgery.</p> <p>Manipulation of Company Systems: Using his position to manipulate the payroll system to divert funds to his personal accounts and to alter reports to conceal his actions.</p>         |
| 41 | <p>Asset Misappropriation: Little stole more than \$419,542 from her former employer, which is a direct misuse of the company's assets.</p>   |

|    |   |
|----|---|
|    | <p>Fraudulent Claims and Invoices: By submitting forged and falsified receipts for reimbursement, Little engaged in making fraudulent claims.</p> <p>Forgery and Counterfeiting: The use of forged receipts, including the repeated use of a receipt from Nando's Chicken that belonged to a celebrity, indicates forgery.</p> <p>Identity Theft, Data Breach and Impersonation: By using another employee's account to submit fraudulent reimbursement requests, Little engaged in identity theft and impersonation.</p>   |
| 42 | <p>Asset Misappropriation: Abboud embezzled funds from Human First, a nonprofit organization, for personal use, which is a clear misuse of the company's assets.</p> <p>Fraudulent Claims and Invoices: The use of inflated invoices to disguise overpayments to contractors, which were then kicked back to Abboud, falls under making fraudulent claims.</p> <p>Collusion and Conspiracy: Abboud conspired with co-defendants to embezzle funds and commit bank fraud, indicating collusion and conspiracy in committing these crimes.</p> <p>Money Laundering: The process of disguising the overpayments through sham bank accounts before depositing them into accounts controlled by Abboud demonstrates elements of money laundering.</p> <p>Bribery and Corruption: Although not explicitly mentioned, the kickback scheme with contractors implies corrupt practices, which can be categorized under bribery and corruption.</p> |
| 43 | <p>Asset Misappropriation: Skidmore misused BCID's funds for personal use, which clearly falls under the misuse of company assets.</p> <p>Fraudulent Claims and Invoices: Creating fictitious invoices to make it appear funds were used for legitimate business expenses when they were actually used for personal benefit.</p> <p>Money Laundering: Charged with 24 counts of money laundering, Skidmore engaged in financial transactions to conceal the origins of the fraudulently obtained money.</p> <p>Manipulation of Company Systems: By making false entries in the BCID's internal accounting records to misrepresent the use of funds, Skidmore manipulated company systems to support her fraudulent activities.</p>  |
| 44 | <p>Asset Misappropriation: Boisture diverted ZoneFlow's money to herself, which directly involves stealing or misusing the company's assets.</p> <p>Fraudulent Claims and Invoices: By making misrepresentations to PayPal and WebBank to induce them to make unauthorized loans, Boisture was essentially submitting fraudulent claims.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: Her actions likely involved manipulating financial records or misrepresenting financial data to PayPal and WebBank to secure the loans, fitting the criteria for financial statement fraud.</p> <p>Collusion and Conspiracy: Given the complexity of defrauding both her employer and lenders through unauthorized loans and misrepresentations, her actions suggest a level of collusion or conspiracy to commit the fraud, even if the case description does not explicitly mention accomplices.</p>             |

|    |  |
|----|--|
| 45 | Asset Misappropriation: Carroll misappropriated funds from Southeastern University by directing payments to a corporation he secretly controlled for work that was not performed by that corporation.                                    |
|    | Creation of Shell Company: Carroll's establishment of a New Mexico corporation that he secretly controlled to funnel university funds constitutes the creation of a shell company.   |
|    | Fraudulent Claims and Invoices: Generating contracts and invoices for payment by the university for work that was never performed by his corporation falls under making fraudulent claims and invoices.                                  |
| 46 | Asset Misappropriation: Lana Pothos embezzled \$1.2 million from elderly customers' savings, which is a clear misuse of the victims' assets.   |
|    | Identity Theft, Data Breach and Impersonation: Pothos used a victim's personal identifiable information to fraudulently open bank accounts and impersonated the victim, constituting identity theft.                                     |
|    | Manipulation of Company Systems: By using the bank's internal systems to change the victims' mailing address and telephone number to facilitate her fraud, Pothos manipulated company systems.   |
|    | Collusion and Conspiracy: Pothos and her accomplice worked together to commit the fraud, indicating collusion and conspiracy.  |
| 47 | Asset Misappropriation: Spilberg embezzled over \$300,000 from his employer by misusing a company charge card for personal expenses, which is a clear misuse of the company's assets.  |
| 48 | Asset Misappropriation: Simkins embezzled funds from Genesys Industrial Corporation, directly stealing money to cover personal expenses, which is a clear case of misusing the company's assets.   |
|    | Tax Evasion and False Tax Claims: By failing to report the stolen income on his federal and state tax returns, Simkins engaged in tax evasion.   |
|    | Collusion and Conspiracy: Simkins's involvement with another employee in embezzling funds from the company shows collusion and conspiracy to commit fraud.   |
| 49 | Asset Misappropriation: Initially involved in an embezzlement case, indicating misuse of company or organizational assets.   |
|    | Fraudulent Claims and Invoices: Falsely applying for PPP loans involves making fraudulent claims to obtain funds.  |
|    | Forgery and Counterfeiting: By providing false information on loan applications, Schulte engaged in a form of forgery.   |
| 50 | Asset Misappropriation: Barbara Chalmers embezzled at least \$29 million from her employer by writing herself checks, which directly involves the misuse of the company's assets.  |
|    | Fraudulent Claims and Invoices: Providing false paperwork to tax preparers to misstate year-end cash-on-hand numbers constitutes making fraudulent claims.   |
|    | Money Laundering: Using the stolen money to fund a construction business, of which she was the president, aligns with the definition of money laundering, as she engaged in transactions to disguise the origins of the embezzled funds. |
| 51 | Collusion and Conspiracy: Pourhassan and Kazempour engaged in a conspiracy to defraud investors through false and misleading representations about the drug development process and regulatory submissions.                              |

|    |  |
|----|--|
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Making false and misleading representations about CytoDyn’s regulatory submissions to the FDA to inflate the stock price and attract new investors.   |
|    | Regulatory Evasion and Deception: Misleading investors about the timeline and status of regulatory submissions, including the submission of an incomplete application to the FDA, constitutes evasion and deception in regulatory processes.   |
| 52 | Asset Misappropriation: Marquez embezzled more than \$700,000 from his employer by transferring funds without authorization into an account he controlled.   |
|    | Forgery and Counterfeiting: By altering the business's bank statements to conceal his embezzlement, Marquez engaged in forgery.  |
|    | Tax Evasion and False Tax Claims: Filing a false tax return for 2017 that did not report the embezzled funds constitutes tax evasion.  |
| 53 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Collins provided false information about a loan portfolio, misleading the bank, investors, and rating agencies, which directly relates to misrepresenting financial information for personal or company gain. |
|    | Collusion and Conspiracy: Collins schemed with another top executive, indicating a collaborative effort to defraud the bank.   |
|    | Asset Misappropriation: While not directly stated, the manipulation of loan statuses and the advancement of funds through improper accounting entries to maintain or increase funding could be seen as a misuse of the bank's assets or credit facilities provided to the company.   |
|    | Forgery and Counterfeiting: This could be implied as Collins selected delinquent vehicle loans, knowing they were not eligible, and misrepresented them, possibly involving the creation or alteration of financial documents or statements to hide the true nature of these loans.  |
| 54 | Asset Misappropriation: Vicars stole money from his employer by submitting and approving fraudulent invoices for work that was never performed.  |
|    | Fraudulent Claims and Invoices: By submitting fraudulent invoices from his own company for fictitious work, Vicars engaged in creating fraudulent claims and invoices.   |
|    | Tax Evasion and False Tax Claims: Vicars filed a false tax return by failing to report the stolen money as income, which constitutes tax evasion and making false tax claims   |
| 55 | Asset Misappropriation: Smith embezzled funds directly from the company’s business bank accounts to finance personal expenditures, which is a clear misuse of the company's assets.  |
|    | Fraudulent Claims and Invoices: By altering her payroll to increase her salary without permission, Smith made fraudulent claims for compensation she was not entitled to.  |
|    | Forgery and Counterfeiting: Altering the company’s general ledger to conceal her activities can be considered as forgery.  |

|    |  |
|----|--|
|    | Manipulation of Company Systems: Smith manipulated the company’s financial and payroll systems by transferring money between accounts and limiting access to banking statements to hide her embezzlement.    |
| 56 | Tax Evasion and False Tax Claims: Reyes did not file income tax returns and did not report over \$1.15 million in wages, thereby evading income taxes.   |
|    | Forgery and Counterfeiting: By submitting false Forms W-4 claiming exemption from federal income tax withholding, Reyes engaged in forgery to mislead his employers and the IRS.                             |
| 57 | Fraudulent Claims and Invoices: Submitting over \$463 million in genetic and other laboratory tests that patients did not need represents making fraudulent claims to Medicare.                              |
|    | Collusion and Conspiracy: Patel's coordination with patient brokers, telemedicine companies, and call centers to defraud Medicare indicates collusion and conspiracy.  |
|    | Bribery and Corruption: Paying kickbacks and bribes to patient brokers for obtaining signed doctors’ orders is an act of bribery and corruption.   |
|    | Money Laundering: Patel was convicted of conspiracy to commit money laundering, involving the processing of proceeds from the healthcare fraud scheme  |
| 58 | Asset Misappropriation: Bowker embezzled more than \$130,000 from the company, indicating misuse of company assets for personal gain.  |
|    | Payroll Tax Evasion: Failing to pay over \$3.6 million in income and FICA tax withholdings to the IRS falls under payroll tax evasion.   |
|    | Regulatory Evasion and Deception: By not accounting for and paying over withholding and FICA taxes, Bowker engaged in evasion of regulatory requirements.  |
| 59 | Asset Misappropriation: Bankman-Fried misappropriated billions of dollars of customer funds deposited with FTX for personal use, investments, and to repay loans.  |
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Concealing misuse of customer deposits in financial information provided to lenders and equity investors of FTX and Alameda Research. |
|    | Money Laundering: Bankman-Fried is charged with conspiracy to commit money laundering, involving the illicit handling of the misappropriated funds.  |
|    | Collusion and Conspiracy: Engaging in a scheme to defraud customers, lenders, and investors through coordinated actions with co-conspirators.  |
|    | Fraudulent Claims and Invoices: By misrepresenting the financial stability and operational integrity of FTX and Alameda Research to customers, lenders, and investors.                                       |
| 60 | Asset Misappropriation: Meeks misused the company's credit cards for unauthorized personal purchases, directly stealing company funds.   |
|    | Fraudulent Claims and Invoices: By mislabeling unauthorized purchases as legitimate payments in the company records, Meeks made fraudulent claims.   |

|    |  |
|----|--|
|    | Manipulation of Company Systems: By withholding pages listing unauthorized purchases before providing records to the owners, Meeks manipulated the company's accounting systems to conceal her fraud   |
| 61 | Asset Misappropriation: Kewalis misused her position to steal \$254,532 in funds from the credit union, directly embezzling company assets.  |
|    | Fraudulent Claims and Invoices: By creating fraudulent accounts and making fraudulent entries in the credit union's accounting system, Kewalis made false claims.  |
|    | Manipulation of Company Systems: Kewalis used her access to manipulate the credit union's accounting system for fraudulent purposes.   |
| 62 | Asset Misappropriation: Hicks embezzled over one million dollars from the company, which includes the misuse of company assets for personal gain.  |
|    | Fraudulent Claims and Invoices: By getting reimbursement for false expense reports and fraudulent invoices, Hicks engaged in creating fraudulent claims.   |
|    | Identity Theft, Data Breach and Impersonation: Although not directly mentioned, the actions of enrolling family members in company services without authorization and misuse of company resources could involve elements of impersonation or misuse of identity. |
|    | Manipulation of Company Systems: Hicks used his IT administrative access to orchestrate schemes and refused to provide his computer and passwords during an investigation, indicating manipulation of company systems to hide his activities.                    |
| 63 | Asset Misappropriation: Ms. Lazzaro embezzled funds directly from the bank, including stealing cash from her teller drawer and as a vault manager, which is a clear misuse of the bank's assets.   |
|    | Manipulation of Company Systems: By inputting false information into the bank's computer system to manipulate teller and vault balances, Ms. Lazzaro engaged in manipulation of company systems.   |
| 64 | Asset Misappropriation: McManus embezzled funds from his employer by using company funds to pay off his personal credit card expenses and issuing reimbursements to himself for personal expenses.   |
|    | Tax Evasion and False Tax Claims: By omitting the embezzled income from his federal income tax returns, McManus engaged in tax evasion, resulting in a tax loss to the IRS.  |
| 65 | Asset Misappropriation: Sharar embezzled over \$2.1 million from her employer, directly misusing the company's assets for personal gain.   |
|    | Fraudulent Claims and Invoices: By falsifying company financial reports to hide the embezzlement, Sharar made fraudulent claims about the financial status of the company.   |
|    | Manipulation of Company Systems: Sharar used her position as CFO to manipulate financial systems and records to conceal her theft  |

|    |  |
|----|--|
| 66 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Neil Cole was involved in a scheme to fraudulently inflate Iconix's revenue and earnings per share (EPS), misleading investors and the public about the company's financial health                    |
|    | Forgery and Counterfeiting: By engaging in "round trip" transactions with inflated buy-in purchase prices and then reimbursing the JV partner for these overpayments, Cole effectively engaged in creating misleading financial transactions that lacked economic substance. |
|    | Collusion and Conspiracy: Cole conspired with at least one senior Iconix executive and a JV partner to execute the fraudulent scheme, indicating collusion to commit financial statement fraud.  |
|    | Manipulation of Company Systems: By hiding the true nature of the transactions from Iconix's lawyers and outside auditors, Cole manipulated company systems to prevent detection of the fraudulent scheme  |
| 67 | Asset Misappropriation: Swanson embezzled \$804,413 from her employer, which is a clear misuse of the company's assets.  |
|    | Payroll Fraud: By fraudulently altering the payroll process to increase the amount of money she received, Swanson committed payroll fraud.   |
| 68 | Asset Misappropriation: Kent embezzled money from his employer through various schemes, which directly involves stealing or misusing the company's assets.   |
|    | Fraudulent Claims and Invoices: By submitting doctored receipts and fictitious invoices for reimbursement, Kent engaged in creating fraudulent claims.   |
|    | Forgery and Counterfeiting: Doctoring receipts to inflate purchase amounts and submitting fictitious invoices involves forgery.  |
| 69 | Tax Evasion and False Tax Claims: Farley failed to pay over the trust fund taxes (Social Security, Medicare, and federal income taxes) that had been withheld from employees' paychecks, which constitutes tax evasion.  |
|    | Asset Misappropriation: Although not directly mentioned, the check kiting scheme and failure to remit employee taxes can be seen as misusing the company's and employees' financial assets for personal gain or to maintain business operations illegitimately.              |
| 70 | Asset Misappropriation: The embezzlement of \$2.9 million from the U.S. Department of Veteran's Affairs constitutes a direct misuse of government assets.  |
|    | Fraudulent Claims and Invoices: Generating phony purchase orders for equipment and materials that were never delivered involves making fraudulent claims and invoices.   |
|    | Creation of Shell Company: Mr. McGlown's establishment of G4 Logistics and Caprice as companies that did not deliver any actual goods or services fits the definition of creating shell companies.   |
|    | Procurement and Vendor Fraud: The scheme to enter a fake company into the medical center's vendor system and generate false purchase orders is a clear case of procurement and vendor fraud.   |

|    |  |
|----|--|
|    | Collusion and Conspiracy: The collaborative effort between Mr. McGlown, Mr. Gates, and the individual identified as J.R. to execute and benefit from this scheme demonstrates collusion and conspiracy.  |
|    | Forgery and Counterfeiting: Creating fake invoices to cover up the non-delivery of goods involves forgery  |
| 71 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: James coordinated to manipulate his company's financial records to falsely reflect profit, which directly relates to falsifying financial statements to mislead stakeholders.   |
|    | Payroll Tax Evasion: James failed to make the payroll taxes payments for his companies, which is a clear case of evading payroll taxes   |
| 72 | Asset Misappropriation: Aggarwal stole \$2.5 million from his employer by submitting fictitious invoices, which constitutes a clear misuse of the company's assets.  |
|    | Fraudulent Claims and Invoices: Submitting fraudulent invoices for consulting services that were never performed.  |
|    | Manipulation of Company Systems: Utilizing his knowledge and position to manipulate the company's policies and procedures for his own benefit.   |
|    | Collusion and Conspiracy: Involving friends and family in submitting fraudulent invoices implies collusion to defraud the employer   |
| 73 | Asset Misappropriation: Michael D. Allen stole millions of dollars from his employer, which is a clear case of misusing the company's assets for personal gain.  |
|    | Money Laundering: Allen also pleaded guilty to money laundering, which involves engaging in financial transactions to conceal the origin of money obtained from illegal activities, such as purchasing a 5.19 carat diamond ring with the stolen funds |
| 74 | Asset Misappropriation: Ritter embezzled funds from customer accounts at Summit Community Bank, which is a direct misuse of the company's assets.  |
|    | Tax Evasion and False Tax Claims: By failing to report the embezzled funds as income on his tax return, Ritter engaged in tax evasion and filed a false tax return.  |
| 75 | Asset Misappropriation: Steele embezzled funds from Victim Company A through various means, directly misusing the company's assets for personal gain.  |
|    | Fraudulent Claims and Invoices: The use of company credit cards for personal expenditures, issuing checks to herself, and executing unauthorized wire transfers are all indicative of making fraudulent claims against company assets.                 |
|    | Manipulation of Company Systems: Steele manipulated company systems, including Quickbooks and bank wire systems, to execute unauthorized transactions.   |
| 76 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Rogas engaged in securities fraud by creating and using fraudulent financial data to obtain financing, misleading investors with materially false financial statements.         |
|    | Forgery and Counterfeiting: By altering bank statements to show non-existent customer revenue and bank balances, Rogas engaged in forgery.   |



|    |  |
|----|--|
|    | Asset Misappropriation: Although not directly mentioned, the personal gain of approximately \$17.5 million from the fraudulent scheme suggests misappropriation of the company's assets.   |
|    | Fraudulent Claims and Invoices: This is implied through the creation of fictitious revenue and customers, essentially making fraudulent claims about the company's financial health  |
| 77 | Bribery and Corruption: Sharon Barnes Sutton accepted cash bribes in exchange for favorable actions or influence, which is a direct form of corruption.  |
|    | Procurement and Vendor Fraud: As explicitly mentioned in the case, Barnes Sutton was convicted of Procurement and Vendor Fraud, demanding payments from a subcontractor under duress.  |
|    | Collusion and Conspiracy: The act of demanding and accepting bribes suggests a collusion between the former commissioner and parties looking to gain favor, although not explicitly stated, the nature of extortion and bribery often involves some level of conspiracy. |
| 78 | Fraudulent Claims and Invoices: Mensinger submitted false loan applications, which is akin to making fraudulent claims to obtain financing.  |
|    | Manipulation of Company Systems: By abusing his position as Chief Lending Officer to authorize and facilitate the approval of these loans, Mensinger manipulated the financial institution's lending systems.  |
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This case involves misrepresentation to obtain loans, which can be considered a form of financial statement fraud, especially since it involved presenting false information to secure financing. |
| 79 | Asset Misappropriation: Valentin embezzled funds directly from Dealers Electrical Supply (DES) by diverting checks intended for DES into her personal account for her own use.   |
|    | Fraudulent Claims and Invoices: By diverting customer payments meant for DES to her personal account, Valentin engaged in making fraudulent claims, as she effectively misrepresented the destination of these funds.  |
| 80 | Bribery and Corruption: Both individuals received cash payments in exchange for approving invoice payments for an asphalt and paving company, which constitutes bribery.   |
|    | Fraudulent Claims and Invoices: The approval of invoices for payments from the municipality to the asphalt and paving company, based on false certifications, falls under fraudulent claims and invoices.  |
|    | Collusion and Conspiracy: Both individuals conspired with others to commit federal program bribery by agreeing to receive and receiving cash payments in exchange for their actions  |
| 81 | Asset Misappropriation: Williams embezzled funds from AESC, a non-profit organization receiving federal funds intended for the operation of PCS, demonstrating a misuse or theft of the organization's assets.   |
|    | Fraudulent Claims and Invoices: This could be inferred if Williams justified the unlawful payments to herself by fabricating or manipulating invoices or claims to conceal the embezzlement.   |
|    | Manipulation of Company Systems: Williams manipulated the financial and operational systems of AESC and FSESC to divert funds for personal use.  |

|    |  |
|----|--|
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: If Williams altered the financial statements of AESC or FSESC to cover up the embezzlement, this action would apply.  |
|    | Regulatory Evasion and Deception: By misappropriating federal funds intended for educational purposes, Williams engaged in deceptive practices to evade regulatory requirements and oversight.   |
| 82 | Asset Misappropriation: Crawford misused her position to embezzle funds from Saint Anselm College for personal use.  |
|    | Fraudulent Claims and Invoices: She submitted fraudulent invoices for a company she created to receive funds from the College.   |
|    | Creation of Shell Company: The fraudulent invoices were for a company that Crawford created, indicating the use of a shell company to facilitate the fraud.  |
|    | Procurement and Vendor Fraud: By submitting fraudulent invoices and manipulating vendor information for her benefit, Crawford engaged in procurement and vendor fraud.   |
|    | Identity Theft, Data Breach and Impersonation: This is indirectly applicable since Crawford misused her authority and the college's financial systems to impersonate legitimate transactions for personal gain.                                    |
| 83 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This is evident from the defendants' actions of deceiving purchasers of Semisub securities about the company's business and operations, including its revenue and expenses. |
|    | Collusion and Conspiracy: The couple worked together over a decade-long scheme, demonstrating a collaborative effort to defraud investors.   |
|    | Asset Misappropriation: The misuse of funds raised from the sale of securities for personal use, such as luxury residences, cars, vacations, and personal credit card bills, falls under this category.  |
|    | Regulatory Evasion and Deception: They continued to sell securities in violation of states' orders, showing deliberate evasion of regulatory requirements.   |
| 84 | Asset Misappropriation: This applies directly as Smith embezzled funds from her employers, which is a clear case of stealing or misusing the company's assets.   |
| 85 | Asset Misappropriation: Since the Sharper couple embezzled funds directly from the Booster Club, using checks, wire transfers, and debit/credit cards for personal expenditures.   |
|    | Fraudulent Claims and Invoices: The submission of fraudulent applications for COVID-19 relief funds, with false information about revenues, payroll, and employment data.  |
|    | Tax Evasion and False Tax Claims: Anthony Sharper's failure to report the embezzled funds on the couple's joint tax returns constitutes tax evasion.   |
|    | Regulatory Evasion and Deception: By submitting fraudulent applications for federal COVID-19 relief funds, Anthony engaged in deception to evade regulatory scrutiny and requirements.   |

|    |  |
|----|--|
|    | <p>Identity Theft, Data Breach and Impersonation: Although not directly stated as identity theft, the act of submitting applications under false pretenses and using the Booster Club's and his CPA firm's names for fraudulent claims could be considered as impersonation within the context of financial fraud.</p> <p>Money Laundering: The process of obtaining COVID-19 relief funds under false pretenses and using them to cover up the theft from the Booster Club can be seen as an attempt to launder the proceeds of their initial crime, making it appear as legitimate income.</p>   |
| 86 | <p>Asset Misappropriation: Coday-Townes misused company funds by writing checks to pay off her personal credit cards instead of paying legitimate vendors.</p> <p>Fraudulent Claims and Invoices: By falsely indicating in the accounting database that the checks were made to vendors rather than her personal credit cards, Coday-Townes engaged in fraudulent claims.</p> <p>Forgery and Counterfeiting: Coday-Townes used the employer's signature stamp on checks to commit the fraud, which involves forgery.</p> <p>Payroll Fraud: Entering overtime hours for herself, despite being ineligible for overtime, constitutes payroll fraud.</p>  |
| 87 | <p>Asset Misappropriation: Pike embezzled over \$1.2 million from his employer over a 16-year period, which constitutes asset misappropriation.</p> <p>Fraudulent Claims and Invoices: Pike prepared and submitted fraudulent invoices to his employer on behalf of a fake temporary staffing company, Consumer Information Systems (CIS).</p> <p>Creation of Shell Company: Pike created a fake temporary staffing company, Consumer Information Systems (CIS), to facilitate his fraudulent scheme of submitting fake invoices.</p> <p>Forgery and Counterfeiting: Pike added approving initials of company personnel to the fraudulent invoices without their knowledge or consent, which involves forgery.</p> |
| 88 | <p>Asset Misappropriation: Sweeten misused her position as a bookkeeper to steal funds from her employer, including issuing company checks to herself and making personal purchases with the company credit card.</p> <p>Forgery and Counterfeiting: Sweeten forged checks and fraudulently endorsed them to herself, indicating the use of forgery in the scheme.</p>   |
| 89 | <p>Asset Misappropriation: Loconte misused company funds for personal expenses instead of paying employment taxes, including using business accounts for personal expenses such as vehicles, property taxes, household improvements, and golf memberships.</p> <p>Payroll Fraud: Loconte engaged in a scheme to defraud the union benefit funds and the IRS by underreporting overtime hours worked by employees and failing to make required payroll tax withholdings and payments.</p> <p>Payroll Tax Evasion: Loconte failed to collect and pay payroll taxes to the IRS, instead diverting those funds for personal expenses.</p>  |
| 90 | <p>Asset Misappropriation: Petrone misused Yale University funds by ordering and stealing millions of dollars of electronic hardware for personal gain.</p>  |

|    |   |
|----|---|
|    | Fraudulent Claims and Invoices: Petrone falsely represented the purchased electronic hardware as being for specified Yale Medical needs to justify the fraudulent transactions.   |
|    | Creation of Shell Company: Petrone used Maziv Entertainment LLC as a shell company to receive funds from the resale of stolen equipment.  |
|    | Tax Evasion and False Tax Claims: Petrone filed false federal tax returns for multiple years, claiming the costs of stolen equipment as business expenses and failing to file returns for other years, causing a loss to the U.S. Treasury.                     |
| 91 | Asset Misappropriation: Thumann embezzled rent payments, which were assets of the Albert Lea Housing and Redevelopment Authority, for her own personal use.   |
|    | Forgery and Counterfeiting: Altering payee information on payments made by check and money order constitutes forgery.   |
|    | Manipulation of Company Systems: Thumann manipulated the HRA's computer system to conceal her theft and prolong her fraudulent scheme.  |
| 92 | Asset Misappropriation: Laansma embezzled over \$1.8 million from her former employer, misusing the company's assets for personal expenditures.   |
|    | Fraudulent Claims and Invoices: Laansma falsely recorded personal expenditures as legitimate business expenses in the company's books, constituting fraudulent claims.  |
|    | Tax Evasion and False Tax Claims: She failed to report the embezzled income as earnings on her tax forms, indicating tax evasion and false tax claims   |
| 93 | Asset Misappropriation: Burke embezzled nearly \$1 million from the school corporation, which constitutes misappropriation of the company's assets.   |
|    | Fraudulent Claims and Invoices: Burke issued approximately 312 checks to herself from ACSC, falsely representing them as payments to an ACSC vendor.  |
|    | Forgery and Counterfeiting: Falsifying ACSC records to conceal the theft by making it appear that the payments were to a legitimate vendor involves forgery and counterfeiting.   |
|    | Tax Evasion and False Tax Claims: Burke willfully failed to report approximately \$225,381 in income derived from the scheme on her tax returns, which constitutes tax evasion.   |
| 94 | Asset Misappropriation: As Burke embezzled \$1.4 million from his employer by authorizing additional payroll payments to himself and writing checks to himself and his credit card company, this directly involves the theft or misuse of the company's assets. |
|    | Payroll Fraud: Burke's actions of authorizing additional payroll payments to himself clearly falls under payroll fraud, as he manipulated payroll systems to benefit personally.  |
|    | Tax Evasion and False Tax Claims: By failing to report \$1.2 million of his illegal income to the IRS and evading more than \$160,000 in federal taxes, Burke engaged in tax evasion and the submission of false tax claims.                                    |

|    |  |
|----|--|
| 95 | Asset Misappropriation: This is the primary action as Ahmed-Elkilani misappropriated more than \$430,000 in funds belonging to his former employer for his own personal use.   |
|    | Manipulation of company systems: He took advantage of his role and access to other employees' operator codes, as well as the company's membership accounts to create and execute false transactions.   |
|    | Fraudulent Claims and Invoices: The creation and execution of multiple false transactions to misappropriate funds could fall under this category.  |
|    | Identity Theft, Data Breach and Impersonation: By using other employees' operator codes, Ahmed-Elkilani engaged in a form of identity impersonation to facilitate his fraudulent activities.   |
| 96 | Asset Misappropriation: Lee embezzled company funds, directly misusing the company's assets for personal gain.   |
|    | Fraudulent Claims and Invoices: He disguised unauthorized transactions as payments to vendors, fabricating or altering invoices or claims to conceal the embezzlement.   |
|    | Manipulation of Company Systems: By falsifying information in the company's recordkeeping software, Lee manipulated internal systems to facilitate and conceal his fraudulent activities.  |
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Redirecting money from an existing line of credit to cover revenue shortfalls could be seen as manipulating financial statements to misrepresent the company's financial condition to stakeholders. |
| 97 | Asset Misappropriation: Stephanie D. Carper embezzled more than \$1.2 million from her employer, which directly involves the theft or misuse of the company's assets.  |
|    | Forgery and Counterfeiting: By filling in her own name on pre-signed checks intended for vendor payments, Carper engaged in forgery.   |
|    | Fraudulent Claims and Invoices: Carper wrote false explanations on bank deposit slips and the check registry to conceal her thefts, which involves creating or manipulating documents to support her fraudulent activities.  |
|    | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This might be applicable if her actions indirectly affected the financial statements through the misrepresentation of the company's financial health or activities                                  |
| 98 | Asset Misappropriation: This applies because Koch and Kangas embezzled money from Park Nicollet by falsifying the amount of work done, leading to unwarranted compensation. This directly involves stealing or misusing the company's assets.                              |
|    | Collusion and Conspiracy: The actions of Koch and Kangas in coordinating their efforts to embezzle funds from Park Nicollet and manipulate company records to hide unauthorized compensation clearly constitute collusion and conspiracy.                                  |
|    | Manipulation of company systems: Koch's actions of entering fraudulent hours and logging into the company network on behalf of Kangas to reset his computer password to conceal the fraud involves direct manipulation of company systems.                                 |
|    | Payroll fraud: Since the fraud involved Koch entering more than 8,500 weekday hours for Kangas for work he did not perform, leading to Kangas being paid for these hours, this directly constitutes payroll fraud.   |

|     |   |
|-----|---|
|     | Money laundering: The sequence of withdrawals and deposits made by Kangas and Koch, designed to evade the federal currency transaction reporting requirement, can be seen as an effort to launder the proceeds of their fraudulent scheme |
| 99  | Asset Misappropriation: Latoski misused corporate credit cards for personal expenses, which is a clear case of stealing or misusing the company's assets.   |
|     | Fraudulent Claims and Invoices: By creating false entries in the company's books to conceal her personal expenses as legitimate business expenses, she engaged in making fraudulent claims.   |
|     | Forgery and Counterfeiting: This could be inferred from her act of creating false entries in the company's records, which involves forging documents to support her fraudulent claims.  |
|     | Manipulation of Company Systems: Utilizing her position to manipulate the company's accounting systems to facilitate payment of the personal expenses charged to the corporate credit cards.  |
| 100 | Bribery and Corruption: Kennedy and his co-conspirators engaged in a scheme where they accepted bribes and kickbacks in exchange for favoring a vendor, which is a clear case of bribery and corruption.                                  |
|     | Collusion and Conspiracy: Kennedy conspired with Ewert, Nguyen, and others to defraud Cargill through a bribery and kickback scheme, indicating collusion and conspiracy.   |
|     | Procurement and Vendor Fraud: The scheme involved manipulating procurement processes to favor WDS, Inc., and concealing overcharges, which falls under procurement and vendor fraud   |
| 101 | Identity Theft, Data Breach and Impersonation: Rigsbee committed identity theft by falsely pretending to be the deceased customer's beneficiary, which involves impersonating another person to gain access to their financial assets.    |
|     | Asset Misappropriation: Rigsbee misappropriated over \$158,000 from bank customers' accounts, which is a direct misuse of the company's assets.   |
|     | Fraudulent Claims and Invoices: By creating a fraudulent request for distribution of assets from a transfer-on-death account, Rigsbee engaged in fraudulent activities involving false claims.  |
|     | Manipulation of Company Systems: The act of transferring funds from customer accounts to brokerage accounts he controlled and attempting to conceal these transfers indicates manipulation of company systems to facilitate his fraud.    |
| 102 | Asset Misappropriation: Ellis diverted funds from the non-profit's bank accounts to his own, which directly indicates the misuse or theft of the organization's assets.   |
|     | Fraudulent Claims and Invoices: Although not explicitly detailed, the diversion of funds might have involved creating or manipulating claims and invoices to justify the unauthorized transfer of money.                                  |
|     | Manipulation of Company Systems: To successfully divert funds over an extended period, Ellis likely manipulated the company's financial systems to hide his fraudulent activities.  |
| 103 | Asset Misappropriation: Hall's actions involve stealing or misusing the company's assets, in this case, the funds of elderly account holders at the credit union.   |
|     | Fraudulent Claims and Invoices: By creating fake loans and monthly loan statements, Hall is essentially fabricating financial transactions that did not actually occur.   |

|     |   |
|-----|---|
|     | <p>Forgery and Counterfeiting: The act of creating fake share loans in the names of relatives and friends involves forgery, as it requires the unauthorized creation of documents or signatures pretending to be real.</p> <p>Manipulation of Company Systems: Hall manipulated the credit union's financial systems to create nominee loans, transfer money across loans, and withdraw funds for personal use.</p> <p>Identity Theft, Data Breach and Impersonation: By creating loans in the names of relatives and friends without their consent, Hall is essentially committing identity theft.</p>   |
| 104 | <p>Identity Theft, Data Breach and Impersonation: Although not a direct case of identity theft, the act of stealing trade secrets involves unauthorized access to and use of proprietary information, which can be aligned with the broader implications of identity theft and data breach as it involves impersonation to a degree by unlawfully acquiring and using the company's intellectual property.</p> <p>Asset Misappropriation: Kim's act of copying and using Broadcom's files for the benefit of another employer directly leads to the misappropriation of Broadcom's assets, which in this case are the trade secrets and intellectual property.</p> <p>Collusion and Conspiracy: By using Broadcom's trade secrets to benefit his new employer, a potential competitor, there's an implication of collusion with the new employer to misuse Broadcom's confidential information.</p> <p>Regulatory Evasion and Deception: This action could be applicable in the broader sense that trade secret theft undermines the legal and regulatory frameworks that protect intellectual property and fair competition.</p> |
| 105 | <p>Asset Misappropriation: Bittner misused the company's credit card reservation system to divert funds to his personal accounts, which is a clear case of stealing or misusing the company's assets.</p> <p>Fraudulent Claims and Invoices: By initiating refunds for stays that actually occurred, Bittner created false claims to secure money that he was not entitled to.</p> <p>Manipulation of Company Systems: He exploited the electronic payment system to benefit personally, which involves manipulating the company's systems for fraudulent purposes.</p>   |
| 106 | <p>Asset Misappropriation: Welch used her position to fraudulently issue checks for her personal benefit, directly misusing company assets.</p> <p>Fraudulent Claims and Invoices: Issuing 341 fraudulent checks can be seen as making fraudulent claims against the company's accounts.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: By engaging in fraudulent activities that resulted in significant financial loss to the company, this could potentially involve misrepresentation in financial statements to cover up the fraud.</p> <p>Forgery and Counterfeiting: Writing fraudulent checks involves forgery, as it likely entailed the unauthorized signing or alteration of financial instruments.</p> <p>Manipulation of Company Systems: To issue these checks without detection over a prolonged period, Welch would have had to manipulate the company's accounting or financial systems.</p>  |
| 107 | <p>Asset Misappropriation: This is directly applicable because Ricker stole company assets (blank checks) and funds.</p>  |

|     |   |
|-----|---|
|     | <p>Fraudulent Claims and Invoices: Writing fraudulent checks can be considered under this category as it involves creating false financial documents to illegitimately gain funds.</p> <p>Forgery and Counterfeiting: Ricker forged the signature of the authorized employee, which directly fits this fraud action.</p> <p>Identity Theft, Data Breach and Impersonation: By forging the signature of the company's authorized signatory, Ricker essentially impersonated that employee to commit fraud.</p>   |
| 108 | <p>Asset Misappropriation: Lutamila stole \$610,000 from the credit union, clearly an act of misappropriating company assets.</p> <p>Manipulation of Company Systems: He misused his position and employment to illegally transfer money from internal operating accounts, indicating manipulation of the company's systems.</p> <p>Money Laundering: Lutamila transferred the stolen money to an E-Trade account he had opened at the beginning of the scheme and used it for personal gains, which falls under money laundering activities.</p>   |
| 109 | <p>Asset Misappropriation: Since Ronald Scott Miller embezzled funds from his employer, this directly involves the theft or misuse of the company's assets.</p> <p>Fraudulent Claims and Invoices : Miller submitted fraudulent invoices and false timesheets, which falls under creating illegitimate claims for payment.</p> <p>Forgery and Counterfeiting : By forging his partner's signature to deposit checks, Miller engaged in forgery.</p> <p>Procurement and Vendor Fraud : The creation of fake companies and submission of invoices for non-existent purchases aligns with procurement and vendor fraud.</p> <p>Payroll Fraud : Submitting false timesheets for himself, his partner, and inflating hours for his son constitute payroll fraud.</p> <p>Manipulation of company systems: By engaging in activities that falsely inflated expenses and created non-existent transactions, Miller was effectively manipulating financial records which could mislead investors or stakeholders about the company's financial health.</p> |
| 110 | <p>Asset Misappropriation: This is directly applicable as Phillip Brian Topping embezzled funds from an on-site ATM and a teller cash drawer, which involves the theft or misuse of the company's (credit union's) assets for personal use.</p>   |
| 111 | <p>Asset Misappropriation: This is evident from Pylant's embezzlement of funds from her employer, the trade association, through unauthorized check deposits and transfers, including forging checks.</p> <p>Forgery and Counterfeiting: Pylant forged the names of trade association executives on checks made payable to herself and others, which she then deposited into accounts she controlled.</p> <p>Manipulation of company systems: By establishing a non-existent entity (LPSR, Inc.) as a vendor in the trade association's computer system without proper registration or tax identification, Pylant manipulated company systems for her benefit.</p>  |



|     |   |
|-----|---|
|     | <p>Tax Evasion and False Tax Claims: Pylant engaged in multiple instances of tax evasion, including failing to report income from the trade association and SSDI payments, creating a fictitious entity to receive payments, and submitting false information in bankruptcy proceedings.</p> <p>Identity Theft, Data Breach and Impersonation: By forging the names of executives on checks and creating a fictitious company to receive payments, Pylant engaged in identity theft and impersonation.</p> <p>Regulatory Evasion and Deception: Through her actions, including the creation of a non-existent entity to funnel payments and the falsification of bankruptcy petitions, Pylant evaded regulatory oversight and engaged in deception.</p> <p>Creation of Shell Company: The manipulation of financial records and creation of fictitious entities likely impacted the financial statements of the trade association</p> |
| 112 | <p>Asset Misappropriation: Since the individual embezzled funds from the company's operating account for personal use.</p> <p>Fraudulent Claims and Invoices: By falsifying company accounting and financial records, including making false journal entries.</p> <p>Forgery and Counterfeiting: This can be inferred from the alteration of bank statements issued to the company.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: The falsification of accounting records and alteration of financial statements to conceal the embezzlement directly impacts the accuracy of financial statements presented to investors and stakeholders.</p>   |
| 113 | <p>Asset Misappropriation: Madison stole funds from WFYI by presenting fake claims and invoices, which is a direct misuse of the company's assets.</p> <p>Fraudulent Claims and Invoices: She presented at least 156 fake claims and invoices for payment, directly fitting this category.</p> <p>Collusion and Conspiracy: Madison conspired with Individual 1, who was not an employee or vendor of WFYI, to commit the fraud.</p> <p>Forgery and Counterfeiting: The falsification of invoices using versions of Individual 1's name and businesses implies forgery.</p>   |
| 114 | <p>Asset Misappropriation: Jones misused company funds by using company credit cards for unauthorized personal purchases and diverting customer revenue for personal use.</p> <p>Fraudulent Claims and Invoices: Setting up a business (KAB Enterprises, LLC) to issue false invoices to Guardian Retention Systems constitutes fraudulent claims and invoices.</p> <p>Creation of Shell Company: Jones established KAB Enterprises, LLC, which was used to issue false invoices and facilitate embezzlement.</p> <p>Forgery and Counterfeiting: While not explicitly mentioned, the creation of false invoices could involve forgery or counterfeiting</p>   |
| 115 | <p>Asset Misappropriation: Weston and his accomplice embezzled approximately \$6.8 million from Hillandale Farms, indicating the misuse of company assets for personal gain.</p>  |

|     |   |
|-----|---|
|     | <p>Money Laundering: Weston and VP laundered the stolen funds through businesses they controlled, using the money to purchase collectible cars, real estate, and other personal expenditures.</p> <p>Tax Evasion and False Tax Claims: Weston either failed to file or filed false federal personal income tax returns, underreporting income and evading taxes on the stolen money.</p> <p>Collusion and Conspiracy: The scheme to embezzle and launder money involved a conspiracy between Weston, his personal secretary, and the company bookkeeper.</p>  |
| 116 | <p>Asset Misappropriation: Cox's unauthorized creation of off-the-books bank accounts and diversion of client and company money fits this category.</p> <p>Fraudulent Claims and Invoices: This could be relevant if false representations to clients or vendors were made to solicit payments or investments.</p> <p>Manipulation of Company Systems: Creating unauthorized bank accounts and diverting funds could fall under this, given the systemic manipulation involved.</p> <p>Procurement and Vendor Fraud: If Cox's schemes involved fraudulent dealings with vendors or procurement processes, this would apply.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: Fabricated bank statements and false statements to a lender indicate manipulation of financial information.</p> <p>Money Laundering: The 11 counts of money laundering indicate that Cox was involved in the process of disguising the origins of illegally obtained money.</p> |
| 117 | <p>Asset Misappropriation: Garrett misused his employer's funds to make unauthorized purchases for personal gain.</p> <p>Fraudulent Claims and Invoices: He submitted false invoices for services never provided.</p> <p>Creation of Shell Company: Garrett used Garrett Ventures, a company he created, to facilitate his fraudulent activities.</p> <p>Manipulation of Company Systems: He entered false or altered information into his employer's accounting system to conceal his unauthorized purchases.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: By manipulating financial records, Garrett misrepresented the financial status of the company.</p> <p>Money Laundering: Garrett was sentenced for money laundering, indicating he engaged in processes to legitimize the proceeds of his fraud</p>   |
| 118 | <p>Collusion and Conspiracy: The coordination between Abouammo and officials of the Kingdom of Saudi Arabia to provide private user information in exchange for bribes indicates a planned conspiracy.</p> <p>Bribery and Corruption: Abouammo accepted bribes, including money and a luxury watch, from an official of the Kingdom of Saudi Arabia for performing actions that were against his duties at Twitter.</p> <p>Money laundering: Abouammo laundered the bribe money he received from the foreign official by transferring it into the United States in small wire transfers with false descriptions.</p>  |

|     |   |
|-----|---|
|     | Identity Theft, Data Breach and Impersonation: By accessing and conveying private information of Twitter users to the Saudi officials, Abouammo was involved in breaching the privacy and potentially the identity of Twitter users.  |
|     | Regulatory Evasion and Deception: By acting as a foreign agent without notice to the Attorney General and falsifying records in a federal investigation, Abouammo engaged in deceptive practices to evade regulatory oversight.   |
| 119 | Collusion and Conspiracy: Sacco conspired with a co-conspirator to defraud his employer and project owners by inflating change orders.  |
|     | Procurement and Vendor Fraud: The fraud involved inflating change orders on projects managed by Sacco, which is a form of procurement fraud.  |
|     | Bribery and Corruption: The co-conspirator subcontractor made payments for Sacco's personal benefits, which can be seen as a form of bribery.   |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Although not directly mentioned, the actions of using nonpublic financial information for personal gain can be seen as indirectly contributing to misleading investors about the market conditions of the company's stock, affecting investor decisions based on manipulated stock prices. |
|     | Manipulation of company systems: This is applicable because Levoff exploited his access to confidential and sensitive company information, which was part of the company's internal systems and controls, for personal gain.  |
| 121 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This action is directly relevant due to the false promises made to investors about extremely high returns based on the supposed imminent acquisition of Chandran's companies by a wealthy consortium, which was misleading.  |
|     | Asset Misappropriation: Since a substantial portion of the funds were misappropriated for purposes other than what was communicated to the investors, including personal benefit, this action applies.  |
|     | Fraudulent Claims and Invoices: This could be relevant if Chandran or his companies fabricated or inflated claims about the expenses or the operational costs to justify the use of investor funds.   |
|     | Identity Theft, Data Breach and Impersonation: The involvement of prominent business figures, including two billionaires, in the purchase (which did not happen), if falsely claimed, could also fall under impersonation to add credibility to the fraud.  |
|     | Money Laundering: Considering the misappropriated funds were used for purchasing luxury cars and real estate, there's a potential element of laundering money obtained from fraudulent activities.  |
| 122 | Collusion and Conspiracy: Daniel Thomas Broyles Sr.'s coordination with Niyato's CEO and others to defraud investors clearly indicates collusion and conspiracy to commit fraud.  |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: False portrayal of Niyato as an operational company engaged in electric vehicle manufacturing and the misleading representations made about EarthWater's business and the use of investor funds fall under this category.  |
|     | Money Laundering: Broyles pleaded guilty to money laundering charges, indicating that the proceeds from the fraud schemes were being laundered to appear as legitimate.   |

|     |  |
|-----|--|
|     | Identity Theft, Data Breach and Impersonation: Broyles's use of an alias to avoid detection by federal law enforcement indicates impersonation, a form of identity theft designed to evade legal consequences.   |
| 123 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: The scheme involved materially false and fraudulent misrepresentations to investors regarding the use of their funds, which is a direct form of investor fraud and misrepresentation.   |
|     | Collusion and Conspiracy: Barnes, Duchinsky, and their co-conspirators participated in a coordinated scheme to defraud investors, which fits the definition of collusion and conspiracy to commit fraud.   |
|     | Money Laundering: Barnes engaged in transactions involving the proceeds of the fraud, specifically to conceal the origin of the funds, which is a clear case of money laundering.  |
|     | Asset Misappropriation: Although not explicitly stated as misuse of company's assets, the fraudulent actions led to the personal benefit of the conspirators at the expense of the company and its investors, which can be considered a form of asset misappropriation since they diverted investor funds for personal gain. |
|     | Identity Theft, Data Breach and Impersonation: While not directly mentioned, the fraudulent mortgage loan application by DeGroot, using pay stubs fraudulently obtained, could fall under impersonation or misuse of identity information for financial gain.  |
| 124 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This is applicable due to the materially false and misleading representations and omissions made to prospective and existing investors regarding compensation, use of funds, and the status of potential acquisitions.                                |
|     | Asset Misappropriation: This applies because Dodson misappropriated \$1.3 million in investor funds for his own benefit, which includes repaying investors in an unrelated investment and covering personal expenses.  |
|     | Money Laundering: Given that Dodson pooled funds from the limited partnerships and conducted multiple transfers between related accounts to divert funds for his own benefit, this action helped him conceal the origins of the fraudulently obtained money, which aligns with money laundering practices.                   |
| 125 | Collusion and Conspiracy: Kurt Phelps and his conspirators clearly worked together to carry out the fraud scheme.  |
|     | Bribery and Corruption: Phelps accepted large cash bribes from his conspirators in exchange for assisting them with the fraudulent scheme.   |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: By providing materially false financial information to obtain and increase a line of credit, Phelps and his conspirators engaged in financial statement fraud.  |
|     | Procurement and Vendor Fraud: This could be relevant if the credit obtained was under the pretense of procurement needs for Starnet Business Solutions Inc., and involved manipulating the bank's processes for vendor selection and payment.  |
|     | Manipulation of company systems: Phelps helped Starnet avoid audits and other quality control measures, indicating manipulation of the bank's systems to prevent detection of the fraud.   |

|     |   |
|-----|---|
| 126 | <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: The CEO's actions of making false and misleading public statements about the procurement of COVID-19 test kits directly mislead investors, affecting their investment decisions based on incorrect company performance and prospects.</p> <p>Manipulation of Company Systems: By causing the company to issue multiple false public statements, the CEO manipulated the company's communication and disclosure systems to support the fraudulent scheme.</p> <p>Regulatory Evasion and Deception: By entering into an agreement based on the false pretense that the Supply Company had FDA permission to distribute COVID-19 tests in the U.S., and continuing to affirm the deal's validity despite contrary information, this involves evasion or deception related to regulatory compliance.</p>  |
| 127 | <p>Asset Misappropriation: Lucas misused the company's funds by not remitting the withheld employment taxes to the IRS as required by law.</p> <p>Payroll Fraud: The act of collecting withholdings from employees and failing to pay those funds to the IRS constitutes payroll fraud.</p> <p>Payroll Tax Evasion: By not paying the employment taxes withheld on behalf of the employees, Lucas engaged in payroll tax evasion.</p> <p>Regulatory Evasion and Deception: Lucas's actions also represent a deliberate attempt to evade regulatory requirements related to employment taxes.</p> <p>Tax Evasion and False Tax Claims: The failure to pay the full amount of taxes due to the IRS can be classified under tax evasion.</p>   |
| 128 | <p>Collusion and Conspiracy: The case involves a scheme where Matthew Clark conspired with others to receive kickbacks and engage in prohibited commodities transactions.</p> <p>Bribery and Corruption: The kickback scheme implies a form of bribery where Clark agreed to direct his employer's trades to a specific brokerage in exchange for personal gains.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: By causing prices to be reported that were not true, Clark and his co-conspirators engaged in activities that would mislead investors and affect financial statements.</p> <p>Regulatory Evasion and Deception: The involvement in illegal prearranged trades and the violation of provisions of the Commodity Exchange Act represent a clear attempt to evade regulatory laws and deceive oversight bodies.</p> <p>Money Laundering: The profits from these fraudulent trades potentially involve the process of concealing the origins of illegally obtained money, making it appear as if it originated from legitimate sources.</p> |
| 129 | <p>Asset Misappropriation :As Abbas misused government funds designated for a specific purpose for her own personal expenses, this constitutes a clear case of asset misappropriation.</p> <p>Fraudulent Claims and Invoices: Submitting or causing the submission of claims to receive funds for a home health agency that was not operational during the pandemic and was not providing the services those funds were intended for.</p> <p>Tax Evasion and False Tax Claims :This might be relevant if the misappropriated funds were not reported as income or were falsely claimed in a way that reduced tax liability improperly.</p>  |

|     |   |
|-----|---|
|     | Identity Theft, Data Breach and Impersonation :This could apply if any aspect of the fraud involved misrepresenting the identity of the health agency or its operational status to unlawfully gain access to the funds.   |
|     | Regulatory Evasion and Deception :By obtaining and misusing the funds under false pretenses, Abbas engaged in deceptive practices to evade regulatory requirements and oversight intended to ensure the proper use of those funds.  |
| 130 | Collusion and Conspiracy: The defendants conspired to fraudulently obtain loan guarantees from the SBA, which involved altering loan payment histories, renaming businesses, and hiding previous defaults.  |
|     | Regulatory Evasion and Deception: By fraudulently obtaining loan guarantees that did not meet the SBA’s guidelines and requirements, the defendants were engaging in deception to evade regulatory standards.   |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Altering loan payment histories and hiding the fact that borrowers had previously defaulted on loans involve manipulation of financial information to mislead investors or regulatory bodies.        |
|     | Procurement and Vendor Fraud: This could be applicable in the context of obtaining loan guarantees under false pretenses, as it involves misrepresenting the eligibility of the loans to the program designed to benefit small businesses.                                  |
| 131 | Collusion and Conspiracy: This is directly mentioned in the case, where the former employees and their co-conspirators colluded to allocate security services contracts and fix prices.   |
|     | Regulatory Evasion and Deception: The actions taken by the former employees to rig bids and fix prices could fall under attempts to evade regulations designed to ensure fair and competitive bidding processes.  |
|     | Procurement and Vendor Fraud: While not explicitly mentioned, the nature of conspiring to rig bids and allocate contracts involves elements of Procurement and Vendor Fraud to influence the outcome of contract awards, especially in cases involving government contracts |
| 132 | Asset Misappropriation: Although not directly mentioned, the scheme's nature suggests misuse of Medicare funds, which can be categorized under this when considering Medicare as an asset to be protected against fraud.  |
|     | Fraudulent Claims and Invoices: The submission of over \$784 million in false and fraudulent claims to Medicare directly aligns with this category.   |
|     | Creation of Shell Company: The use of shell companies in foreign countries for funneling kickbacks supports this fraud action.  |
|     | Bribery and Corruption: The solicitation of illegal kickbacks and bribes from DME suppliers and marketers in exchange for orders.   |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Falsely claiming to prospective investors about the revenue sources and amounts.   |
|     | Tax Evasion and False Tax Claims: Harry committed income tax evasion by not reporting income received through the fraud scheme.   |
|     | Regulatory Evasion and Deception: By structuring payments through shell companies and making false representations to regulators and investors, this type of fraud is implicated.   |

|     |   |
|-----|---|
|     | Money Laundering: The conspiracy to commit money laundering is explicitly charged, indicating the effort to conceal the origins of the illegally obtained money   |
| 133 | Bribery and Corruption: The scheme involved making bribe payments to Venezuelan officials to obtain contracts, directly aligning with the definition of bribery and corruption.   |
|     | Money Laundering: Wakil laundered funds related to the bribery scheme, clearly indicating the action of money laundering.   |
|     | Collusion and Conspiracy: The involvement in a scheme with others to bribe officials and launder money demonstrates collusion and conspiracy to commit fraud.   |
|     | Regulatory Evasion and Deception: By engaging in bribery and money laundering to secure contracts, Wakil was evading regulatory norms and engaging in deception   |
| 134 | Asset Misappropriation: Ray misused Center's funds for personal expenses, demonstrating a clear case of asset misappropriation.   |
|     | Fraudulent Claims and Invoices: By falsifying financial reports and creating incomplete lists of bills, Ray engaged in making fraudulent claims.  |
|     | Forgery and Counterfeiting: Issuing unauthorized checks and falsifying accounting records suggest activities akin to forgery.   |
|     | Manipulation of Company Systems: Ray manipulated Center's financial and accounting systems to hide her fraudulent activities.   |
|     | Payroll Fraud: Issuing additional payroll checks to herself indicates payroll fraud.  |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: Falsifying cash balances and financial accounting records to mislead the Board of Aldermen and possibly investors or stakeholders.   |
| 135 | Money laundering: Weinzierl and Waldstein were involved in a scheme to launder money through the U.S. financial system, involving the movement of funds through various banks and shell company accounts to disguise the origins and use of the money, primarily for paying bribes and evading taxes. |
|     | Creation of Shell Company: The indictment mentions the use of offshore shell company bank accounts secretly controlled by Odebrecht for funneling slush funds used to pay bribes, indicating the creation of shell companies as part of the scheme.   |
|     | Bribery and Corruption: The scheme involved paying hundreds of millions of dollars in bribes to public officials worldwide, directly implicating bribery and corruption as central elements of the fraud.   |
|     | Tax Evasion and False Tax Claims: Odebrecht engaged in fraudulent accounting practices, falsely recording international wire transfers as legitimate business expenses to reduce its taxable income and evade over \$100 million in taxes.  |
|     | Collusion and Conspiracy: Weinzierl, Waldstein, and their co-conspirators worked together with Odebrecht and others in a concerted effort to defraud Brazil's tax authority and to facilitate the payment of bribes, demonstrating collusion and conspiracy.  |

|     |   |
|-----|---|
| 136 | Bribery and Corruption: Halilov paid bribes to NGO officers in exchange for sensitive procurement information.  |
|     | Collusion and Conspiracy: Halilov coordinated a bid-rigging scheme with preferred companies and NGO officers.   |
|     | Procurement and Vendor Fraud: This fraud is evident in Halilov's manipulation of the procurement process to favor certain vendors.  |
|     | Regulatory Evasion and Deception: By engaging in bribery and bid-rigging, Halilov evaded the regulatory requirements meant to ensure a fair and competitive bidding process   |
| 137 | Fraudulent Claims and Invoices: The submission of fraudulent loan applications with falsified borrowers' information fits under this category.  |
|     | Forgery and Counterfeiting: Falsification of documents and material information about borrowers' qualifications implies forgery.  |
|     | Manipulation of Company Systems: The scheme involved manipulating the financial institution's loan origination process.   |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This is applicable due to the fraudulent representation of borrowers' financial information to secure loans.   |
|     | Money Laundering: The case explicitly mentions facilitating loans to borrowers involved in money laundering.  |
|     | Tax Evasion and False Tax Claims: Involved indirectly as part of the scheme to facilitate financial crimes, including tax evasion by borrowers  |
| 138 | Asset Misappropriation: Barry misused the campaign's funds by directing payments to himself beyond his salary, which is a classic example of asset misappropriation.  |
|     | Fraudulent Claims and Invoices: By causing the campaign to make excess payments to him, it can be inferred that Barry might have used or fabricated claims and invoices to justify these payments.  |
| 139 | Asset Misappropriation: This is a clear instance where the company's assets (in this case, checks intended for vendors) were misappropriated by the employee for personal use.  |
|     | Fraudulent Claims and Invoices: Although not explicitly mentioned, the act of diverting vendor checks could involve manipulation or creation of fraudulent claims or invoices to justify the checks being issued or rerouted.                                   |
|     | Procurement and Vendor Fraud: The fraud directly involves vendors by embezzling money intended for vendor payments, fitting the definition of procurement and vendor fraud.   |
|     | Forgery and Counterfeiting: This could be applicable if altering or creating fraudulent documentation was part of the scheme to redirect the checks to her account, although the case description does not specify forgery or counterfeiting actions explicitly |
| 140 | Fraudulent Claims and Invoices: By allegedly obtaining federal grant money through false statements regarding his affiliations and financial support from another source, this action seems to involve making fraudulent claims to secure funding.              |



|     |   |
|-----|---|
|     | Regulatory Evasion and Deception: By not disclosing his affiliations and financial support from a foreign government and university, the professor attempted to evade regulations and deceive the grant-awarding body, which requires transparency about funding sources  |
| 141 | <p>Fraudulent Claims and Invoices: Scott submitted invoices making it appear as though he were being paid for hourly marketing services, rather than per referral, to conceal illegal kickbacks.</p> <p>Collusion and Conspiracy: Scott was convicted of conspiracy to commit health care fraud and conspiracy to pay and receive unlawful health care kickbacks, indicating collusion and conspiracy in the fraudulent activities.</p> <p>Bribery and Corruption: Scott paid unlawful bribes and kickbacks to telemedicine companies to obtain doctor's orders authorizing the CGx tests.</p> <p>Regulatory Evasion and Deception: By falsely stating that Medicare covered expensive cancer screening genetic tests and involving telemedicine doctors in approving tests without proper medical justification, Scott engaged in regulatory evasion and deception.</p> <p>Procurement and Vendor Fraud: Scott's scheme involved manipulating the procurement process of genetic tests and doctor's orders, benefiting from kickbacks in the process</p> |
| 142 | <p>Tax Evasion and False Tax Claims: This is directly applicable as Brassart evaded paying his income tax by concealing his income and assets.</p> <p>Regulatory Evasion and Deception: Filing false bankruptcy petitions and making false statements in those petitions to discharge tax debt falls under attempts to evade regulatory oversight and deceive regulatory bodies.</p> <p>Asset Misappropriation : Although not directly mentioned, the use of nominee corporations to conceal ownership interests and assets can be considered a form of asset misappropriation, as it involves misusing the company's assets for personal benefit.</p> <p>Identity Theft, Data Breach and Impersonation : The use of nominee corporations to conceal his income and assets could also be seen as a form of impersonation, as it involves using entities to hide his true financial status</p>   |
| 143 | <p>Collusion and Conspiracy: Heredia conspired with other employees to manipulate the price of fuel oil, indicating a collaborative effort to engage in fraudulent activities.</p> <p>Regulatory Evasion and Deception: The manipulation of commodity prices to create artificial prices undermines regulatory standards meant to ensure fair market practices.</p> <p>Financial Statement Fraud or the Investor Fraud and Misrepresentation: By manipulating the price of fuel oil, the financial statements of Company A and Company B would likely reflect artificial profits or losses, misleading investors and stakeholders.</p>  |
| 144 | <p>Collusion and Conspiracy: This is evident from the coordinated actions between the individual and co-conspirators to manipulate contracts in exchange for bribes.</p> <p>Bribery and Corruption: The acceptance of bribes in exchange for business favors directly points to this type of fraud.</p>   |

|     |  |
|-----|--|
|     | Money laundering: The process of disguising the origins of the bribe money through various intermediaries and transactions, including some that involved the United States, fits the definition of money laundering  |
| 145 | Collusion and Conspiracy: The involvement in a conspiracy to commit health care fraud and to pay kickbacks and bribes.   |
|     | Bribery and Corruption: Paying kickbacks and bribes to customers to influence their decisions.   |
|     | Fraudulent Claims and Invoices: Billing Medicare and Medicaid for expensive prescription drugs that were not eligible for reimbursement.   |
|     | Asset Misappropriation: The unlawful spending of the proceeds of his fraud, including wiring money to pay for a luxury car.  |
|     | Regulatory Evasion and Deception: Engaging in activities to deceive regulatory bodies by making ineligible claims for reimbursement  |
| 146 | Asset Misappropriation: While not directly involving the theft or misuse of company assets, the scheme resulted in the misappropriation of Medicare funds, which can be seen as indirectly involving asset misappropriation due to the fraudulent acquisition of government funds. |
|     | Fraudulent Claims and Invoices: The administration of unnecessary back injections in exchange for opioid prescriptions involved submitting fraudulent claims to Medicare for procedures that were medically unnecessary.   |
|     | Manipulation of Company Systems: The development and approval of a corporate policy that intentionally defrauded Medicare by submitting claims for unnecessary procedures indicates manipulation of company systems for fraudulent purposes.                                       |
|     | Procurement and Vendor Fraud: Although not involving traditional vendors, the scheme essentially treated Medicare as a 'vendor' being defrauded through false claims for unnecessary medical procedures.   |
|     | Collusion and Conspiracy: Rashid and 21 other defendants, including 12 physicians, conspired to commit healthcare fraud, indicating a coordinated effort to defraud Medicare.  |
|     | Bribery and Corruption: Rashid incentivized physicians to disregard patient care in pursuit of money, essentially bribing them to participate in the fraud scheme by offering to split Medicare reimbursements   |
|     | Regulatory Evasion and Deception: The entire scheme was designed to evade healthcare regulations by performing unnecessary procedures and exploiting Medicare's reimbursement system.  |
|     | Money Laundering: Rashid was convicted of money laundering, which involved the processing of proceeds from the healthcare fraud scheme to make them appear legitimate  |
| 147 | Payroll Fraud: This involves fraudulent actions related to the handling of the payroll system, which in this case includes not paying employment taxes as required.  |
|     | Payroll Tax Evasion: This specifically relates to the deliberate failure to pay taxes owed on employee wages, which is a central element of the case described.  |
|     | Regulatory Evasion and Deception: This pertains to actions taken to evade regulatory requirements, including the failure to file required tax returns and payments   |

|     |  |
|-----|--|
| 148 | Asset Misappropriation: Devillez misused the company funds for personal use, which is a direct theft of company assets.  |
|     | Fraudulent Claims and Invoices: By falsifying records to reflect full payment to vendors when partial or no payments were made.  |
|     | Manipulation of Company Systems: By altering company records to hide the unauthorized transfers.   |
|     | Procurement and Vendor Fraud: As the fraudulent activity involves the manipulation of vendor payments  |
| 149 | Forgery and Counterfeiting: This directly applies to the act of forging prescriptions to obtain controlled substances.   |
|     | Identity Theft, Data Breach and Impersonation: The employees impersonated the physician or misused the physician's identity to create fake prescriptions.  |
|     | Collusion and Conspiracy: The act of working together to forge prescriptions and distribute controlled substances indicates a planned conspiracy between the two individuals   |
| 150 | Asset Misappropriation: Mercedes misused her employer's assets by fraudulently transferring money from the company to accounts controlled by her relatives, friends, or associates.  |
|     | Manipulation of Company Systems: She exploited the company's computer system to facilitate the fraudulent wire transfers.  |
|     | Identity Theft, Data Breach and Impersonation: Mercedes used her family members' and friends' identities to open fraudulent accounts and impersonated a co-worker to approve the transfers.  |
|     | Money Laundering: The stolen funds were laundered through bank accounts and reloadable debit/credit accounts before being used for personal expenses   |
| 151 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: The executives engaged in a scheme to mislead shareholders, auditors, lenders, regulators, and the investing public about the company's financial condition, involving sham accounting entries, misstated accounts, and fraudulent inflation of financial performance.  |
|     | Manipulation of Company Systems: The scheme included delaying recognizing expenses, misstating accounts, and "cushion" accounting to fraudulently inflate the company's financial performance.   |
|     | Collusion and Conspiracy: The indictment charges the executives with conspiracy to make false statements to accountants and to falsify the company's books, records, and accounts, indicating a collaborative effort to commit fraud.  |
|     | Asset Misappropriation: Although not explicitly mentioned as stealing or misuse of company assets in the traditional sense (like theft of physical assets), the manipulation of financial records to overstate assets and understate liabilities indirectly leads to misappropriation of shareholder value and could be considered under this category due to the broad impact on the company's assets |
| 152 | Asset Misappropriation: Moreland is alleged to have embezzled cash from the Davidson County Drug Court Foundation, which directly involves the theft or misuse of the organization's assets for personal gain.   |
|     | Collusion and Conspiracy: The act of directing the Drug Court Foundation's director to deliver envelopes of cash to his office in exchange for allowing her to increase her compensation involves a collaborative effort to defraud, indicating collusion and conspiracy.  |

|     |   |
|-----|---|
|     | Bribery and Corruption: The scheme implies that Moreland abused his official position for personal benefit, which is indicative of corruption. The exchange of cash for favorable treatment (allowing the director to increase her compensation) also suggests bribery.   |
| 153 | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This applies because the case involves TBW's engagement in a fraudulent scheme that affected its financial statements, which were then audited and inaccurately reported by Deloitte & Touche LLP. The failure to detect and report TBW's severe financial distress and fraudulent activities directly relates to the misrepresentation of financial statements. |
|     | Fraudulent Claims and Invoices: TBW's purported sale of fictitious or double-pledged mortgage loans can be classified under fraudulent claims and invoices, as these actions involve making false claims to the government for FHA-insured loans.   |
|     | Asset Misappropriation: Given that TBW was engaged in a scheme that involved the sale of fictitious or double-pledged mortgage loans, this can also be seen as a misuse or theft of company assets or assets under their control, which were then misrepresented in their financial statements.   |
|     | Regulatory Evasion and Deception: TBW's failure to comply with HUD requirements, coupled with Deloitte's failure to detect this non-compliance, falls under regulatory evasion and deception. This action involved evading the regulatory framework designed to prevent such fraudulent activities.   |
|     | Collusion and Conspiracy: The sustained failure of Deloitte to detect and report TBW's fraudulent activities over several years suggests a potential collusion or lack of due diligence that enabled TBW's fraudulent scheme to continue, implicating a form of conspiracy or collusion in failing to uncover the fraud   |
| 154 | Forgery and Counterfeiting: Calaiaro wrote checks to himself by forging the signature of a partner from the firm, which directly involves the creation of fraudulent documents or signatures.   |
|     | Asset Misappropriation: Calaiaro misused the firm's assets (in this case, funds) for his own personal use, which falls under the misuse or theft of company's assets  |
| 155 | Asset Misappropriation: Hauk embezzled funds from his firm's clients for personal use, which directly aligns with the misuse or theft of company's assets.  |
|     | Forgery and Counterfeiting: He forged a victim's signature to endorse fraudulent checks.  |
|     | Manipulation of company systems: Hauk created false accounting entries to conceal his theft, demonstrating manipulation of the company's accounting system.   |
|     | Money laundering: He laundered the embezzled funds through purchases of luxury vehicles and other high-value items, then used companies he created to wash the proceeds.  |
|     | Financial Statement Fraud or the Investor Fraud and Misrepresentation: This is indicated by Hauk's creation of false accounting entries and false representations to banks and other entities to secure loans and purchase luxury items.  |
|     | Identity Theft, Data Breach and Impersonation: Hauk stole the identity of at least one victim to further his fraud schemes.   |
| 156 | Collusion and Conspiracy: Polos and Glover conspired to conceal their ownership and employment at the adult entertainment establishment from federal authorities, specifically on national security forms.  |

|     |  |
|-----|--|
|     | Regulatory Evasion and Deception: By not disclosing their involvement with the club, which was known to have activities related to drug use and sales, they evaded regulatory oversight related to their suitability for holding positions with access to classified information.  |
|     | Bribery and Corruption: Although not explicitly mentioned, their positions within the DEA and their undisclosed involvement with a business potentially connected to criminal activities suggest a risk of corruption and the possibility of being bribed due to their dual roles. |
| 157 | Identity Theft, Data Breach and Impersonation: The scheme involved the unauthorized access and download of credit reports, leading to the assumption of victims' identities by others.   |
|     | Collusion and Conspiracy: The operation required coordination between multiple parties, including Cummings, his co-conspirator (CW), and others who bought the credit reports.   |
|     | Regulatory Evasion and Deception: The use of confidential passwords and codes to access consumer credit information without authorization involves evasion of legal and regulatory frameworks designed to protect consumer data.   |
|     | Manipulation of Company Systems: The scheme exploited the computerized systems of Teledata Communications Inc. and the credit bureaus to obtain unauthorized access to consumer credit reports   |

APPENDIX D:  
ANALYSIS OF OPPORTUNITIES

| Case | Analysis Data  |
|------|--|
| 1    | 1. Position of Trust & Authority: Stollery's role as CEO allowed him to control investor funds.  |
|      | 2. Lack of Segregation of Duties: Insufficient checks and balances enabled fund misappropriation.  |
|      | 3. Poor Accounting system: Falsified white papers and financial information.   |
|      | 4. Poor monitoring and security of personal data: Planted fake testimonials.   |
| 2    | Position of Trust & Authority: As mayor, Pérez-Otero held a position of substantial authority, enabling him to manipulate contracts.                       |
|      | Lack of Segregation of Duties: His ability to both secure contracts and ensure prompt payment indicates a lack of segregation in duties.                   |
|      | Poor Audit Performance and Management Oversight: The prolonged nature of the scheme suggests inadequate audit performance and oversight in the management. |
|      | Lack of Systems of Authorization: The ease with which he could expedite payments indicates a lack of robust systems for authorization.                     |
| 3    | Position of Trust & Authority: As CFO, Firlé was in a position of authority, facilitating his embezzlement.  |
|      | Lack of Segregation of Duties: He had the ability to carry out various financial transactions without checks.  |
|      | Poor Audit Performance and Management Oversight: The prolonged embezzlement indicates inadequate auditing and oversight.                                   |
|      | Lack of Systems of Authorization: The ability to make unauthorized wire transfers and issue checks points to a lack of proper authorization systems.       |
| 4    | Position of Trust & Authority: As the Director of Finance, Murray had direct access to financial resources and information.                                |
|      | Lack of Segregation of Duties: She was able to execute transactions without adequate oversight.  |

|   |  |
|---|--|
|   | Poor Audit Performance and Management Oversight: The duration of the embezzlement scheme suggests insufficient auditing and management attention.            |
|   | Lack of Systems of Authorization: The ease with which she executed unauthorized transactions shows a lack of robust authorization systems.                   |
| 5 | Position of Trust & Authority: Hickman and Whiteman's roles as Sales Manager and Assistant Sales Manager provided them the opportunity to execute the fraud. |
|   | Lack of Segregation of Duties: Their overlapping roles in sales and inventory management enabled the fraud.  |
|   | Poor Audit Performance and Management Oversight: The failure to detect unusual sales activities or inventory discrepancies indicates poor oversight.         |
|   | Lack of Systems of Authorization: The ability to conduct transactions without adequate checks or balances facilitated the fraud.                             |
| 6 | Position of Trust & Authority: Peterson's ability to embezzle funds indicates a position of trust within the organization.                                   |
|   | Lack of Segregation of Duties: The prolonged embezzlement suggests that duties were not adequately segregated, allowing the misuse of funds.                 |
|   | Poor Audit Performance and Management Oversight: The duration and scale of the theft indicate ineffective auditing and managerial oversight.                 |
|   | Lack of Systems of Authorization: The ability to misappropriate funds over an extended period suggests a lack of effective authorization systems in place.   |
| 7 | Position of Trust & Authority: Arnold's role as an accountant gave him access to financial resources.  |
|   | Lack of Segregation of Duties: Ability to create and authorize fraudulent transactions.  |
|   | Poor Audit Performance and Management Oversight: Ineffective auditing allowed the scheme to continue for years.  |
|   | Lack of Systems of Authorization: Insufficient controls on financial transactions.   |
| 8 | Position of Trust & Authority: As a surgeon, Payne's position allowed him to exploit the system.   |
|   | Lack of Independent Checks and Control of the Accounting System: This enabled the masking of bribes as legitimate payments.                                  |
|   | Poor Monitoring and Security of Personal Data: A lack of oversight in handling patients' referrals and surgeries.  |

|    |  |
|----|--|
| 9  | Position of Trust & Authority: Figg's role provided him direct access to bank records and accounts.  |
|    | Lack of Segregation of Duties: Ability to manipulate accounts and loans without checks.  |
|    | Poor Monitoring and Security of Personal Data: Insufficient oversight of Figg's activities with customer data.                                       |
|    | Lack of independent checks and control of the accounting system: Figg's prolonged embezzlement indicates a lack of effective monitoring.             |
|    | Lack of Physical and Digital Access Controls: Figg's ability to access and manipulate customer accounts and loan information.                        |
|    | Poor Audit performance and Management oversight: The fraud continued for several years, suggesting ineffective auditing and lack of regular reviews. |
| 10 | Position of Trust & Authority: As a branch manager, Cherry had direct access to the bank's vault and financial assets.                               |
|    | Lack of Physical and Digital Access Controls: Insufficient controls over cash access enabled the embezzlement.                                       |
|    | Absence of Cash Reconciliation and Surprise Checks on Cash: Lack of regular and unannounced audits contributed to the undetected theft.              |
|    | Poor Monitoring and Security of Personal Data: The bank's system failed to detect unusual activities in cash handling by Cherry.                     |
| 11 | Position of Trust & Authority: Dinoto abused her trusted position to manipulate financial records.   |
|    | Lack of Segregation of Duties: She had control over both recording and executing financial transactions.   |
|    | Poor Audit Performance and Management Oversight: The long duration of fraud indicates weak audit and oversight mechanisms.                           |
|    | Poor Control of Signed Cheques: The ability to forge checks suggests inadequate controls.  |
|    | Hiring without Background Checks: Not detecting the use of a fake Social Security number for employment.   |
|    | Poor Payroll management: The company failed to adequately monitor and review inflated payroll.   |
| 12 | Position of Trust & Authority: Lindberg's control over the companies provided him the opportunity to manipulate funds.                               |
|    | Lack of Segregation of Duties: His ability to direct funds for personal use suggests a lack of duty segregation.                                     |



|    |   |
|----|---|
|    | Poor Audit Performance and Management Oversight: The scheme's duration suggests poor audit and oversight practices.                                 |
| 13 | Position of Trust & Authority: As a bookkeeper, she had direct access to financial records.   |
|    | Lack of Segregation of Duties: Control over payroll and invoice payments without oversight.   |
|    | Lack of independent checks and control of the accounting system: No effective checks on her activities.   |
|    | Poor Audit Performance and Management Oversight: The ongoing fraud suggests poor auditing and management oversight.                                 |
|    | Hiring without Background Checks: Hiring Burley without adequate background checks, especially post her termination for similar misconduct.         |
| 14 | Position of Trust & Authority: Collins's role as financial secretary provided her with the authority to access and manipulate funds.                |
|    | Lack of Segregation of Duties: She managed various financial aspects, allowing her to conduct unauthorized transactions without detection.          |
|    | Poor Audit Performance and Management Oversight: The duration and scale of the embezzlement indicate poor auditing and managerial oversight.        |
|    | Lack of Systems of Authorization: The ability to use church credit cards for personal expenses points to a lack of proper authorization mechanisms. |
| 15 | Position of Trust & Authority: The status of Dooling and Anderson as former NBA players gave them credibility to recruit others.                    |
|    | Lack of Systems of Authorization: The Plan lacked robust systems to authenticate the legitimacy of claims.  |
|    | Poor Monitoring and Security of Personal Data: Inadequate verification of the authenticity of the medical records submitted.                        |
|    | Absence of Cash Reconciliation and Surprise Checks: Lack of thorough checking of the validity of claims against actual services rendered.           |
|    | Lack of Segregation of Duties: The process for claims submission and approval likely lacked sufficient checks and balances.                         |
| 16 | Position of Trust & Authority: Tischer's role as trustee gave her direct access and control over the funds.   |

|    |  |
|----|--|
|    | Lack of Segregation of Duties: She had unchecked authority to withdraw and spend the trust's money.                                      |
|    | Poor Monitoring and Security of Personal Data: Her ability to forge ledger entries indicates poor monitoring.                            |
|    | Lack of Systems of Authorization: The ease with which she misappropriated funds suggests a lack of proper authorization systems.         |
| 17 | Position of Trust & Authority: His position allowed him to influence contract decisions unduly.  |
|    | Lack of Segregation of Duties: Being able to both establish and ensure hospital contracts with MES indicates a lack of duty segregation. |
|    | Poor Procurement Policies: Ineffective policies that allowed the hospital to contract with an employee-owned company.                    |
|    | Lack of Systems of Authorization: Ineffective verification and authorization of the contractual relationship with MES.                   |
|    | Poor Audit performance and Management oversight: Inadequate monitoring of financial transactions and contract fulfillment.               |
| 18 | Position of Trust & Authority: Suni Munshani's role as CEO allowed him to manipulate company funds.                                      |
|    | Lack of Segregation of Duties: The CEO's ability to direct funds without adequate oversight.   |
|    | Poor Audit Performance and Management Oversight: The scheme's success over several years indicates poor audit processes.                 |
|    | Lack of Systems of Authorization: The misuse of company funds without proper authorization systems in place.                             |
|    | Poor Control of Signed Cheques: The ability to transfer large sums to a fake company suggests poor control over financial instruments.   |
| 19 | Position of Trust & Authority: Carson's role as business manager enabled her control over funds.   |
|    | Lack of Segregation of Duties: She had sole responsibility for financial transactions.   |
|    | Poor Audit Performance and Management Oversight: The scheme's longevity suggests inadequate auditing.                                    |
|    | Lack of Systems of Authorization: The ease of transferring funds indicates a lack of strict authorization protocols.                     |
|    | Poor Accounting system: False entries in the database went unchecked.  |

|    |  |
|----|--|
| 20 | Position of Trust & Authority: As the founder and operator of EminiFX, Alexandre held a position of authority that he exploited.                           |
|    | Lack of Segregation of Duties: His ability to handle investments and financial transactions without oversight reflects a lack of duty segregation.         |
|    | Poor Audit Performance and Management Oversight: The failure to detect the fraudulent activities suggests poor auditing and oversight practices.           |
|    | Lack of Systems of Authorization: The misuse of investor funds without proper authorization systems being in place.  |
| 21 | Position of Trust & Authority: Ryan's role as CEO provided him the authority to manipulate information.  |
|    | Lack of independent checks and control of the accounting system: Insufficient checks allowed the perpetuation of fraud.                                    |
|    | Poor Audit Performance and Management Oversight: Ineffective audits enabled the concealment of the bank's true financial condition.                        |
|    | Lack of Systems of Authorization: Ineffective systems to properly authorize and review transactions.   |
|    | Poor Control of Signed Cheques: Potential mismanagement in the authorization of financial transactions.  |
| 22 | Position of Trust & Authority: As the business owner and manager, Downey had significant control, enabling her fraudulent activities.                      |
|    | Lack of Segregation of Duties: She could manipulate financial transactions, indicating a lack of duty segregation.   |
|    | Poor Audit Performance and Management Oversight: The duration of the fraud suggests inadequate auditing and management oversight.                          |
|    | Lack of Systems of Authorization: Downey's ability to overpay herself and make unauthorized transactions points to a lack of proper authorization systems. |
| 23 | Position of Trust & Authority: As the operations manager, Owens-Sharp was in a key position to exploit her access to payroll processes.                    |
|    | Lack of Segregation of Duties: Her role allowed her to both request and alter checks, highlighting a lack of checks and balances.                          |
|    | Poor Audit Performance and Management Oversight: The prolonged fraudulent activity indicates weak audit practices and poor management oversight.           |

|    |  |
|----|--|
|    | Lack of Systems of Authorization: The unauthorized salary increase and check alterations demonstrate a failure in authorization protocols.                             |
|    | Poor Payroll Management: Ineffective management of payroll processes enabled the fraud.  |
| 24 | Position of Trust & Authority: Both Woodson and Thompson held positions that allowed them to access and manipulate city funds.   |
|    | Lack of Segregation of Duties: Their ability to issue checks to themselves suggests a significant lack of segregation of duties.                                       |
|    | Poor Audit Performance and Management Oversight: The fact that this activity went undetected for years indicates poor audit and oversight practices.                   |
|    | Poor Control of Signed Cheques: The ability to forge signatures and issue checks without detection points to poor control over cheque signing processes.               |
| 25 | Position of Trust & Authority: As a multi-service banker, Tigler was in a position to manipulate client accounts.  |
|    | Lack of Segregation of Duties: Her role allowed her to access, forge, and cash checks, indicating insufficient segregation of duties.                                  |
|    | Poor Monitoring and Security of Personal Data: Tigler's access to and misuse of client information suggest inadequate data security.                                   |
|    | Poor Control of Signed Cheques: The ability to forge signatures and cash checks highlights weak controls over cheque handling.   |
| 26 | Position of Trust & Authority: Rivero's role as an investment advisor gave him access to and control over client funds.  |
|    | Lack of Segregation of Duties: The ability to manage and divert funds suggests inadequate segregation of duties within the firm.                                       |
|    | Lack of Independent Checks and Control of the Accounting System: The duration of the fraud indicates a lack of effective checks and balances in the accounting system. |
|    | Poor Monitoring and Security of Personal Data: Rivero's access to and misuse of client information points to poor monitoring and data security.                        |
| 27 | Position of Trust & Authority: Sharp's role as a senior developer gave him the necessary access to carry out the fraud.  |

|    |  |
|----|--|
|    | Lack of Physical and Digital Access Controls: Inadequate control over sensitive data and network access enabled the theft.   |
|    | Poor monitoring and security of personal data: The company's failure to monitor data access and usage allowed Sharp to exploit its resources.                              |
| 28 | Position of Trust & Authority: Chabaud's role as an accountant provided her with access and knowledge to exploit.  |
|    | Lack of Physical and Digital Access Controls: Continued access to bank accounts post-termination shows a lack of secure access controls.                                   |
|    | Poor Monitoring and Security of Personal Data: The prolonged unauthorized access indicates a lack of monitoring and security over sensitive financial data.                |
| 29 | Position of Trust & Authority: Girardi's status and authority in the law firm provided him the opportunity to manipulate settlements.                                      |
|    | Lack of Segregation of Duties: The ability of Girardi and Kamon to directly control client funds indicates a failure to segregate duties adequately.                       |
|    | Poor Audit Performance and Management Oversight: The duration of the fraud suggests poor audit practices and management oversight.   |
|    | Lack of Systems of Authorization: The ability to transfer and misappropriate large amounts of money without detection points to a lack of effective authorization systems. |
| 30 | Position of Trust & Authority: As a manager and CEO, Cory had significant control over company finances.   |
|    | Lack of Segregation of Duties: His ability to redirect funds without oversight points to a lack of duty segregation.   |
|    | Poor Audit Performance and Management Oversight: The undetected fraudulent activities suggest inadequate auditing and oversight.   |
|    | Lack of Systems of Authorization: Cory's ability to fabricate services and redirect funds indicates a lack of effective authorization systems.                             |
| 31 | Position of Trust & Authority: As CFO, Bowker had significant control over financial transactions, enabling his fraud.   |
|    | Lack of Segregation of Duties: He managed tax withholdings and payments, indicating a lack of duty segregation.  |
|    | Poor Audit Performance and Management Oversight: The prolonged undetected embezzlement and tax evasion suggest poor auditing and oversight.                                |

|    |  |
|----|--|
|    | Lack of Systems of Authorization: His ability to unilaterally authorize payments reflects a lack of robust authorization systems.                |
|    | Poor Control of Signed Cheques: Successfully bypassing the two-signature requirement on checks shows poor control in check management.           |
| 32 | Position of Trust & Authority: Dunican's role as CEO provided the opportunity to misrepresent business opportunities.                            |
|    | Lack of Segregation of Duties: The ability to transfer large sums to personal accounts indicates poor segregation of financial responsibilities. |
|    | Poor Audit Performance and Management Oversight: The fraud went undetected, pointing to weak audit and oversight functions.                      |
|    | Lack of Systems of Authorization: The absence of robust authorization systems facilitated the unauthorized transfer of funds.                    |
| 33 | Position of Trust & Authority: As an executive chairman and managing partner, Dodson had significant authority to influence investor decisions.  |
|    | Lack of Segregation of Duties: His control over various critical functions facilitated the fraud.  |
|    | Poor Audit Performance and Management Oversight: The prolonged duration of the fraud suggests inadequate auditing and oversight.                 |
|    | Lack of Systems of Authorization: Dodson's ability to misappropriate funds indicates a lack of effective authorization systems in place.         |
| 34 | Position of Trust & Authority: Bernardi's role as CEO provided him the authority to manipulate company information.                              |
|    | Lack of Independent Checks and Control of the Accounting System: The ability to fabricate financial statements indicates inadequate checks.      |
|    | Poor Audit Performance and Management Oversight: The use of false audit materials suggests poor audit performance and oversight.                 |
|    | Lack of Systems of Authorization: The fabrication of legal letters and financial documents indicates a lack of authorization systems.            |
| 35 | Position of Trust & Authority: Jackson's role gave her direct access to cash and control over accounts.  |

|    |   |
|----|---|
|    | Lack of Segregation of Duties: Her ability to manipulate accounts and vault access without checks indicates inadequate segregation of duties.                     |
|    | Poor Audit Performance and Management Oversight: The prolonged period of embezzlement implies ineffective auditing and oversight.                                 |
|    | Lack of Systems of Authorization: The unauthorized opening of credit lines and fund transfers suggests a lack of robust authorization systems.                    |
| 36 | Position of Trust & Authority: Her role as an accounts payable clerk gave her access to manipulate financial transactions.  |
|    | Lack of Segregation of Duties: Her role allowed her to both create and approve financial transactions.  |
|    | Poor Audit Performance and Management Oversight: The prolonged undetected fraud suggests poor auditing and oversight.   |
|    | Lack of Systems of Authorization: The ability to make unauthorized transactions indicates weak authorization systems.   |
| 37 | Position of Trust & Authority: Briggs abused her position at the bank to access and misuse customer information.  |
|    | Lack of Segregation of Duties: Her ability to access customer data without oversight indicates poor segregation of duties.  |
|    | Poor Monitoring and Security of Personal Data: The fraud highlights weaknesses in monitoring and securing customer data.  |
|    | Lack of Physical and Digital Access Controls: Allowing an employee to access and misuse customer data without detection.  |
|    | Lack of independent checks and control of the accounting system: Insufficient monitoring of employee activities, leading to the exploitation of internal systems. |
| 38 | Position of Trust & Authority: Stephens' position allowed him to influence the bidding process.   |
|    | Lack of Segregation of Duties: There appears to be a lack of separation in duties that would prevent bid-rigging.   |
|    | Poor Audit Performance and Management Oversight: The duration and scale of the scheme indicate poor audit performance and inadequate management oversight.        |
|    | Lack of Systems of Authorization: The ability to manipulate bids suggests a lack of proper systems for authorizing and overseeing contract bids.                  |

|    |   |
|----|---|
|    | Poor Procurement policies: The successful manipulation of contract bids points to a lack of effective oversight mechanisms.           |
| 39 | Position of Trust & Authority: As CEO, Slingerland had significant authority and control over the organization's finances.            |
|    | Poor Payroll management: Inflated payroll payments to self indicate poor payroll system.  |
|    | Poor Audit Performance and Management Oversight: Extended period of undetected fraud indicates poor audit performance.                |
|    | Lack of Systems of Authorization: The ability to misuse funds without detection suggests a lack of robust authorization systems.      |
|    | Poor Accounting system: The organization failed to effectively monitor and reconcile expenditures.                                    |
| 40 | Position of Trust & Authority: As payroll manager, Maurello had authority over payroll processing, which he exploited.                |
|    | Lack of Segregation of Duties: He was able to execute and conceal his fraudulent activities due to a lack of oversight in his role.   |
|    | Poor Audit Performance and Management Oversight: The fraud's duration indicates ineffective auditing and management oversight.        |
|    | Lack of Systems of Authorization: The ability to redirect payments and alter records suggests inadequate authorization systems.       |
|    | Poor Payroll management: Failure in reconciling payroll records allowed the fraud to go undetected.                                   |
|    | Poor Accounting system: Ability to alter payroll accounting records without detection indicates weak data integrity measures.         |
| 41 | Position of Trust & Authority: Little's role gave her access to reimbursement systems.  |
|    | Lack of Physical and Digital Access Controls: Continued access to the reimbursement platform even after termination.                  |
|    | Poor Monitoring and Security of Personal Data: The ability to use other employees' accounts for fraud.                                |
|    | Poor control of signed cheques: The ease of submitting reimbursement requests without adequate verification.                          |
|    | Lack of independent checks and control of the accounting system: No immediate flagging of unusual or repeated reimbursement requests. |



|    |   |
|----|---|
| 42 | Position of Trust & Authority: As Executive Director, Abboud had significant authority over the organization's finances.                        |
|    | Lack of Segregation of Duties: Her role allowed her to initiate and approve financial transactions without adequate checks.                     |
|    | Poor Audit Performance and Management Oversight: The prolonged fraud indicates ineffective audit and management oversight.                      |
|    | Lack of Systems of Authorization: The ability to misuse funds for personal expenses without detection suggests weak authorization protocols.    |
| 43 | Position of Trust & Authority: Skidmore's role provided her the authority and access needed to embezzle funds.                                  |
|    | Lack of Segregation of Duties: Control over various financial functions without checks enabled the fraudulent activities.                       |
|    | Lack of Independent Checks and Control of the Accounting System: The prolonged undetected fraud indicates poor independent checks.              |
|    | Poor Audit Performance and Management Oversight: The scheme's duration suggests inadequate auditing and management oversight.                   |
|    | Lack of Systems of Authorization: Unauthorized account openings and transactions indicate weak authorization systems.                           |
| 44 | Position of Trust & Authority: As the chief financial employee, Boisture had significant authority over financial matters, which she exploited. |
|    | Lack of Segregation of Duties: Control over multiple financial functions enabled her to execute fraudulent transactions.                        |
|    | Poor Audit Performance and Management Oversight: The prolonged undetected fraud suggests inadequate audit and management oversight.             |
|    | Lack of Systems of Authorization: The ease of obtaining unauthorized loans indicates weak systems of financial authorization.                   |
|    | Poor Accounting system: The organization lacked effective mechanisms to monitor and verify financial transactions.                              |
| 45 | Position of Trust & Authority: As the COO, Carroll had significant authority and control over financial operations.                             |
|    | Lack of Segregation of Duties: His ability to initiate and approve transactions without oversight suggests a lack of duty segregation.          |

|    |   |
|----|---|
|    | Poor Audit Performance and Management Oversight: The fraud's duration and scale indicate inadequate audit performance and oversight.                        |
| 46 | Position of Trust & Authority: Pothos' role gave her access to client accounts and personal information, which she exploited.                               |
|    | Lack of Physical and Digital Access Controls: Her ability to modify client information without detection indicates weak access controls.                    |
|    | Poor monitoring and security of personal data: The ease with which she could impersonate clients and redirect communications highlights poor data security. |
| 47 | Position of Trust & Authority: As a manager, Spilberg held a trusted position, enabling him to misuse the company debit card.                               |
|    | Lack of Physical and Digital Access Controls: The ability to use the company card freely for personal expenses suggests inadequate access controls.         |
|    | Poor Monitoring and Security of Personal Data: Failure to detect and prevent the misuse of the company card indicates poor monitoring.                      |
| 48 | Position of Trust & Authority: As CFO, Simkins had significant control and authority over financial transactions.   |
|    | Lack of Segregation of Duties: Simkins' ability to write company checks for personal use indicates poor segregation of duties.                              |
|    | Poor Audit Performance and Management Oversight: Extended period of undetected embezzlement suggests weak audit processes and management oversight.         |
|    | Poor Control of Signed Cheques: Lack of controls over check issuance facilitated the embezzlement.  |
| 49 | Position of Trust & Authority: Schulte's role allowed her access to funds and information, enabling her embezzlement and fraudulent loan applications.      |
|    | Poor Audit Performance and Management Oversight: The embezzlement suggests inadequate auditing and oversight in her previous employment.                    |
|    | Lack of Systems of Authorization: Her ability to manipulate financial transactions indicates weak systems of authorization.                                 |
| 50 | Position of Trust & Authority: As the bookkeeper, Chalmers had significant trust and authority over financial transactions.                                 |

|    |  |
|----|--|
|    | Lack of Segregation of Duties: Her ability to issue checks to herself shows a clear lack of segregation in financial responsibilities.                                 |
|    | Poor Control of Signed Cheques: The large number of checks written to herself indicates poor control over check issuance.  |
| 51 | Position of Trust & Authority: As executives, Pourhassan and Kazempour had significant influence over company operations and information disclosure.                   |
|    | Lack of Independent Checks and Control of the Accounting System: Inadequate verification of financial and regulatory information provided to investors and the public. |
|    | Poor Audit Performance and Management Oversight: The lack of effective oversight enabled the prolonged dissemination of false information.                             |
| 52 | Position of Trust & Authority: As an accountant and cash manager, Marquez had significant control over financial transactions.   |
|    | Lack of Segregation of Duties: His dual role provided the opportunity to misappropriate funds without immediate detection.   |
|    | Poor Monitoring and Security of Personal Data: Inadequate monitoring allowed Marquez to alter bank statements without being noticed.                                   |
|    | Lack of Systems of Authorization: The unauthorized transfers suggest a failure in systems of financial authorization.  |
| 53 | Position of Trust & Authority: As CEO, Collins had significant control over company operations and financial reporting.  |
|    | Lack of Segregation of Duties: His ability to manipulate loan information without checks indicates a failure in segregating duties.                                    |
|    | Poor Audit Performance and Management Oversight: The extended period of fraud suggests inadequate auditing and management oversight.                                   |
|    | Lack of Systems of Authorization: The manipulation of loan portfolios suggests a failure in robust systems of financial authorization.                                 |
| 54 | Position of Trust & Authority: As vice president, Vicars had significant control over project oversight and invoice approval.  |
|    | Lack of Segregation of Duties: His dual role allowed him to execute and approve his own fraudulent transactions.   |

|    |   |
|----|---|
|    | Lack of Systems of Authorization: The unauthorized approval of own invoices indicates weak systems of financial authorization.  |
|    | Poor Procurement policies: There was a lack of robust processes to verify the legitimacy of vendor invoices, especially those connected to executives.                      |
| 55 | Position of Trust & Authority: Smith's role as an office manager with payroll responsibilities provided her with the opportunity to manipulate financial records.           |
|    | Lack of Segregation of Duties: Control over payroll and access to business accounts allowed her to execute and conceal fraudulent transactions.                             |
|    | Poor Monitoring and Security of Personal Data: Inadequate monitoring enabled her to transfer funds and alter records without detection.                                     |
|    | Absence of Cash Reconciliation and Surprise Checks: Lack of regular reconciliation processes facilitated the ongoing embezzlement.  |
|    | Poor Payroll management: The organization did not have robust reconciliation procedures in place to identify discrepancies in payroll and bank statements.                  |
| 56 | Lack of Systems of Authorization: The ability to submit false W-4 forms without detection shows a lack of robust authorization processes in the employers' payroll systems. |
|    | Poor Payroll Management: Employers not detecting fraudulent tax exemption claims indicates weaknesses in payroll management.  |
|    | Hiring without Background Checks: Employers failed to adequately verify the authenticity of Reyes' claims on his W-4 forms.   |
| 57 | Position of Trust & Authority: Patel's position as the owner gave him the authority to perpetrate the fraud.  |
|    | Lack of Systems of Authorization: The scheme's success indicates inadequate systems to authorize and validate medical tests and claims.                                     |
|    | Poor Monitoring and Security of Personal Data: Exploiting Medicare beneficiaries' information for fraudulent claims.  |
|    | Poor Audit Performance and Management Oversight: The scale of fraud suggests inadequate oversight and poor audit performance.   |
| 58 | Position of Trust & Authority: Bowker's role as CFO gave him direct control over financial transactions and tax payments.   |

|    |   |
|----|---|
|    | Lack of Segregation of Duties: His dual responsibilities facilitated the embezzlement and tax evasion without immediate detection.                        |
|    | Poor Audit Performance and Management Oversight: The duration and scale of the fraud indicate poor audit performance and inadequate management oversight. |
|    | Lack of Systems of Authorization: The misuse of the company credit card and transfer of funds suggests a lack of robust authorization systems.            |
| 59 | Position of Trust & Authority: As CEO, Bankman-Fried had significant control over the company's funds and operations.                                     |
|    | Lack of Segregation of Duties: His control over both FTX and Alameda Research facilitated the misappropriation of funds.                                  |
|    | Poor Audit Performance and Management Oversight: Inadequate auditing and oversight allowed the fraudulent activities to continue undetected.              |
|    | Lack of Systems of Authorization: The ease with which funds were misappropriated indicates weak authorization systems.                                    |
| 60 | Position of Trust & Authority: As a bookkeeper, Meeks had access and authority over financial records and transactions.                                   |
|    | Lack of Segregation of Duties: Her control over multiple financial functions enabled the fraud.   |
|    | Poor Monitoring and Security of Personal Data: Inadequate monitoring allowed Meeks to use the company credit cards without detection.                     |
|    | Lack of Systems of Authorization: The ease of making unauthorized purchases suggests a lack of robust authorization systems.                              |
| 61 | Position of Trust & Authority: As President and CEO, Kewalis had significant control and authority, which she misused.                                    |
|    | Lack of Segregation of Duties: Her ability to manipulate the accounting system without oversight.   |
|    | Poor Audit Performance and Management Oversight: The prolonged period of undetected fraudulent activities suggests inadequate auditing and oversight.     |
|    | Lack of Systems of Authorization: The ability to create fraudulent accounts indicates a failure in authorization systems.                                 |
|    | Poor Accounting system: The fact that fraudulent accounts could be created and used without detection points to weak financial controls.                  |

|    |  |
|----|--|
| 62 | Position of Trust & Authority: As IT Director, Hicks had significant control over important company resources.   |
|    | Lack of Segregation of Duties: His role allowed him to manage various systems, facilitating fraudulent activities.   |
|    | Poor Monitoring and Security of Personal Data: Inadequate monitoring enabled Hicks to misuse company resources without detection.  |
|    | Lack of Systems of Authorization: The ability to make unauthorized purchases suggests weak financial authorization systems.  |
| 63 | Position of Trust & Authority: As a vault manager, Lazzaro had direct access to large amounts of cash, providing the opportunity for theft.  |
|    | Lack of Segregation of Duties: Her dual roles in handling and managing cash lacked sufficient oversight and segregation.   |
|    | Lack of Physical and Digital Access Controls: The ease with which she manipulated the bank's system indicates weak monitoring and security protocols.                              |
|    | Absence of cash reconciliation and surprise checks on cash: The bank lacked robust cash handling and reconciliation procedures to prevent theft from teller drawers and the vault. |
| 64 | Position of Trust & Authority: As CFO, McManus had significant authority and trust, enabling him to embezzle funds.  |
|    | Lack of Segregation of Duties: Control over financial transactions without adequate oversight facilitated the fraud.   |
|    | Poor Audit Performance and Management Oversight: The duration of the embezzlement indicates poor audit performance and management oversight.                                       |
|    | Lack of Systems of Authorization: The ability to self-reimburse personal expenses points to a failure in authorization systems.  |
| 65 | Position of Trust & Authority: As CFO, Sharar had significant authority and control, which she exploited for embezzlement.   |
|    | Lack of Segregation of Duties: Control over financial transactions and reporting enabled the fraud.  |
|    | Poor Audit Performance and Management Oversight: The duration of the fraud suggests inadequate audit performance and oversight.  |
|    | Lack of Systems of Authorization: The ability to transfer funds unchecked indicates a lack of robust authorization systems.  |
|    | Poor Accounting system: Sharar's ability to manipulate financial transactions points to weak oversight.  |

|    |   |
|----|---|
| 66 | Position of Trust & Authority: As CEO, Cole had the leverage to manipulate financial records.   |
|    | Lack of independent checks and control of the accounting system: Insufficient scrutiny over financial statements and transactions.                                    |
|    | Poor Audit performance and Management oversight: Ineffective audit processes enabling the persistence of fraudulent activities.                                       |
|    | Lack of systems of authorization: Weak controls over financial transactions and JV agreements.  |
|    | Organizational Structure Weaknesses: The corporate structure may have allowed for unchecked executive actions.  |
| 67 | Position of Trust & Authority: Swanson's role provided her with the authority and trust necessary to manipulate financial records.                                    |
|    | Lack of Segregation of Duties: Her role as both an accountant and controller enabled her to carry out and conceal the fraud.  |
|    | Poor Payroll Management: Inadequate oversight and control over the payroll process facilitated the embezzlement.  |
|    | Lack of Independent Checks and Control of the Accounting System: The absence of independent reviews or audits allowed the fraudulent activity to continue undetected. |
| 68 | Position of Trust & Authority: Kent's role as a maintenance supervisor allowed him direct access to procurement processes.  |
|    | Lack of Segregation of Duties: His ability to manipulate procurement and reimbursement processes indicates a lack of duty segregation.                                |
|    | Poor Audit Performance and Management Oversight: The duration and success of his schemes suggest inadequate auditing and oversight.                                   |
|    | Lack of Systems of Authorization: The ease with which he fabricated and submitted invoices indicates weak authorization systems.                                      |
|    | Poor Accounting system: The organization failed to effectively verify the authenticity of receipts and invoices.  |
| 69 | Position of Trust & Authority: As CEO, Farley had the authority to manipulate financial transactions.   |
|    | Poor Accounting System: The ability to execute a check kiting scheme indicates weaknesses in the accounting system.   |
|    | Poor Payroll Management: Failure to properly manage and remit employee taxes.   |

|    |   |
|----|---|
|    | Lack of Independent Checks and Control of the Accounting System: Insufficient controls to detect and prevent fraudulent financial activities.   |
| 70 | Position of Trust & Authority: McGlown's position as an inventory manager gave him the authority to manipulate the vendor system.   |
|    | Lack of Segregation of Duties: Their roles allowed manipulation of purchase orders and invoices without independent verification.   |
|    | Lack of Systems of Authorization: The successful submission of fake invoices and use of a purchase card for fraudulent activities indicates weak systems of authorization and verification. |
|    | Poor Audit Performance and Management Oversight: The prolonged period of undetected fraudulent activities suggests a lack of effective auditing and oversight.                              |
|    | Poor Procurement policies: The ease of entering fake companies into the vendor system indicates weak procurement processes.   |
| 71 | Position of Trust & Authority: As a co-owner, James had significant authority and control over financial reporting.   |
|    | Lack of Segregation of Duties: The coordination with the accountant to manipulate records points to a lack of duty segregation.   |
|    | Poor Audit Performance and Management Oversight: The prolonged manipulation of records and failure to pay taxes suggest weak audit and oversight practices.                                 |
|    | Poor Accounting System: The ease with which financial records were manipulated indicates flaws in the accounting system.  |
|    | Poor Payroll Management: Failing to pay payroll taxes shows a lack of proper payroll management practices.  |
| 72 | Position of Trust & Authority: Aggarwal's senior role in internal auditing gave him direct access to manipulate financial transactions.   |
|    | Lack of Segregation of Duties: Control over vendor payments and auditing enabled the fraud.   |
|    | Poor Monitoring and Security of Personal Data: Inadequate monitoring of financial transactions involving vendors.   |
|    | Lack of Systems of Authorization: Weaknesses in the authorization of vendor payments.   |
|    | Poor Procurement policies: The company failed to verify the authenticity of services invoiced by vendors.   |



|    |  |
|----|--|
| 73 | Position of Trust & Authority: As a manager, Allen had significant control over company finances, which he exploited.  |
|    | Lack of Segregation of Duties: Allen's ability to divert funds indicates a lack of proper segregation in financial responsibilities.                                 |
|    | Poor Audit Performance and Management Oversight: The undetected embezzlement over a period suggests poor auditing and management oversight.                          |
|    | Lack of Systems of Authorization: The ease of diverting funds suggests inadequate systems for authorizing and tracking financial transactions.                       |
| 74 | Position of Trust & Authority: As a bank teller, Ritter had direct access to customer accounts, facilitating the embezzlement.                                       |
|    | Lack of Segregation of Duties: His role possibly allowed him to execute transactions without sufficient oversight or verification.                                   |
|    | Poor Monitoring and Security of Personal Data: The ability to access and withdraw funds indicates inadequate monitoring and security measures for customer accounts. |
|    | Lack of Systems of Authorization: Ritter's ability to embezzle funds suggests a lack of robust systems for transaction authorization and verification.               |
|    | Absence of Cash Reconciliation and Surprise Checks on Cash: Regular reconciliation of accounts and surprise audits could have detected the fraud earlier.            |
| 75 | Position of Trust & Authority: As CEO, Steele had significant control, enabling her to manipulate financial transactions.  |
|    | Lack of Segregation of Duties: Her ability to execute transactions across various methods shows a lack of duty segregation.  |
|    | Poor Audit Performance and Management Oversight: The prolonged embezzlement suggests inadequate auditing and oversight practices.                                    |
|    | Lack of Systems of Authorization: The ease of making unauthorized transactions indicates a lack of robust authorization systems.                                     |
|    | Poor Accounting System: The ability to execute fraudulent transactions across different methods points to weaknesses in the accounting system.                       |
|    | Poor Control of Signed Cheques: Issuing checks to herself indicates poor control over cheque authorization.  |

|    |   |
|----|---|
| 76 | Position of Trust & Authority: Rogas exploited his roles as CEO, CFO, and board member to manipulate financial data.                                      |
|    | Lack of Segregation of Duties: His control over key financial processes allowed the fraud to occur.   |
|    | Poor Audit Performance and Management Oversight: The fraudulent scheme's success indicates ineffective auditing and management oversight.                 |
|    | Lack of Systems of Authorization: The ability to unilaterally alter financial statements suggests weak financial authorization systems.                   |
|    | Poor Accounting System: The ease with which financial records were manipulated indicates systemic weaknesses in accounting practices.                     |
| 77 | Position of Trust & Authority: As a commissioner, Sutton was in a position of authority, enabling her to exploit her role for personal gain.              |
|    | Lack of Systems of Authorization: The ability to extort money indicates a lack of effective systems to authorize and monitor financial transactions.      |
|    | Poor Monitoring and Security of Personal Data: Inadequate monitoring mechanisms that failed to detect or prevent corrupt activities.                      |
| 78 | Position of Trust & Authority: Mensinger abused his role as Chief Lending Officer to facilitate fraudulent loans.   |
|    | Lack of Segregation of Duties: His ability to both authorize and facilitate loan approvals without oversight.   |
|    | Poor Monitoring and Security of Personal Data: The misuse of personal and financial information in loan applications.                                     |
|    | Poor Audit performance and Management oversight: Ineffective or absent internal auditing processes that failed to identify the fraudulent activities.     |
| 79 | Position of Trust & Authority: Valentin's role as credit manager gave her control over customer payments, which she exploited.                            |
|    | Lack of Physical and Digital Access Controls: Inadequate controls allowed her to divert checks to her personal account.                                   |
|    | Poor Monitoring and Security of Personal Data: The failure to detect unusual activity in customer payments indicates poor financial monitoring.           |
|    | Poor Control of Signed Cheques: The ability to deposit checks meant for the company into her personal account points to weak controls over signed checks. |

|    |   |
|----|---|
| 80 | Position of Trust & Authority: As Directors of Public Works, they had significant control over project approvals and invoice processing.  |
|    | Lack of Segregation of Duties: Their roles allowed them to both certify projects and approve payments, facilitating the bribery.  |
|    | Lack of Systems of Authorization: The absence of robust authorization systems for invoice approvals and project certifications.   |
|    | Poor Control of Signed Cheques: The manipulation of invoice payments indicates poor control over the payment processes.   |
|    | Poor Procurement policies: The ability to approve invoices and certify projects without adequate oversight.   |
| 81 | Position of Trust & Authority: Williams' position as president provided her the authority to access and misappropriate funds.   |
|    | Lack of Segregation of Duties: Her control over financial transactions enabled the misappropriation of funds.   |
|    | Poor Audit Performance and Management Oversight: The duration and scale of the fraud indicate ineffective auditing and oversight.   |
| 82 | Position of Trust & Authority: Crawford's senior finance position allowed her to manipulate financial processes.  |
|    | Lack of Segregation of Duties: Her responsibilities in multiple finance areas enabled the fraud.  |
|    | Poor Audit performance and Management oversight: Lack of effective monitoring allowed fraudulent activities to go unnoticed.  |
|    | Lack of independent checks and control of the accounting system: Crawford's ability to generate and approve fraudulent transactions suggests a lack of effective checks and controls. |
| 83 | Position of Trust & Authority: As executives, the Jacksons had significant control over Semisub's operations and finances.  |
|    | Poor Audit Performance and Management Oversight: The prolonged fraud suggests inadequate auditing and oversight mechanisms.   |
| 84 | Position of Trust & Authority: Holding executive positions at both companies provided Smith with the authority to access and misappropriate funds.                                    |
|    | Lack of Independent Checks and Control of the Accounting System: The duration of the fraud suggests inadequate checks and controls within the accounting systems of both companies.   |

|    |   |
|----|---|
|    | Hiring without Background Checks: The ability to embezzle from two companies indicates hiring without background checks.  |
| 85 | Position of Trust & Authority: Anthony Sharper's roles as president and CPA allowed him access and control over funds.  |
|    | Lack of Segregation of Duties: Control over financial transactions and reporting enabled the embezzlement.  |
|    | Poor Audit Performance and Management Oversight: The prolonged and varied nature of the fraud indicates ineffective oversight and auditing.                               |
|    | Poor Accounting System: The ease of manipulating financial statements and tax returns suggests weaknesses in accounting practices.  |
|    | Lack of Systems of Authorization: The unauthorized use of funds and creation of fraudulent loan applications indicate a lack of robust financial authorization processes. |
| 86 | Position of Trust & Authority: Her role as office manager gave her access to financial processes and the signature stamp.   |
|    | Lack of Segregation of Duties: Control over both bookkeeping and accounts payable enabled fraudulent activities.  |
|    | Poor Audit Performance and Management Oversight: The prolonged undetected fraud suggests ineffective auditing and management oversight.                                   |
|    | Poor Accounting System: The ease with which she manipulated accounting records indicates a flawed accounting system.  |
|    | Lack of Systems of Authorization: Unauthorized use of the signature stamp and false payroll entries point to weak authorization systems.                                  |
| 87 | Position of Trust & Authority: Pike's position as a general manager gave him the authority to create and approve invoices.  |
|    | Lack of Segregation of Duties: His ability to fabricate and approve invoices indicates a failure in segregating financial responsibilities.                               |
|    | Poor Audit Performance and Management Oversight: The prolonged nature of the fraud suggests inadequate auditing and managerial oversight.                                 |
|    | Lack of Systems of Authorization: The unauthorized use of initials and approval of invoices without verification points to weak authorization systems.                    |

|    |  |
|----|--|
|    | Poor Monitoring and Security of Personal Data: The misuse of company personnel initials without detection indicates poor monitoring of sensitive information.              |
| 88 | Position of Trust & Authority: Sweeten's role as a bookkeeper and her relationship with the company president provided her with the opportunity to embezzle funds.         |
|    | Lack of Segregation of Duties: Controlling multiple financial functions enabled her to execute and conceal fraudulent transactions.  |
|    | Poor Monitoring and Security of Personal Data: The ability to intercept and misuse company mail and credit cards indicates inadequate monitoring of sensitive information. |
|    | Lack of Systems of Authorization: The unauthorized issuance of checks and credit card usage suggests weak financial authorization processes.                               |
|    | Poor Control of Signed Cheques: The misuse of company checks points to inadequate controls over signed cheques.  |
| 89 | Position of Trust & Authority: Loconte's positions as president of two companies allowed him to orchestrate the fraud.   |
|    | Lack of Segregation of Duties: His control over financial and payroll processes enabled the fraudulent activities.   |
|    | Poor Payroll Management: Mishandling payroll and tax withholdings points to inadequate payroll management practices.   |
|    | Poor Accounting System: Underreporting wages and misusing company funds for personal expenses indicates flaws in the accounting system.                                    |
|    | Absence of Cash Reconciliation and Surprise Checks on Cash: Paying employees in cash without proper accounting reflects a lack of cash management controls.                |
| 90 | Position of Trust & Authority: As Director of Finance and Administration, Petrone had significant control over departmental purchases.                                     |
|    | Lack of Segregation of Duties: Her ability to authorize and execute purchases without additional approval enabled the fraud.   |
|    | Poor Audit Performance and Management Oversight: The prolonged undetected fraud indicates inadequate auditing and managerial oversight.                                    |
|    | Lack of Systems of Authorization: The exploitation of the \$10,000 purchase threshold shows a weakness in the authorization process.                                       |

|    |  |
|----|--|
|    | Poor Accounting System: The system failed to flag the pattern of just under-threshold purchases, indicating flaws in accounting practices.   |
| 91 | Position of Trust & Authority: Thumann's role as a bookkeeper gave her direct access to rent payments and the authority to manipulate records.                                       |
|    | Lack of Segregation of Duties: Her ability to receive, record, and reconcile payments indicates a failure in separating financial responsibilities.                                  |
|    | Poor Audit Performance and Management Oversight: The undetected nature of the fraud for several years suggests weak audit performance and managerial oversight.                      |
|    | Poor Accounting system: Thumann's ability to manipulate tenant payments and records points to significant lapses in financial oversight.   |
|    | Lack of Physical and Digital Access Controls: Thumann's ability to manipulate the HRA's computer system indicates a weakness in the effective use and security of financial systems. |
| 92 | Position of Trust & Authority: As Financial Controller, Laansma had the authority to manage finances and manipulate records.   |
|    | Lack of Segregation of Duties: Her control over financial transactions and record-keeping enabled the embezzlement.  |
|    | Poor Audit Performance and Management Oversight: The fact that the fraud continued until the company's acquisition suggests weak audit performance and oversight.                    |
|    | Lack of Systems of Authorization: The ability to utilize and hide a corporate credit card points to inadequate financial authorization processes.                                    |
|    | Poor Accounting System: Misclassification of personal expenses as business expenses indicates flaws in the accounting system.  |
| 93 | Position of Trust & Authority: Burke's position as a bookkeeper gave her the authority to manage and manipulate financial records.   |
|    | Lack of Segregation of Duties: Her ability to issue checks and maintain financial records indicates a failure in separating financial responsibilities.                              |
|    | Poor Audit Performance and Management Oversight: The undetected nature of the fraud for several years suggests weak audit performance and managerial oversight.                      |

|    |  |
|----|--|
|    | Lack of Systems of Authorization: The unauthorized issuance of checks to herself points to inadequate financial authorization controls.                    |
|    | Poor Accounting System: The ease with which financial records were manipulated indicates systemic weaknesses in accounting practices.                      |
| 94 | Position of Trust & Authority: Burke's role as controller gave him authority over financial transactions, enabling embezzlement.                           |
|    | Lack of Segregation of Duties: His ability to direct payroll and sign checks indicates a lack of appropriate duty segregation.                             |
|    | Poor Audit Performance and Management Oversight: The duration of the fraud suggests weak audit performance and managerial oversight.                       |
|    | Lack of Systems of Authorization: The unauthorized personal use of company funds suggests inadequate systems of financial authorization.                   |
|    | Poor Payroll Management: Misusing payroll for personal gain indicates flawed payroll management practices.   |
| 95 | Position of Trust & Authority: As a marketing manager, Ahmed-Elkilani had the authority and access needed to manipulate transactions.                      |
|    | Lack of Segregation of Duties: His ability to access and use other employees' operator codes shows a lack of duty segregation.                             |
|    | Poor Monitoring and Security of Personal Data: The misuse of employee codes and company accounts points to inadequate data security and monitoring.        |
|    | Lack of Systems of Authorization: The ease with which funds were misappropriated suggests weak systems of financial authorization.                         |
| 96 | Position of Trust & Authority: As a controller, Lee had significant authority over the company's finances and recordkeeping.                               |
|    | Lack of Segregation of Duties: His ability to execute and conceal fraudulent transactions indicates a failure in separating financial responsibilities.    |
|    | Poor Audit Performance and Management Oversight: The prolonged undetected fraud suggests weak audit performance and managerial oversight.                  |
|    | Lack of Systems of Authorization: The ease with which Lee could falsify records and transfer funds indicates inadequate financial authorization processes. |

|     |   |
|-----|---|
|     | Poor Accounting System: The successful manipulation of the company's financial records reflects weaknesses in the accounting system.                                |
| 97  | Position of Trust & Authority: Carper's role as secretary provided her with access to financial instruments and records.  |
|     | Lack of Segregation of Duties: Her ability to manipulate financial transactions without oversight indicates a lack of duty segregation.                             |
|     | Lack of Systems of Authorization: The use of pre-signed checks without proper authorization controls facilitated the embezzlement.                                  |
|     | Poor Control of Signed Cheques: Pre-signing checks and inadequate tracking of their use allowed Carper to misuse them.  |
| 98  | Position of Trust & Authority: Koch's supervisory role enabled him to fraudulently manipulate time records.   |
|     | Lack of Segregation of Duties: Koch had the ability to enter hours and access network credentials, pointing to a failure in segregating responsibilities.           |
|     | Lack of Systems of Authorization: The ease of manipulating time records suggests inadequate systems for authorizing and verifying work hours.                       |
|     | Poor Payroll management: The ability to falsify records over several years indicates significant lapses in monitoring employee work hours.                          |
| 99  | Position of Trust & Authority: Latoski's position allowed her direct access to corporate financial resources and decision-making power.                             |
|     | Lack of Segregation of Duties: Her control over both using corporate credit cards and managing accounting records suggests a lack of duty segregation.              |
|     | Poor Audit Performance and Management Oversight: The ability to manipulate financial records undetected for years indicates poor auditing and managerial oversight. |
|     | Lack of Systems of Authorization: The unauthorized use of corporate funds for personal expenses points to inadequate financial authorization processes.             |
|     | Poor Accounting System: The manipulation of accounting records to conceal personal expenses suggests systemic weaknesses in accounting practices.                   |
| 100 | Position of Trust & Authority: Kennedy's senior position enabled him to influence vendor selection and conceal kickbacks.   |



|     |  |
|-----|--|
|     | Lack of Segregation of Duties: His role allowed him to both influence procurement decisions and receive bribes.  |
|     | Poor Audit Performance and Management Oversight: The prolonged nature of the scheme suggests ineffective auditing and managerial oversight.  |
|     | Lack of Systems of Authorization: Inadequate controls over vendor selection and payment verification.  |
|     | Poor Procurement Policies: Weaknesses in procurement processes enabled favoritism and overcharging.  |
| 101 | Position of Trust & Authority: Rigsbee's position as a financial advisor provided him direct access to customer accounts and the ability to execute transactions.                                |
|     | Lack of Segregation of Duties: His ability to initiate and complete transfers without additional verification indicates a lack of duty segregation.  |
|     | Poor Audit Performance and Management Oversight: The undetected nature of the fraud for multiple years suggests a lack of effective auditing and managerial supervision.                         |
|     | Lack of Systems of Authorization: The unauthorized transfers and creation of fraudulent requests show weak systems of financial authorization and security.                                      |
|     | Poor Monitoring and Security of Personal Data: The ease with which Rigsbee was able to impersonate customers and access their funds indicates inadequate monitoring of sensitive financial data. |
| 102 | Position of Trust & Authority: Ellis's role as Financial Officer granted him direct access to and control over the non-profit's finances.  |
|     | Lack of Segregation of Duties: His ability to both manage and manipulate financial transactions indicates a failure in segregating responsibilities.   |
|     | Poor Audit Performance and Management Oversight: The fact that the fraud continued for eight years indicates a lack of effective auditing and managerial supervision.                            |
|     | Lack of Systems of Authorization: The unauthorized transfer of funds from SBHS to personal accounts shows weaknesses in financial authorization processes.                                       |
| 103 | Position of Trust & Authority: Hall's role as a manager gave her direct access to accounts and the authority to execute financial transactions.  |
|     | Lack of Segregation of Duties: Control over creating loans and transferring funds without additional oversight or verification.  |

|     |  |
|-----|--|
|     | <p>Poor Audit Performance and Management Oversight: Ineffective auditing and managerial supervision allowed fraudulent activities to continue undetected.</p> <p>Lack of Systems of Authorization: The ability to create and approve fake loans and transfers without additional checks.</p> <p>Lack of independent checks and control of the accounting system: The ability to manipulate financial operations and records for personal gain points to significant lack of independent checks and controls</p>  |
| 104 | <p>Position of Trust &amp; Authority: Kim's long tenure and senior engineering position gave him trusted access to sensitive information.</p> <p>Lack of Segregation of Duties: His role possibly allowed him broad access to various sensitive documents without sufficient oversight.</p> <p>Lack of Physical and Digital Access Controls: The ability to copy and remove large amounts of data indicates insufficient digital security measures.</p> <p>Poor Monitoring and Security of Personal Data: Inadequate monitoring of the usage and copying of sensitive documents.</p> <p>Hiring without Background Checks: Failure to prevent or detect the transfer of sensitive information upon an employee's resignation and his subsequent hiring in another company demonstrates the hiring policies without adequate background checks in place.</p> |
| 105 | <p>Position of Trust &amp; Authority: Bittner's managerial position gave him the authority and access to manipulate the reservation system.</p> <p>Lack of Segregation of Duties: His ability to initiate and direct refunds without additional checks indicates a failure in separating financial responsibilities.</p> <p>Poor Audit Performance and Management Oversight: The sustained nature of the fraud suggests inadequate auditing and managerial supervision.</p> <p>Lack of Systems of Authorization: The unauthorized direction of refunds to personal accounts points to weak systems of financial authorization and control.</p> <p>Poor Accounting System: The ease with which financial records were manipulated indicates systemic weaknesses in the resort's accounting practices.</p>   |
| 106 | <p>Position of Trust &amp; Authority: Welch's position as a bookkeeper enabled her to access and manipulate the company's financial transactions.</p>  |

|     |   |
|-----|---|
|     | Lack of Segregation of Duties: Her ability to issue checks and manage financial records without additional oversight or verification indicates a failure in segregating duties.             |
|     | Poor Audit Performance and Management Oversight: The sustained nature of the fraud suggests ineffective auditing and lack of adequate managerial supervision.                               |
|     | Lack of Systems of Authorization: The unauthorized issuance of checks without detection points to weak systems of financial authorization.  |
|     | Poor control of signed cheques: The ease with which cheques were manipulated and deposited into the fraudster's account indicates systemic weaknesses in Kasco's cheque security measures.. |
| 107 | Position of Trust & Authority: Ricker's various positions within the company provided her with access to checks and the opportunity to commit fraud.  |
|     | Lack of Segregation of Duties: Her ability to access, write, and cash checks without supervision indicates a failure in separating financial responsibilities.                              |
|     | Poor Audit Performance and Management Oversight: The duration of the fraud suggests ineffective auditing and managerial supervision.  |
|     | Poor Control of Signed Cheques: The ease with which Ricker accessed and misused signed checks indicates poor control over such financial instruments.                                       |
| 108 | Position of Trust & Authority: Lutamila's roles as Controller and Acting CFO provided him with the necessary access and authority to misappropriate funds.                                  |
|     | Lack of Segregation of Duties: His ability to initiate and complete financial transfers without additional oversight.   |
|     | Poor Audit Performance and Management Oversight: The undetected embezzlement over time suggests poor auditing and oversight.  |
|     | Lack of independent checks and control of the accounting system: The ability to carry out the scheme over several months indicates a failure in monitoring financial transactions.          |
| 109 | Position of Trust & Authority: Miller's role as a supervisor gave him the authority to manipulate payroll and procurement processes.  |
|     | Poor Payroll management: The lack of effective verification of timesheets, and reimbursements allowed fraudulent activities to proceed undetected.  |

|     |   |
|-----|---|
|     | Poor Procurement policies: The lack of effective verification of invoices, and vendor data allowed fraudulent activities to proceed undetected.                           |
|     | Poor Accounting System: The ease with which Miller manipulated financial records indicates weaknesses in the company's accounting system.                                 |
| 110 | Position of Trust & Authority: Topping's managerial position gave him access to and control over ATM and cash drawer funds.   |
|     | Lack of Segregation of Duties: His ability to access and embezzle funds without detection points to a failure in separating financial responsibilities.                   |
|     | Lack of Physical and Digital Access Controls: The unauthorized access to the ATM and cash drawer shows inadequate controls over physical and digital financial resources. |
|     | Absence of cash reconciliation and surprise checks on cash: The ability to embezzle cash from a teller drawer indicates absence of cash reconciliation.                   |
| 111 | Position of Trust & Authority: Pylant's role gave her direct access to financial records and the ability to issue checks.   |
|     | Lack of Segregation of Duties: Her responsibilities included multiple aspects of financial handling, facilitating the embezzlement.                                       |
|     | Poor Audit Performance and Management Oversight: The multi-year span of her schemes suggests ineffective auditing and managerial supervision.                             |
|     | Poor monitoring and security of personal data: Committing Identity Theft for an extended period of time shows the poor monitoring of personal data                        |
|     | Lack of Independent Checks and Control of the Accounting System: The prolonged undetected fraud indicates poor independent checks.  |
| 112 | Position of Trust & Authority: As CFO and director of operations, Aldi had significant control over financial transactions, facilitating the embezzlement.                |
|     | Lack of Segregation of Duties: Her ability to conduct and conceal fraudulent transactions demonstrates a failure in segregating financial responsibilities.               |
|     | Poor Audit Performance and Management Oversight: The undetected nature of the fraud over years indicates ineffective auditing and managerial supervision.                 |

|     |   |
|-----|---|
|     | <p>Poor Accounting System: The ease with which financial records were manipulated shows weaknesses in the company's accounting system.</p> <p>Lack of Systems of Authorization: Aldi's unauthorized withdrawals and record falsification indicate a lack of robust financial authorization processes.</p> <p>Absence of cash reconciliation and surprise checks on cash: Aldi's extensive cash theft highlights significant lapses in the company's cash reconciliation mechanisms.</p>   |
| 113 | <p>Position of Trust &amp; Authority: Madison's position enabled her to manage and manipulate financial documentation.</p> <p>Lack of Segregation of Duties: Her role encompassed preparing, presenting, and executing payment processes, indicating a lack of duty segregation.</p> <p>Poor Audit Performance and Management Oversight: The ability to embezzle funds over a period of time points to weak auditing and oversight.</p> <p>Poor Accounting System: The ease with which Madison manipulated the accounting system indicates systemic weaknesses in financial control.</p> <p>Poor Procurement policies: Processing of fake claims and invoices shows a significant lapse in procurement policies by the company</p>  |
| 114 | <p>Position of Trust &amp; Authority: As office manager, Jones had significant control over financial operations and access to company accounts.</p> <p>Lack of Segregation of Duties: Her control over accounts payable/receivable, payroll, and other financial aspects allowed for unchecked embezzlement.</p> <p>Poor Audit Performance and Management Oversight: The prolonged nature of the fraud suggests weak auditing and lack of effective management supervision.</p> <p>Poor Accounting System: The ease with which she manipulated financial records indicates a flawed accounting system.</p> <p>Lack of Systems of Authorization: Unauthorized use of company funds and creation of fake invoices without detection points to inadequate financial controls.</p> |
| 115 | <p>Position of Trust &amp; Authority: Weston's position enabled him to manage, manipulate, and embezzle significant funds.</p> <p>Lack of Segregation of Duties: His dual role in accounting and handling funds indicates a failure in separating financial responsibilities.</p>   |

|     |   |
|-----|---|
|     | Poor Audit Performance and Management Oversight: The sustained nature of the fraud suggests weak auditing and managerial supervision.                       |
| 116 | Position of Trust & Authority: Cox's status as a congressman and business owner gave him significant influence over financial transactions.                 |
|     | Lack of Segregation of Duties: His ability to manipulate business and campaign finances without checks indicates a failure in segregating responsibilities. |
|     | Poor Procurement Policies: The manner in which contracts and loans were obtained suggests inadequate procurement controls.                                  |
|     | Lack of independent checks and control of the accounting system: The case clearly demonstrates the lack of independent checks on the performance of Cox.    |
| 117 | Position of Trust & Authority: Garrett's position allowed him direct access to financial transactions and records.  |
|     | Lack of Segregation of Duties: His role in managing both payable and receivable accounts, without separate checks, facilitated the fraud.                   |
|     | Lack of Systems of Authorization: The unauthorized creation of invoices and purchases without detection points to a lack of robust authorization processes. |
| 118 | Position of Trust & Authority: Abouammo's position at Twitter allowed him access to confidential user data.   |
|     | Poor Monitoring and Security of Personal Data: The ability to access and disclose user data without detection suggests inadequate data security measures.   |
|     | Lack of Segregation of Duties: His role possibly combined data access and external communications, lacking oversight.                                       |
| 119 | Position of Trust & Authority: As a project manager, Sacco had the authority to manage and influence project costs.   |
|     | Lack of Segregation of Duties: His role allowed him to oversee financial aspects without adequate checks, facilitating the fraud.                           |
|     | Poor Audit Performance and Management Oversight: The sustained nature of the scheme suggests weak auditing and managerial supervision.                      |
|     | Poor Procurement Policies: The ability to manipulate change orders indicates weaknesses in procurement and financial control policies.                      |
| 120 | Position of Trust & Authority: Levoff's senior roles at Apple gave him access to nonpublic financial information.   |

|     |  |
|-----|--|
|     | Poor Audit Performance and Management Oversight: The ability to engage in insider trading for years points to weak auditing and oversight.                                   |
|     | Size of Organization: Larger organizations tend to have a weaker control over processes, facilitating fraud like Insider Trading.  |
| 121 | Position of Trust & Authority: As owner of multiple companies, Chandran had significant control over operations and investor communications.                                 |
|     | Poor Audit Performance and Management Oversight: The prolonged fraudulent scheme suggests inadequate auditing and oversight mechanisms.                                      |
|     | Poor Accounting System: The ability to divert funds for personal use indicates weaknesses in the companies' financial record-keeping and accounting systems.                 |
| 122 | Position of Trust & Authority: Broyles' role in the companies gave him the authority to misrepresent business operations and mismanage funds.                                |
|     | Poor Audit Performance and Management Oversight: Ineffective oversight and auditing processes failed to uncover fraudulent representations.                                  |
|     | Lack of Systems of Authorization: Inadequate verification of the legitimacy of business claims and transactions.   |
|     | Poor Monitoring and Security of Personal Data: Using personal information and aliases to evade law enforcement indicates a failure in monitoring personal identity security. |
| 123 | Position of Trust & Authority: Barnes and DeGroot exploited their senior positions to mislead investors and misuse funds.  |
|     | Poor Audit Performance and Management Oversight: Ineffective oversight and auditing of financial operations and representations to investors.                                |
|     | Absence of Cash Reconciliation and Surprise Checks on Cash: Failure to reconcile cash inflows from investments with the company's stated operational expenses.               |
| 124 | Position of Trust & Authority: Dodson's executive position allowed him to control bank accounts and disseminate financial information.                                       |
|     | Lack of Segregation of Duties: His ability to raise funds, control accounts, and manage financial information indicates a failure in separating responsibilities.            |
|     | Poor Audit Performance and Management Oversight: The ability to engage in fraudulent activities for years points to weak auditing and managerial supervision.                |

|     |   |
|-----|---|
|     | Poor Accounting System: The ease with which financial records were manipulated indicates systemic weaknesses in financial control.                        |
| 125 | Position of Trust & Authority: Phelps' position allowed him to influence the credit approval process.   |
|     | Lack of Segregation of Duties: His involvement in reviewing and approving fraudulent financial information.   |
|     | Poor Audit Performance and Management Oversight: Ineffectiveness in detecting the fraud scheme and auditing the credit process.                           |
|     | Lack of Systems of Authorization: Inadequate controls to validate the authenticity of financial information.  |
|     | Size of Organization: Larger organizations such as banks have a complex structure and tend to have a weaker control over processes, facilitating fraud.   |
| 126 | Position of Trust & Authority: Schessel used his position as CEO to influence investor perceptions and company announcements.                             |
|     | Lack of Segregation of Duties: His ability to make unilateral statements without checks indicates a failure in duty segregation.                          |
|     | Poor Audit Performance and Management Oversight: The inability to detect false statements suggests inadequate managerial supervision.                     |
| 127 | Position of Trust & Authority: Lucas's position enabled him to control financial affairs and make decisions on tax withholdings and payments.             |
|     | Poor Audit Performance and Management Oversight: The ability to evade tax payments over several years points to weak auditing and managerial supervision. |
|     | Poor Payroll Management: Mismanaging employee withholdings and failing to fulfill tax obligations indicates poor payroll management.                      |
| 128 | Position of Trust & Authority: Clark's roles as a trader and company president provided him with access to sensitive information and trading authority.   |
|     | Poor Audit Performance and Management Oversight: Prolonged undetected insider trading and kickbacks point to weak auditing and managerial supervision.    |
|     | Lack of Systems of Authorization: The absence of robust controls to authorize and monitor trading activities.   |



|     |   |
|-----|---|
| 129 | Position of Trust & Authority: Abbas's role as the owner of the healthcare agency gave her direct control over the handling of funds.                             |
|     | Lack of Segregation of Duties: Her ability to issue checks without additional oversight indicates inadequate segregation of financial duties.                     |
|     | Lack of Systems of Authorization: The ease with which the funds were diverted for personal use indicates weak financial control and authorization systems.        |
| 130 | Position of Trust & Authority: The executives' roles allowed them to manipulate loan information and SBA applications.  |
|     | Poor Audit Performance and Management Oversight: The prolonged and large-scale nature of the fraud suggests weak auditing and oversight.                          |
| 131 | Position of Trust & Authority: As directors, Verbeeck and Van Mele held positions that allowed them to influence contract bidding processes.                      |
|     | Poor Procurement policies: Failure to detect and prevent collusion in the bidding process suggests a lack of effective monitoring.                                |
| 132 | Position of Trust & Authority: Harry's ownership gave him the authority to direct company operations and manipulate transactions.                                 |
|     | Lack of Independent Checks and Control of the Accounting System: The manipulation of financial transactions for kickbacks indicates inadequate internal controls. |
|     | Poor Monitoring and Security of Personal Data: Utilizing straw owners and foreign shell companies demonstrates a lack of effective monitoring.                    |
|     | Poor Procurement policies: Accepting bribes and kickbacks and directing of payments to shell companies suggests a lack of control over procurement policies.      |
| 133 | Poor Monitoring and Security of Personal Data: The use of financial systems to launder money indicates inadequate safeguards.                                     |
|     | Absence of Cash Reconciliation and Surprise Checks on Cash: A lack of mechanisms to verify the legitimacy of transactions.  |
|     | Lack of independent checks and control of the accounting system: Failure to detect and prevent large-scale money laundering activities.                           |
| 134 | Position of Trust & Authority: Ray's role as City Clerk gave her direct access to and control over municipal funds.   |

|     |   |
|-----|---|
|     | Lack of Segregation of Duties: Her ability to issue checks, handle cash, and manage financial records without adequate checks indicates a failure in separating duties.       |
|     | Poor Audit Performance and Management Oversight: The ability to embezzle funds over several years points to weak auditing and managerial supervision.                         |
|     | Lack of Systems of Authorization: Inadequate controls in authorizing financial transactions and verifying their legitimacy.   |
|     | Poor Payroll management: The ease with which payroll records were manipulated indicates systemic weaknesses in payroll processes.   |
| 135 | Position of Trust & Authority: Their executive roles in the banks provided them with the means to facilitate and conceal fraudulent transactions.                             |
|     | Lack of independent checks and control of the accounting system: Their positions allowed them to oversee and manipulate financial transactions without adequate checks.       |
|     | Poor Audit Performance and Management Oversight: The failure to detect this complex scheme over a decade points to weak auditing and managerial supervision.                  |
|     | Poor Accounting and Procurement Policies: The ability to move large sums of money and record them as legitimate expenses indicates systemic weaknesses in financial controls. |
|     | Absence of Cash Reconciliation and Surprise Checks on Cash: A lack of mechanisms to reconcile and verify the authenticity of large financial transactions.                    |
| 136 | Position of Trust & Authority: Halilov's role in the NGO allowed him access to sensitive procurement details and the power to influence contract awards.                      |
|     | Poor Audit Performance and Management Oversight: The scheme's success over several years suggests inadequate auditing and managerial supervision.                             |
|     | Lack of Systems of Authorization: The ease with which Halilov could access and distribute confidential information indicates weak authorization and security systems.         |
|     | Poor Procurement policies: The ability to manipulate bidding processes for personal gain highlights significant gaps in oversight and control of procurement activities.      |
| 137 | Position of Trust & Authority: Their roles within the financial institution provided the opportunity to manipulate loan processes.  |

|     |   |
|-----|---|
|     | <p>Poor Audit Performance and Management Oversight: The prolonged undetected fraud suggests inadequate auditing and managerial supervision within the loan origination process.</p> <p>Lack of Systems of Authorization: Inadequate controls and checks in the verification and approval of loans, allowing for the approval of fraudulent applications.</p> <p>Poor Control of Signed Cheques and Financial Transactions: The ability to manipulate financial transactions and documents without detection points to weak controls in managing and authorizing financial activities.</p> <p>Lack of independent checks and control of the accounting system: Failure to detect and prevent fraudulent loan origination activities over several years suggests insufficient monitoring and verification mechanisms.</p> |
| 138 | <p>Position of Trust &amp; Authority: Barry's role as a deputy campaign manager and consultant provided him with the authority and access to direct financial transactions.</p> <p>Lack of Segregation of Duties: His ability to both manage and direct funds without additional checks indicates a failure in segregating financial responsibilities.</p> <p>Poor Audit Performance and Management Oversight: The sustained nature of the fraud suggests inadequate auditing and managerial supervision.</p> <p>Poor Control of Signed Cheques: The ability to misdirect funds to personal accounts indicates poor control over financial instruments like checks.</p>   |
| 139 | <p>Position of Trust &amp; Authority: Lewis's position as an accounts payable clerk gave her direct access to and control over vendor payments.</p> <p>Lack of Segregation of Duties: Her ability to prepare, handle, and divert checks indicates a failure in separating financial responsibilities.</p> <p>Poor Audit Performance and Management Oversight: The prolonged undetected fraud suggests inadequate auditing and managerial supervision.</p> <p>Poor control of signed cheques: The ease with which Lewis manipulated cheque payment system indicates systemic weaknesses in financial control.</p>  |
| 140 | <p>Poor Monitoring and Security of Personal Data: A lack of mechanisms to detect Xiao's affiliations with foreign entities and undisclosed financial engagements.</p>   |

|     |   |
|-----|---|
|     | Lack of Independent Checks and Control of the Accounting System: Insufficient verification of Xiao's financial disclosures and background checks related to his grant activities. |
| 141 | Position of Trust & Authority: Scott's position as the owner of a telemarketing call center provided him with the means to influence and deceive beneficiaries.                   |
|     | Poor Monitoring and Security of Personal Data: Exploiting Medicare beneficiaries' information for fraudulent purposes indicates a lack of secure data handling.                   |
|     | Poor Procurement Policies: The process of obtaining and selling doctor's orders and genetic tests without proper validation suggests weak procurement policies.                   |
| 142 | Position of Trust & Authority: Brassart's control over his financial affairs and use of corporations suggests a position of authority enabling his fraudulent actions.            |
|     | Lack of Independent Checks and Control of the Accounting System: Brassart exploited weaknesses in tax oversight and bankruptcy procedures.  |
| 143 | Position of Trust & Authority: As a trader, Heredia had the authority to influence market operations and trading decisions.   |
|     | Lack of Segregation of Duties: His ability to direct trading activities without adequate checks indicates a failure in separating responsibilities.                               |
|     | Poor Audit Performance and Management Oversight: The ability to engage in price manipulation over several years points to weak auditing and managerial supervision.               |
| 144 | Position of Trust & Authority: Ribas's roles as chairman and advisor gave him significant influence over contract decisions.  |
|     | Lack of Segregation of Duties: Ribas's ability to influence contract awards without checks and balances highlights a failure in duty segregation.                                 |
|     | Poor Audit Performance and Management Oversight: The extended duration of the scheme suggests a lack of effective auditing and supervision.                                       |
|     | Poor Procurement policies: The operation of the bribery scheme suggests a lack of transparency in the contract awarding process and a failure to hold key individuals accountable |
| 145 | Position of Trust & Authority: Sabet's ownership provided direct control over pharmacy operations and financial dealings.   |

|     |  |
|-----|--|
|     | Poor Monitoring and Security of Personal Data: Inadequate safeguards against misuse of customer information for fraud.   |
| 146 | Position of Trust & Authority: As CEO, Rashid held a position of authority, allowing him to dictate unethical practices.   |
|     | Lack of Independent Checks and Control of the Accounting System: Insufficient oversight of billing practices and financial transactions.   |
|     | Poor Procurement Policies: Lack of proper protocols to ensure that medical procedures were necessary and not driven by financial incentives.   |
|     | Absence of Cash Reconciliation and Surprise Checks on Cash: A lack of mechanisms to reconcile financial records with actual medical practices.   |
| 147 | Position of Trust & Authority: Sreckovic's managerial role allowed him to oversee and manipulate financial transactions.   |
|     | Lack of Segregation of Duties: His ability to unilaterally direct payroll activities and financial decisions indicates a failure in separating financial responsibilities.                     |
|     | Poor Audit Performance and Management Oversight: The failure to detect non-compliance with tax obligations for several years suggests a lack of effective auditing and managerial supervision. |
|     | Poor Payroll management: Sreckovic's ability to stop tax payments without triggering internal alarms points to significant weaknesses in the payroll processes.                                |
| 148 | Position of Trust & Authority: Devillez's role in handling vendor payments gave him direct control over financial transactions.  |
|     | Lack of Segregation of Duties: His ability to prepare, approve, and execute payments without additional oversight indicates inadequate separation of financial responsibilities.               |
|     | Poor Audit Performance and Management Oversight: The prolonged undetected misappropriation suggests ineffective auditing and managerial supervision.   |
|     | Lack of Systems of Authorization: Inadequate controls in verifying the authenticity of payments and reconciliation with vendor accounts.   |
| 149 | Position of Trust & Authority: Their positions in the physician's office gave them access to prescription pads and the ability to create forgeries.  |
|     | Lack of Physical and Digital Access Controls: Insufficient safeguards on access to prescription pads and verification of prescription authenticity.  |

|     |   |
|-----|---|
|     | Poor Monitoring and Security of Personal Data: A lack of mechanisms to detect inappropriate use of patient information or prescription resources.   |
| 150 | Position of Trust & Authority: Mercedes' access to the company's system as a payment processor enabled her to manipulate transactions.  |
|     | Lack of Segregation of Duties: Her ability to both create and approve wire transfers indicates a failure in internal control segregation.   |
|     | Poor Audit Performance and Management Oversight: The prolonged, undetected nature of the fraud suggests insufficient auditing and managerial supervision.   |
|     | Lack of Physical and Digital Access Controls: The ease with which she accessed and manipulated the computer system points to weak digital security measures.  |
|     | Poor Control of Signed Cheques: Exploiting the escrow check process without detection indicates inadequate control over check handling.   |
| 151 | Position of Trust & Authority: As CFO and finance executives, they had significant control over financial reporting.  |
|     | Lack of Independent Checks and Control of the Accounting System: Inadequate oversight and verification of financial disclosures.  |
|     | Poor Audit Performance and Management Oversight: Failure of internal and external audits to identify fraudulent activities.   |
| 152 | Position of Trust & Authority: Moreland's role as a judge gave him significant influence over the operations of the Drug Court Foundation.  |
|     | Lack of Segregation of Duties: His ability to direct financial transactions without appropriate checks and balances.  |
|     | Poor Audit Performance and Management Oversight: The prolonged undetected embezzlement points to weak auditing and managerial supervision.  |
|     | Lack of Systems of Authorization: Inadequate verification processes for financial transactions within the foundation.   |
|     | Absence of Cash Reconciliation and Surprise Checks on Cash: Lack of proper financial reconciliation processes that could have detected the misappropriation of funds.   |
| 153 | Poor Audit Performance and Management Oversight: Deloitte's alleged deviation from auditing standards and failure to identify TBW's fraudulent activities indicates a significant lapse in audit quality and oversight. |

|     |   |
|-----|---|
| 154 | Position of Trust & Authority: Calaiaro's role as an office manager provided him with access to checks and financial records.   |
|     | Lack of Segregation of Duties: His ability to both access and forge checks indicates a failure to separate duties effectively.  |
|     | Poor Control of Signed Cheques: The ease with which he could forge signatures suggests inadequate controls over check issuance and signature verification.              |
| 155 | Position of Trust & Authority: Hauk's role as an accountant gave him access and control over client funds.  |
|     | Lack of Segregation of Duties: His ability to manage client accounts and conduct transactions without additional oversight.   |
|     | Poor Audit Performance and Management Oversight: The failure to detect the fraudulent activities over several years points to weak auditing and managerial supervision. |
|     | Poor Monitoring and Security of Personal Data: The ease of stealing identity and using fraudulent checks suggests inadequate data security.                             |
|     | Poor Accounting System: The ability to manipulate financial records indicates systemic weaknesses in financial controls.  |
| 156 | Position of Trust & Authority: Both individuals abused their trusted positions within the DEA to conceal their external activities.                                     |
|     | Lack of Segregation of Duties: As DEA employees, they should have had their external interests and activities more closely monitored.                                   |
|     | Hiring without Background Checks: The failure to uncover undisclosed external employment indicates a weakness in verifying employee disclosures.                        |
| 157 | Position of Trust & Authority: Cummings' role at TCI provided him with access to sensitive information, which he exploited.   |
|     | Lack of Segregation of Duties: His role included responsibilities that allowed him unsupervised access to confidential data.  |
|     | Poor Monitoring and Security of Personal Data: The scheme highlights a failure in adequately monitoring and securing sensitive customer data.                           |

APPENDIX E:  
ANALYSIS OF BEHAVIOURAL FLAGS

| Case | Analysis Data  |
|------|--|
| 1    | Living Beyond Their Means: Stollery used investor funds for personal luxury expenses.  |
|      | Desire for Personal Gain: Deceived investors to misappropriate funds for personal use.   |
|      | Scheming attitude: Falsified white papers and testimonials to deceive investors.   |
|      | Challenge to beat the system: Failed to register ICO with the SEC to avoid regulations.  |
|      | Family pressure: Misappropriated funds for personal bills and expenses.  |
| 2    | Desire for Personal Gain: Accepted bribes, indicating a strong motivation for personal enrichment.                                       |
|      | Challenge to Beat the System: Engaging in bribery suggests a mentality of outsmarting legal and ethical boundaries.                      |
|      | Scheming Attitude: The systematic acceptance of bribes over an extended period indicates a calculated, scheming behavior.                |
| 3    | Living Beyond Their Means: The extravagant personal expenses at luxury stores indicate a lifestyle beyond his means.                     |
|      | Desire for Personal Gain: His actions were clearly motivated by personal financial gain.   |
|      | Challenge to Beat the System: Continuously misusing funds over several years shows a challenge to beat the system.                       |
| 4    | Living Beyond Their Means: The purchase of luxury items and a cat treadmill indicates lifestyle expenses beyond her legitimate earnings. |
|      | Desire for Personal Gain: Murray's actions were driven by personal financial gain.   |
| 5    | Desire for Personal Gain: Both Hickman and Whiteman engaged in the scheme for personal financial benefit.                                |
|      | Scheming Attitude: The elaborate plan to divert sales and conceal the involvement of Heritage demonstrates a scheming attitude.          |



|    |   |
|----|---|
| 6  | Living Beyond Their Means: The substantial amount stolen suggests spending beyond her regular income.   |
|    | Desire for Personal Gain: The act of embezzlement itself indicates a desire for personal financial benefit.   |
| 7  | Living Beyond Their Means: Extravagant spending on personal luxuries.   |
|    | Desire for Personal Gain: Engaging in fraudulent activities for self-enrichment.  |
|    | Scheming Attitude: Methodically creating false documents and transactions.  |
| 8  | Living Beyond Their Means: The large amount of money received suggests a lifestyle possibly beyond his legitimate earnings.                         |
|    | Desire for Personal Gain: Accepting bribes clearly indicates a motivation for personal financial gain.  |
|    | No Recognition at the Workplace: Possibly driven by a lack of recognition in his professional field, leading to unethical behavior.                 |
| 9  | Living Beyond Their Means: The large sum embezzled suggests a lifestyle surpassing his legitimate income.   |
|    | Desire for Personal Gain: Clearly driven by personal financial benefit.   |
|    | Scheming Attitude: Manipulating bank records and creating fake loans indicate a calculated approach to fraud.                                       |
| 10 | Living Beyond Their Means: The embezzlement might indicate financial pressure or a lifestyle beyond Cherry's legitimate earnings.                   |
|    | Desire for Personal Gain: Cherry's actions were primarily driven by the desire for personal gain, possibly influenced by her personal relationship. |
|    | Family Pressure: Giving the stolen money to her boyfriend suggests influence or pressure from a family or close relationship.                       |
| 11 | Living Beyond Their Means: Utilization of corporate credit for personal expenses indicates a lifestyle beyond her legitimate income.                |
|    | Desire for Personal Gain: The systematic embezzlement for personal financial benefit is evident.  |
|    | Scheming Attitude: The complexity of her scheme, including identity theft, shows a scheming mindset.  |

|    |  |
|----|--|
| 12 | Living Beyond Their Means: Lindberg's use of funds for personal real estate indicates living extravagantly.                                |
|    | Desire for Personal Gain: Misappropriation of insurance company funds for personal benefits reflects a strong personal gain motive.        |
|    | Scheming Attitude: The complexity and scale of the scheme demonstrate a calculated and scheming mindset.                                   |
| 13 | Living Beyond Their Means: The use of embezzled funds for personal expenses indicates living beyond means.                                 |
|    | Desire for Personal Gain: Misusing position for personal financial gain.   |
|    | High Personal Debt: Payments towards personal loans and credit cards suggest high personal debt.   |
|    | Scheming Attitude: The methodical alteration of payroll information shows a calculated approach to fraud.                                  |
| 14 | Living Beyond Their Means: The lavish expenditures suggest a lifestyle exceeding her financial means.                                      |
|    | Desire for Personal Gain: The embezzlement for personal expenses and benefits clearly indicates a motive for personal gain.                |
|    | Scheming Attitude: The continuous and varied use of funds for personal benefit shows a calculated approach.                                |
| 15 | Living Beyond Their Means: The large amount of fraudulent claims suggests a lifestyle requiring significant financial resources.           |
|    | Desire for Personal Gain: The deliberate participation in the fraud scheme for personal enrichment.  |
|    | Scheming Attitude: Orchestrating a complex fraud scheme demonstrates a calculated, deceptive approach.                                     |
|    | Challenge to Beat the System: Engaging in an elaborate fraud to deceive a well-established health care plan.                               |
| 16 | Living Beyond Their Means: Spending trust funds at casinos indicates a lifestyle beyond her means.   |
|    | Desire for Personal Gain: Misappropriation of funds for personal use, including home improvements, shows a clear desire for personal gain. |
|    | Scheming Attitude: The forging of ledger entries to hide her activities demonstrates a calculated and deceptive approach.                  |
|    | Challenge to Beat the System: Her continuous fraudulent activities reflect a challenge to outwit the system.                               |

|    |  |
|----|--|
| 17 | Living Beyond Their Means: Using defrauded money for personal benefit suggests a lifestyle exceeding legitimate earnings.                      |
|    | Desire for Personal Gain: The scheme was motivated by the desire to financially benefit himself and his family.                                |
|    | Challenge to Beat the System: Orchestrating a long-term fraudulent scheme reflects a mentality of outsmarting the system.                      |
|    | Scheming Attitude: The creation of MES and the concealment of his interest indicate a calculated, deceptive approach.                          |
| 18 | Living Beyond Their Means: The large-scale theft suggests a lifestyle or ambitions beyond legitimate means.                                    |
|    | Desire for Personal Gain: The deliberate creation of a fake company and fraud for substantial financial gain.                                  |
|    | Scheming Attitude: The complex arrangement of fraud and money laundering shows a calculated, scheming approach.                                |
|    | Close Association with the Customer or Vendor: The conspiracy involved a close familial relationship, used to facilitate fraud.                |
|    | Challenge to Beat the System: The prolonged fraudulent activity demonstrates a mindset of trying to outsmart the system.                       |
| 19 | Gambling Habits: Usage of embezzled funds for vacations and gambling.  |
|    | Desire for Personal Gain: Embezzlement to finance personal luxuries.   |
|    | Gambling Habits: The money was used for casino gambling.   |
|    | Scheming Attitude: Maintained the scheme through deliberate false entries.   |
| 20 | Living Beyond Their Means: Alexandre's purchase of luxury cars like BMW and Mercedes Benz suggests a lifestyle beyond his legitimate means.    |
|    | Desire for Personal Gain: The misappropriation of investor funds for personal purchases indicates a strong motive for personal financial gain. |

|    |  |
|----|--|
|    | <p>Scheming Attitude: The creation and operation of a fraudulent investment platform demonstrate a calculated and manipulative approach.</p> <p>Challenge to Beat the System: By fabricating returns and misleading investors, Alexandre demonstrated a desire to outsmart the system.</p>   |
| 21 | <p>Scheming Attitude: The intricate scheme to disguise loan realities indicates a scheming mindset.</p> <p>Desire for Personal Gain: Engaging in fraud to maintain his position and bank's appearance suggests a desire for personal and professional gain.</p> <p>Challenge to Beat the System: Persistently misleading auditors and examiners demonstrates a challenge to beat the system.</p>   |
| 22 | <p>Living Beyond Their Means: Unauthorized purchases and cash withdrawals suggest a lifestyle beyond her means.</p> <p>Desire for Personal Gain: Her actions to overpay herself and misuse funds indicate a strong motive for personal financial gain.</p> <p>Scheming Attitude: The systematic theft over an extended period shows a calculated, scheming approach.</p>   |
| 23 | <p>Living Beyond Their Means: The significant amount embezzled suggests a lifestyle beyond her legitimate earnings.</p> <p>Desire for Personal Gain: The deliberate manipulation to increase her salary indicates a strong motive for personal financial gain.</p> <p>Scheming Attitude: The complexity and duration of the fraudulent scheme demonstrate a calculated approach.</p>   |
| 24 | <p>Living Beyond Their Means: The use of embezzled funds for personal expenses suggests a lifestyle beyond legitimate means.</p> <p>Desire for Personal Gain: The motive behind the fraud was personal financial gain.</p> <p>Gambling Habits: The use of stolen funds for gambling indicates problematic gambling behavior.</p> <p>Scheming Attitude: The systematic and continuous forgery and embezzlement over several years demonstrate a scheming mindset.</p> |

|    |   |
|----|---|
| 25 | Living Beyond Their Means: Cashing checks for personal expenses suggests Tigler was living beyond her means.                        |
|    | Scheming Attitude: The systematic forgery and concealment of embezzlement reveal a calculated, deceitful behavior.                  |
|    | Gambling Habits: The failure to report gambling winnings indicates a habit of gambling.   |
|    | Challenge to Beat the System: Tigler's complex scheme to defraud the bank and the tax system shows a desire to outsmart the system. |
| 26 | Living Beyond Their Means: Using stolen funds for personal expenses and gambling indicates living beyond his financial means.       |
|    | Desire for Personal Gain: Misappropriating client funds for self-enrichment reflects a primary motive for personal gain.            |
|    | Gambling Habits: The misuse of funds for gambling suggests a problematic habit contributing to the fraud.                           |
|    | Scheming Attitude: Deceiving clients under the pretense of investment demonstrates a calculated, deceptive approach.                |
| 27 | Desire for Personal Gain: Sharp's attempt to extort \$2 million demonstrates a clear motive for personal financial gain.            |
|    | Scheming Attitude: Orchestrating a complex fraud and extortion scheme shows a calculated, deceptive mindset.                        |
|    | Living Beyond Their Means: The scale of the demanded ransom suggests aspirations beyond a legitimate income.                        |
| 28 | Living Beyond Their Means: The embezzlement suggests a lifestyle potentially beyond her means.                                      |
|    | Desire for Personal Gain: Misappropriating funds for personal gain was the primary motive.  |
|    | Scheming Attitude: Continuously accessing and misusing funds over several years demonstrates a calculated and deceptive behavior.   |
| 29 | Living Beyond Their Means: Misappropriation of funds for personal expenses suggests a lifestyle beyond legitimate earnings.         |

|    |  |
|----|--|
|    | <p>Desire for Personal Gain: The deliberate misappropriation of client funds indicates a primary motive of personal financial gain.</p> <p>Scheming Attitude: The complexity and duration of the fraud demonstrate a calculated and deceptive mindset.</p> <p>Challenge to Beat the System: Manipulating legal settlements and deceiving clients and the legal system shows an attitude of outsmarting the system.</p>   |
| 30 | <p>Living Beyond Their Means: Cory's use of fraudulently obtained funds for personal expenses indicates living beyond means.</p> <p>Desire for Personal Gain: Orchestrating a scheme for personal financial enrichment.</p> <p>Scheming Attitude: Creation of a shell company and fabrication of consulting services demonstrate a calculated approach.</p> <p>Challenge to Beat the System: Evading taxes over several years shows an attempt to outsmart the legal system.</p> |
| 31 | <p>Living Beyond Their Means: Significant personal purchases suggest a lifestyle beyond his legitimate income.</p> <p>Desire for Personal Gain: Deliberately embezzling funds and evading tax payments demonstrate a strong motive for personal gain.</p> <p>Challenge to Beat the System: His evasion from the law and manipulative conduct indicate a challenge to beat the system.</p>  |
| 32 | <p>Desire for Personal Gain: Groom's involvement in diverting funds for personal use demonstrates this motive.</p> <p>Scheming Attitude: The creation of a shell company and the recruitment of an impersonator indicate a calculated, deceptive approach.</p> <p>Challenge to Beat the System: The elaborate scheme to defraud a tribe shows an attempt to outsmart regulatory and oversight mechanisms.</p>  |
| 33 | <p>Living Beyond Their Means: Misappropriation of \$1.3 million for personal expenses indicates living beyond financial means.</p>   |

|    |   |
|----|---|
|    | Desire for Personal Gain: Dodson's deliberate misrepresentation to investors suggests a strong desire for personal financial gain.                            |
|    | Scheming Attitude: Systematic misrepresentation and fund misappropriation show a calculated, deceitful approach.  |
| 34 | Desire for Personal Gain: Bernardi's actions were driven by the motive to financially benefit his company and potentially himself.                            |
|    | Scheming Attitude: The creation of fabricated documents and impersonation indicate a calculated, deceptive approach.  |
|    | Challenge to Beat the System: The complexity of the fraud scheme shows an attempt to outsmart investors and lenders.  |
| 35 | Living Beyond Their Means: The substantial amount embezzled suggests Jackson was living beyond her means.   |
|    | Desire for Personal Gain: Stealing and transferring funds for personal use demonstrates a clear motive for personal gain.                                     |
|    | Scheming Attitude: The use of various methods to embezzle funds over several years indicates a calculated, scheming approach.                                 |
|    | Challenge to Beat the System: The sophisticated means of concealing her activities, like locking account access, reflects a challenge to outsmart the system. |
| 36 | Living Beyond Their Means: Using embezzled funds for personal expenses suggests a lifestyle beyond her means.   |
|    | Desire for Personal Gain: The extent of embezzlement for personal use indicates a strong motive for personal financial gain.                                  |
|    | Scheming Attitude: Creating fake companies and manipulating invoices show a calculated, deceptive approach.   |
| 37 | Desire for Personal Gain: Briggs' participation in the fraud scheme was motivated by personal financial gain.   |
|    | Scheming Attitude: Her systematic theft of customer information for fraudulent purposes indicates a scheming approach.  |

|    |  |
|----|--|
|    | Challenge to Beat the System: Involvement in an elaborate fraud scheme demonstrates a desire to outsmart banking systems.                                  |
| 38 | Desire for Personal Gain: Engaging in bid-rigging for contracts worth over \$17.2 million indicates a strong motive for personal financial gain.           |
|    | Scheming Attitude: The systematic and deliberate manipulation of the bidding process demonstrates a calculated, deceptive mindset.                         |
|    | Challenge to Beat the System: The involvement in an extensive bid-rigging conspiracy shows an attempt to outsmart regulatory systems.                      |
| 39 | Living Beyond Their Means: Personal expenditures like family dinners at expensive restaurants indicate living beyond means.                                |
|    | Desire for Personal Gain: Using organizational funds for personal expenses reflects a strong motive for personal gain.                                     |
|    | Challenge to Beat the System: Misusing funds and underreporting income for years shows an attempt to outsmart the system.                                  |
|    | No Recognition at the Workplace: As CEO, seeking additional, illegitimate ways to benefit financially might indicate a perceived lack of recognition.      |
| 40 | Scheming Attitude: The systematic and prolonged embezzlement and covering up indicate a scheming mindset.  |
|    | Living Beyond Their Means: Misappropriating large sums suggests lifestyle expenses beyond legitimate income.   |
|    | Challenge to Beat the System: Constant manipulation of the payroll system and lying about transactions show an intent to outsmart organizational controls. |
| 41 | Living Beyond Their Means: The scale of the fraud suggests spending beyond her legitimate income.  |
|    | Desire for Personal Gain: The systematic fraud for personal expenses indicates a clear motive for personal financial gain.                                 |



|    |   |
|----|---|
|    | <p>Scheming Attitude: The complexity and duration of the fraudulent activities demonstrate a deliberate and calculated approach.</p> <p>No Recognition at the Workplace: Engaging in fraud after termination might indicate feelings of entitlement or lack of recognition.</p>   |
| 42 | <p>Living Beyond Their Means: Funding an extravagant lifestyle through embezzlement suggests living beyond means.</p> <p>Desire for Personal Gain: Engaging in fraud for personal benefits like vacations and surgeries indicates a strong personal gain motive.</p> <p>Scheming Attitude: Complex schemes involving inflated invoices and sham bank accounts show a calculated, deceptive mindset.</p> <p>Challenge to Beat the System: Manipulating contractor payments and deceiving a mortgage lender demonstrate an attempt to outsmart financial systems.</p> |
| 43 | <p>Living Beyond Their Means: The large sum embezzled suggests Skidmore was spending beyond her legitimate earnings.</p> <p>Desire for Personal Gain: Her actions clearly indicate a primary motive of personal financial gain.</p> <p>Scheming Attitude: Creating fictitious invoices and manipulating records shows a calculated approach to fraud.</p> <p>Challenge to Beat the System: Successfully carrying out a complex scheme over several years demonstrates an attempt to outsmart organizational controls.</p>   |
| 44 | <p>Living Beyond Their Means: Diverting company funds for personal use suggests a lifestyle exceeding personal financial means.</p> <p>Desire for Personal Gain: The act of fraudulently acquiring money indicates a strong desire for personal gain.</p> <p>Scheming Attitude: The systematic approach to defraud her employer and financial institutions shows a calculated, deceptive mindset.</p>   |
| 45 | <p>Desire for Personal Gain: Carroll's creation of a scheme to overcharge the university reflects a strong motive for personal financial gain.</p>  |

|    |   |
|----|---|
|    | <p>Scheming Attitude: The complexity of setting up a corporation and creating false invoices demonstrates a calculated, deceptive approach.</p> <p>Challenge to Beat the System: Deceiving the university's leadership and managing fraudulent transactions indicate an attempt to outsmart organizational controls.</p>  |
| 46 | <p>Living Beyond Their Means: The transfer of stolen money for personal expenses suggests a lifestyle beyond her financial means.</p> <p>Desire for Personal Gain: The intentional theft of a large sum of money indicates a strong motive for personal gain.</p> <p>Scheming Attitude: Orchestrating a complex scheme involving identity theft and fraudulent transfers demonstrates a calculated, deceptive approach.</p>           |
| 47 | <p>Living Beyond Their Means: Spending excessively at adult entertainment clubs indicates a lifestyle beyond his financial capacity.</p> <p>Desire for Personal Gain: The systematic misuse of company funds for personal entertainment demonstrates a strong inclination for personal gain.</p> <p>Challenge to Beat the System: Repeatedly using the company card for personal expenses shows an attempt to exploit the system.</p> |
| 48 | <p>Living Beyond Their Means: Expenditures on luxury items, travel, and entertainment suggest a lifestyle beyond legitimate means.</p> <p>Desire for Personal Gain: The systematic embezzlement for personal enrichment demonstrates a strong motive for personal gain.</p> <p>Challenge to Beat the System: Continuously increasing the scale of embezzlement over years shows an attempt to outsmart organizational controls.</p>   |
| 49 | <p>Living Beyond Their Means: Obtaining loans under false pretenses suggests a lifestyle beyond legitimate financial means.</p> <p>Desire for Personal Gain: The fraudulent loan applications and embezzlement indicate a motive for personal gain.</p>   |

|    |  |
|----|--|
|    | <p>Scheming Attitude: Applying for loans with false information while facing legal trouble for embezzlement demonstrates a calculated, deceptive approach.</p> <p>Challenge to Beat the System: Engaging in fraud during legal proceedings for similar misconduct shows a disregard for legal constraints and a desire to outsmart the system.</p>   |
| 50 | <p>Living Beyond Their Means: The large sum embezzled suggests a lifestyle far beyond her legitimate income.</p> <p>Desire for Personal Gain: Her extensive embezzlement over several years clearly indicates a motive for personal financial gain.</p> <p>Scheming Attitude: The methodical approach to embezzlement and crafting false paperwork shows a calculated and deceptive behavior.</p>  |
| 51 | <p>Scheming Attitude: The conspiracy and intentional submission of incomplete information demonstrate a calculated, deceptive approach.</p> <p>Desire for Personal Gain: Selling personal shares for profit based on the fraudulent scheme shows a clear motive for personal financial gain.</p> <p>Challenge to Beat the System: Deliberately misleading investors and regulatory bodies indicate an attempt to outsmart market and regulatory systems.</p> |
| 52 | <p>Living Beyond Their Means: Using embezzled funds for personal expenses and credit card bills indicates living beyond financial means.</p> <p>Desire for Personal Gain: The act of embezzling large sums for personal use demonstrates a strong motivation for personal gain.</p> <p>Scheming Attitude: Altering bank statements to conceal embezzlement shows a calculated, deceptive approach.</p>   |
| 53 | <p>Desire for Personal Gain: Orchestrating a scheme for financial benefits indicates a strong motivation for personal gain.</p> <p>Scheming Attitude: Deliberate selection of ineligible loans and falsifying information demonstrate a calculated, deceptive approach.</p>  |

|    |   |
|----|---|
|    | Challenge to Beat the System: Manipulating loan information to deceive a bank and investors shows an attempt to outsmart financial systems.             |
| 54 | Living Beyond Their Means: Using stolen money to pay personal expenses suggests spending beyond his financial means.                                    |
|    | Desire for Personal Gain: Creating and approving fraudulent invoices for personal benefit indicates a strong motive for personal gain.                  |
|    | Scheming Attitude: Systematically submitting and approving fraudulent invoices over years demonstrates a calculated, deceptive mindset.                 |
| 55 | Living Beyond Their Means: Using stolen funds for home renovations and luxury purchases indicates a lifestyle beyond her financial means.               |
|    | Desire for Personal Gain: Increasing her salary and using company funds for personal use demonstrate a strong motivation for personal enrichment.       |
|    | Scheming Attitude: The deliberate manipulation of payroll and concealment of her activities show a calculated, deceptive approach.                      |
| 56 | High Personal Debt: The failure to pay taxes might indicate financial pressure or high personal debt.   |
|    | Desire for Personal Gain: Avoiding tax payments demonstrates a motive for personal financial gain.  |
|    | Challenge to Beat the System: Submitting false tax forms and evading taxes for multiple years shows an attempt to outsmart legal and financial systems. |
| 57 | Desire for Personal Gain: Patel's orchestration of a large-scale fraud for significant financial gain.  |
|    | Scheming Attitude: The complex scheme involving kickbacks, telemarketing, and false claims indicates a calculated, deceitful approach.                  |
|    | Living Beyond Their Means: Earning over \$21 million from fraudulent activities suggests a lifestyle beyond legitimate financial means.                 |

|    |  |
|----|--|
| 58 | Living Beyond Their Means: The use of company funds for personal purchases suggests living a lifestyle beyond personal financial means.              |
|    | Desire for Personal Gain: Embezzling company funds for personal use indicates a strong motivation for personal gain.                                 |
|    | Scheming Attitude: Manipulating company finances over a prolonged period demonstrates a calculated and deceptive approach.                           |
|    | Challenge to Beat the System: Failing to pay large sums of taxes and committing bank fraud shows an attempt to outsmart financial and legal systems. |
| 59 | Living Beyond Their Means: Using customer funds for personal expenses and political contributions indicates living extravagantly.                    |
|    | Desire for Personal Gain: Misappropriating customer funds for personal investments and loan repayments shows a clear motive for personal gain.       |
|    | Scheming Attitude: The complex nature of the fraud and efforts to conceal it demonstrate a calculated, deceptive approach.                           |
| 60 | Living Beyond Their Means: The significant amount spent on personal items like a bouncy house suggests living beyond personal financial means.       |
|    | Desire for Personal Gain: The continuous use of company funds for personal purchases indicates a strong motive for personal gain.                    |
|    | Scheming Attitude: The effort to mislabel transactions and conceal them from company owners shows a calculated and deceptive approach.               |
| 61 | Living Beyond Their Means: The embezzlement suggests Kewalis might have been living beyond her financial means.                                      |
|    | Desire for Personal Gain: Her actions indicate a clear motive for personal financial gain.   |
|    | Scheming Attitude: Creating fraudulent accounts and making unauthorized entries show a calculated and deceptive approach.                            |

|    |  |
|----|--|
| 62 | Living Beyond Their Means: Excessive personal purchases and services indicate living beyond financial means.                             |
|    | Desire for Personal Gain: Misappropriating company funds for personal use shows a strong desire for personal financial gain.             |
|    | Scheming Attitude: Creating fraudulent invoices and manipulating company resources demonstrate a calculated, deceptive approach.         |
| 63 | Living Beyond Their Means: Stealing cash indicates living a lifestyle beyond her legitimate earnings.                                    |
|    | Desire for Personal Gain: Directly taking cash from the bank shows a clear motive for personal financial gain.                           |
|    | Scheming Attitude: The methodical approach of stealing and covering it up by altering computer records demonstrates a scheming behavior. |
| 64 | Living Beyond Their Means: Using embezzled funds for personal credit card payments suggests a lifestyle beyond financial means.          |
|    | Desire for Personal Gain: Embezzling funds for personal benefit clearly indicates a motive for personal gain.                            |
|    | Scheming Attitude: Manipulating company finances and tax filings over several years demonstrates a deceptive and calculated approach.    |
| 65 | Living Beyond Their Means: The shopping addiction indicates spending beyond financial means.   |
|    | Desire for Personal Gain: Embezzling funds for personal use shows a clear motive for personal gain.                                      |
|    | Scheming Attitude: Systematically falsifying financial reports to conceal theft shows a deceptive, calculated approach.                  |
| 66 | Scheming Attitude: Orchestrating complex transactions to manipulate financial figures.   |
|    | Challenge to Beat the System: Manipulating data to surpass market expectations.  |
|    | High Personal Debt: Potentially driven by personal financial obligations or desires.   |
|    | No Recognition at the Workplace: Engaging in fraud to gain recognition for company performance.  |

|    |  |
|----|--|
| 67 | Living Beyond Their Means: The significant amount embezzled suggests living a lifestyle beyond her regular income.                                 |
|    | Desire for Personal Gain: Swanson's actions were clearly motivated by personal financial gain.   |
|    | Scheming Attitude: Altering payroll processes for personal benefit demonstrates a calculated and deceitful approach.                               |
| 68 | Living Beyond Their Means: Expenditure on luxury items and gambling suggests spending beyond financial means.                                      |
|    | Desire for Personal Gain: Kent's actions were clearly motivated by personal financial gain.  |
|    | Gambling Habits: Use of embezzled funds for gambling indicates a gambling habit.   |
| 69 | Desire for Personal Gain: Engaging in check kiting and not remitting taxes indicates a motive for personal financial benefit.                      |
|    | Scheming Attitude: The complex check kiting scheme demonstrates calculated and deceptive behavior.   |
|    | Living Beyond Their Means: The large amount involved in the fraud suggests spending or financial needs beyond legitimate means.                    |
| 70 | Desire for Personal Gain: The creation of fake companies and embezzlement of funds clearly show a strong desire for personal financial gain.       |
|    | Scheming Attitude: The systematic approach to creating fake companies and invoices indicates a calculated and deceptive mindset.                   |
|    | Challenge to Beat the System: Orchestrating a complex embezzlement scheme demonstrates an attempt to outsmart and exploit the system.              |
| 71 | Desire for Personal Gain: Manipulating financial records for maintaining business relationships indicates a motive for personal and business gain. |
|    | Scheming Attitude: Coordinating with an accountant to falsify records shows a calculated, deceptive approach to financial management.              |
| 72 | Desire for Personal Gain: The creation of fraudulent invoices for personal financial gain.   |

|    |  |
|----|--|
|    | Scheming Attitude: Elaborate manipulation of company procedures and use of family and friends' businesses for fraud.   |
|    | Living Beyond Their Means: The embezzlement may suggest a lifestyle beyond his legitimate income.  |
| 73 | Living Beyond Their Means: Purchasing a luxury item like a diamond ring indicates a lifestyle beyond normal financial means.                                 |
|    | Desire for Personal Gain: Embezzling funds for personal benefit clearly shows a motive for personal gain.  |
|    | Scheming Attitude: The systematic diversion of funds over time indicates a calculated, deceptive approach.   |
| 74 | Living Beyond Their Means: The embezzlement suggests spending beyond legitimate income.  |
|    | Desire for Personal Gain: The act of stealing from customer accounts clearly indicates a pursuit of personal financial gain.                                 |
|    | Scheming Attitude: Failing to report stolen money on tax returns shows a calculated effort to conceal illegal gains.   |
| 75 | Living Beyond Their Means: The use of embezzled funds for high-end purchases and personal events indicates living beyond financial means.                    |
|    | Desire for Personal Gain: The systematic embezzlement for personal benefit and funding her own business ventures demonstrates a strong personal gain motive. |
|    | Scheming Attitude: Manipulation of company communication and systematic embezzlement show a calculated and deceptive approach.                               |
| 76 | Living Beyond Their Means: Rogas's use of fraudulent proceeds for luxury purchases indicates a lifestyle beyond legitimate financial means.                  |
|    | Desire for Personal Gain: Manipulating financial data for substantial personal financial benefit reflects a strong motive for personal gain.                 |
|    | Scheming Attitude: The systematic alteration of financial documents and deception of investors and auditors demonstrate a calculated, deceptive mindset.     |
| 77 | Desire for Personal Gain: Demanding and accepting bribes for personal financial gain.  |



|    |   |
|----|---|
|    | Scheming Attitude: Systematically increasing demands and accepting bribes indicate a calculated approach.   |
|    | Challenge to Beat the System: Engaging in extortion while in a position of power shows a disregard for legal and ethical standards.                             |
| 78 | Desire for Personal Gain: Mensinger's orchestration of the loan scheme for his own financial benefit clearly demonstrates this motive.                          |
|    | Scheming Attitude: The deliberate manipulation of loan processes and use of false applications reflect a calculated, deceptive approach.                        |
|    | Challenge to Beat the System: Exploiting his position to bypass eligibility requirements for personal loans.  |
| 79 | Living Beyond Their Means: Using embezzled funds for personal services and expenses indicates living beyond legitimate financial means.                         |
|    | Desire for Personal Gain: Diverting customer payments to a personal account demonstrates a clear motive for personal financial gain.                            |
|    | Scheming Attitude: The long-term, systematic diversion of funds shows a calculated, deceptive approach to financial management.                                 |
| 80 | Desire for Personal Gain: Receiving kickbacks in exchange for invoice approvals demonstrates a clear motive for personal financial gain.                        |
|    | Scheming Attitude: The systematic acceptance of bribes for falsifying project completions and manipulating invoices indicates a calculated, deceptive approach. |
| 81 | Living Beyond Their Means: Using embezzled funds for personal expenses indicates a lifestyle beyond legitimate means.   |
|    | Desire for Personal Gain: The act of diverting funds for personal use reflects a strong motivation for personal financial gain.                                 |
|    | Scheming Attitude: Systematically misappropriating funds over time demonstrates a calculated, deceptive approach.   |

|    |  |
|----|--|
| 82 | Living Beyond Their Means: Use of embezzled funds for personal luxuries like vacations indicates living beyond legitimate means.             |
|    | Desire for Personal Gain: The act of creating a fake company to channel funds for personal use reflects a clear motive for personal gain.    |
|    | Scheming Attitude: Systematic submission of fraudulent invoices shows a calculated, deceptive approach to embezzlement.                      |
| 83 | Desire for Personal Gain: The misappropriation of funds for personal benefits suggests a strong motivation for personal enrichment.          |
|    | Scheming Attitude: Systematic deception of investors and regulatory defiance demonstrate a calculated and deceptive approach.                |
| 84 | Desire for Personal Gain: Embezzling from two employers indicates a clear motive for personal financial gain.                                |
|    | Scheming Attitude: Engaging in fraudulent activities over several years demonstrates a calculated and deceptive approach.                    |
| 85 | Living Beyond Their Means: Misusing Booster Club funds and COVID-19 relief for personal expenses indicates spending beyond legitimate means. |
|    | Desire for Personal Gain: Engaging in multiple fraudulent activities for financial benefit shows a strong personal gain motive.              |
|    | Scheming Attitude: Complex fraudulent schemes involving tax fraud and misuse of federal funds demonstrate a calculated, deceptive approach.  |
| 86 | Living Beyond Their Means: Using stolen funds for personal credit card payments indicates living beyond legitimate means.                    |
|    | Desire for Personal Gain: Systematic theft for personal financial gain.  |
|    | Scheming Attitude: Creating false accounting entries to conceal her actions reveals a deceptive and calculated approach.                     |

|    |   |
|----|---|
| 87 | Desire for Personal Gain: The creation of fraudulent invoices for personal gain shows a clear motive for financial benefit.                           |
|    | Scheming Attitude: Pike's methodical fabrication of invoices over 16 years demonstrates a calculated and deceptive approach.                          |
| 88 | Desire for Personal Gain: Sweeten's actions of issuing checks to herself and making personal purchases demonstrate a strong motive for personal gain. |
|    | Living Beyond Their Means: The significant amount of personal purchases on the company credit card suggests spending beyond her financial means.      |
|    | Scheming Attitude: The systematic theft of funds and manipulation of company resources indicate a calculated and deceptive mindset.                   |
| 89 | Living Beyond Their Means: Using company funds for personal luxuries suggests a lifestyle beyond legitimate means.                                    |
|    | Desire for Personal Gain: Deliberately defrauding workers and evading taxes shows a motive for personal financial benefit.                            |
|    | Scheming Attitude: The sophisticated nature of the payroll fraud demonstrates a calculated and deceptive approach.                                    |
| 90 | Living Beyond Their Means: Petrone's purchase of luxury items with stolen funds indicates living extravagantly beyond her legitimate income.          |
|    | Desire for Personal Gain: Orchestrating a multi-million dollar fraud for personal enrichment demonstrates a strong motivation for personal gain.      |
|    | Scheming Attitude: The systematic and prolonged nature of her fraudulent activities reflects a calculated, deceptive approach.                        |
| 91 | Living Beyond Their Means: Pocketing cash payments for personal use suggests living a lifestyle beyond legitimate financial means.                    |
|    | Desire for Personal Gain: Embezzlement of rent payments indicates a strong motivation for personal financial benefit.                                 |

|    |   |
|----|---|
|    | Scheming Attitude: Manipulating the computer system and altering payment information shows a deceptive and calculated approach.                             |
| 92 | Living Beyond Their Means: Laansma's use of embezzled funds for personal luxuries and expenses indicates living beyond her means.                           |
|    | Desire for Personal Gain: The deliberate embezzlement for personal benefit shows a clear motive for personal gain.  |
|    | Scheming Attitude: Manipulating company records to cover up personal expenses demonstrates a deceptive and calculated approach.                             |
| 93 | Gambling Habits: Usage of embezzled funds for vacations and gambling.   |
|    | Desire for Personal Gain: Embezzling such a significant amount reflects a strong motivation for personal financial benefit.                                 |
|    | Scheming Attitude: Systematically falsifying records to conceal theft demonstrates a calculated and deceptive approach.                                     |
| 94 | Living Beyond Their Means: Writing checks for personal use, including credit card payments, indicates living a lifestyle beyond legitimate financial means. |
|    | Desire for Personal Gain: The deliberate misdirection of funds for personal enrichment reflects a strong motivation for personal financial benefit.         |
|    | Scheming Attitude: Systematic embezzlement and tax evasion over several years demonstrate a calculated and deceptive approach.                              |
| 95 | Desire for Personal Gain: Misappropriating significant amounts of company funds for personal use indicates a strong motivation for financial gain.          |
|    | Scheming Attitude: The calculated creation and execution of false transactions demonstrate a deceitful and strategic approach to fraud.                     |
| 96 | Living Beyond Their Means: Embezzling such a large sum suggests spending beyond legitimate financial means.   |

|     |   |
|-----|---|
|     | Desire for Personal Gain: The significant amount embezzled indicates a strong motivation for personal financial benefit.                                |
|     | Scheming Attitude: The deliberate manipulation of financial records and transactions shows a calculated, deceptive approach.                            |
| 97  | Living Beyond Their Means: Purchasing luxury items and extravagant vacations indicates a lifestyle beyond legitimate financial means.                   |
|     | Desire for Personal Gain: Embezzling funds for personal luxuries shows a strong motivation for personal financial benefit.                              |
|     | Scheming Attitude: Systematically falsifying records to hide thefts demonstrates a calculated, deceptive mindset.                                       |
| 98  | Scheming Attitude: The deliberate falsification of work hours and assistance in covering up these actions demonstrate a calculated, deceptive approach. |
|     | Challenge to Beat the System: Manipulating time records and structuring cash transactions to avoid detection shows an intent to outsmart the system.    |
| 99  | Living Beyond Their Means: The lavish nature of the expenses (vacations, timeshares, cruises) indicates living well beyond legitimate financial means.  |
|     | Desire for Personal Gain: Using corporate funds for personal expenses and family businesses demonstrates a strong motive for personal financial gain.   |
|     | Scheming Attitude: The deliberate creation of false accounting entries to conceal her actions shows a calculated, deceptive approach.                   |
| 100 | Living Beyond Their Means: Receiving lavish trips and luxurious gifts indicates a lifestyle beyond legitimate means.                                    |
|     | Desire for Personal Gain: Accepting bribes and kickbacks reflects a strong motivation for personal benefit.   |
|     | Scheming Attitude: The conspiracy and efforts to conceal the illicit benefits demonstrate a calculated, deceptive approach.                             |

|     |  |
|-----|--|
| 101 | Desire for Personal Gain: Embezzling customer funds for personal use clearly shows a motive for personal financial gain.   |
|     | Scheming Attitude: Devising a complex scheme involving transfers between accounts and creating fraudulent requests demonstrates a calculated, deceptive approach.        |
|     | Challenge to Beat the System: Attempting to conceal his fraudulent activities by manipulating financial transactions indicates a mindset of outsmarting banking systems. |
| 102 | Living Beyond Their Means: Misappropriating substantial funds for personal use suggests living a lifestyle beyond legitimate means.                                      |
|     | Desire for Personal Gain: The act of diverting funds for personal benefit shows a strong motivation for financial gain.  |
|     | Scheming Attitude: Systematically embezzling from a non-profit organization over several years demonstrates a calculated, deceptive approach.                            |
| 103 | Desire for Personal Gain: The embezzlement of significant sums for personal use clearly indicates a motive for personal financial gain.                                  |
|     | Scheming Attitude: Creating fraudulent loans and manipulating financial records demonstrate a calculated, deceptive approach.  |
|     | Living Beyond Their Means: Using embezzled funds for personal expenditures suggests a lifestyle beyond legitimate financial means.                                       |
| 104 | Desire for Personal Gain: Kim's theft of trade secrets to improve his performance at a new employer indicates a strong motive for personal and professional gain.        |
|     | Scheming Attitude: Methodically copying sensitive files and using them at a competitor demonstrates a calculated and deceptive approach.                                 |
| 105 | Desire for Personal Gain: Diverting funds to personal accounts indicates a clear motive for personal enrichment.   |
|     | Scheming Attitude: Manipulating the reservation system for personal gain shows a calculated and deceptive approach to fraud.   |

|     |   |
|-----|---|
| 106 | Living Beyond Their Means: Expending embezzled funds on properties, vehicles, and travel indicates living a lifestyle beyond legitimate means.          |
|     | Desire for Personal Gain: Systematic issuance of fraudulent checks for personal benefit shows a clear motive for personal financial gain.               |
|     | Scheming Attitude: Executing a complex scheme involving numerous fraudulent checks over several years demonstrates a deceptive and calculated approach. |
| 107 | Desire for Personal Gain: Writing fraudulent checks to herself and others indicates a clear motive for financial benefit.                               |
|     | Scheming Attitude: The systematic theft and forgery of checks demonstrate a calculated, deceptive approach to fraud.                                    |
| 108 | Living Beyond Their Means: Using embezzled funds for personal luxuries like paying off a car and buying stocks.   |
|     | Desire for Personal Gain: The embezzlement for personal financial benefit after not being promoted indicates a motive for personal gain.                |
|     | Scheming Attitude: The complex scheme of transferring funds and laundering money shows a calculated and deceptive approach.                             |
| 109 | Desire for Personal Gain: The systematic creation of false timesheets and invoices for personal financial gain.   |
|     | Scheming Attitude: Employing multiple methods to embezzle funds, including forging signatures and creating fake companies.                              |
| 110 | Desire for Personal Gain: Utilizing embezzled funds for personal expenses highlights a strong motive for personal enrichment.                           |
|     | Scheming Attitude: Systematically taking money over a five-year period demonstrates calculated, deceptive behavior.                                     |
| 111 | Living Beyond Their Means: Excessive spending at a bingo hall and on retail suggests spending beyond legitimate financial means.                        |

|     |  |
|-----|--|
|     | <p>Desire for Personal Gain: Embezzling funds and fraudulently obtaining disability payments indicate a strong motive for personal financial gain.</p> <p>Scheming Attitude: The systematic approach to forging checks, evading taxes, and manipulating disability claims demonstrates a calculated and deceptive mindset.</p>   |
| 112 | <p>Living Beyond Their Means: Excessive cash withdrawals for personal use suggest a lifestyle beyond legitimate financial means.</p> <p>Desire for Personal Gain: Systematic embezzlement for personal benefit clearly indicates a strong motive for financial gain.</p> <p>Scheming Attitude: The deliberate falsification of financial records to conceal theft shows a calculated, deceptive mindset.</p>                 |
| 113 | <p>Living Beyond Their Means: Using embezzled funds for personal expenditures indicates a lifestyle beyond her legitimate earnings.</p> <p>Desire for Personal Gain: The deliberate creation of fake claims for financial benefit shows a strong motivation for personal enrichment.</p> <p>Scheming Attitude: Collaborating to create and approve fraudulent invoices demonstrates a calculated and deceptive approach.</p> |
| 114 | <p>Living Beyond Their Means: Personal use of company funds suggests spending beyond legitimate earnings.</p> <p>Desire for Personal Gain: Creating a fake business and misusing company assets indicate a clear motive for personal enrichment.</p> <p>Scheming Attitude: The elaborate setup of false invoicing and misuse of company funds shows calculated deceit.</p>   |
| 115 | <p>Living Beyond Their Means: Purchasing luxury vehicles and real estate with embezzled funds indicates a lifestyle beyond legitimate earnings.</p> <p>Desire for Personal Gain: Engaging in embezzlement for personal enrichment and business investments reflects a motive for financial benefit.</p>  |



|     |  |
|-----|--|
|     | Scheming Attitude: The complex scheme involving embezzlement, money laundering, and tax fraud demonstrates a calculated, deceptive mindset.                    |
| 116 | Desire for Personal Gain: Cox's involvement in various fraudulent schemes indicates a clear pursuit of personal financial gain.                                |
|     | Scheming Attitude: Fabricating bank statements and board resolutions demonstrates a calculated, deceptive mindset.   |
|     | Challenge to Beat the System: Engaging in complex fraud schemes shows an intent to outsmart financial and legal systems.                                       |
| 117 | Desire for Personal Gain: The purchase of personal items like electronics and vehicles indicates a clear motive for personal gain.                             |
|     | Living Beyond Their Means: The acquisition of high-value items suggests spending beyond legitimate financial means.  |
|     | Scheming Attitude: Creating false invoices and altering accounting records to conceal unauthorized purchases demonstrates a calculated and deceptive approach. |
| 118 | Desire for Personal Gain: Accepting bribes in exchange for violating user privacy indicates a strong motivation for personal benefit.                          |
|     | Scheming Attitude: Engaging in complex schemes involving bribery, information theft, and money laundering demonstrates a calculated and deceptive mindset.     |
| 119 | Living Beyond Their Means: The acceptance of payments for personal expenses like tuition and parties suggests spending beyond legitimate means.                |
|     | Desire for Personal Gain: The receipt of substantial personal benefits demonstrates a strong motivation for financial gain.                                    |
|     | Scheming Attitude: Engaging in a conspiracy to inflate orders and receive personal benefits shows a calculated, deceptive approach.                            |
| 120 | Desire for Personal Gain: Levoff's use of confidential information for personal trading demonstrates a clear motive for financial gain.                        |

|     |   |
|-----|---|
|     | Scheming Attitude: Manipulating his access to sensitive information and trading during blackout periods show a calculated and deceptive approach. |
| 121 | Living Beyond Their Means: Using embezzled funds for extravagant purchases like luxury cars and real estate.                                      |
|     | Desire for Personal Gain: Orchestrating a large-scale fraud to enrich himself at the expense of thousands of investors.                           |
|     | Scheming Attitude: Devising a complex scheme involving false promises and misuse of investor funds.   |
| 122 | Desire for Personal Gain: Exploiting investment opportunities for personal enrichment clearly demonstrates a motive for financial gain.           |
|     | Scheming Attitude: Devising fraudulent investment schemes and using an alias to evade law enforcement show calculated deception.                  |
|     | Living Beyond Their Means: The use of fraudulently obtained funds suggests a lifestyle funded by illegal means.                                   |
| 123 | Desire for Personal Gain: Engaging in a fraudulent scheme for personal financial benefit.   |
|     | Scheming Attitude: Orchestrating a complex scheme involving false promises and misrepresentations to investors.                                   |
| 124 | Desire for Personal Gain: Using investor funds for personal expenses and other investments shows a clear motivation for financial benefit.        |
|     | Scheming Attitude: Creating a Ponzi scheme and making false representations to investors indicate a calculated, deceptive approach.               |
| 125 | Desire for Personal Gain: Accepting bribes shows a clear motive for financial enrichment.   |
|     | Scheming Attitude: Coaching conspirators on falsifying financial information indicates a calculated and deceptive approach.                       |
|     | High Personal Debt: The acceptance of bribes could suggest a need to address personal financial issues.   |
| 126 | Scheming Attitude: Deliberately misleading investors with false statements about a critical health product during a pandemic.                     |
|     | Challenge to Beat the System: Attempting to manipulate the market and take advantage of a public health crisis.                                   |

|     |   |
|-----|---|
| 127 | Desire for Personal Gain: Withholding taxes from employees but not paying them to the IRS suggests a motive for financial benefit.                            |
|     | Scheming Attitude: Manipulating tax obligations for multiple companies demonstrates a calculated and deceptive approach.                                      |
| 128 | Desire for Personal Gain: Engaging in kickbacks and insider trading indicates a strong motivation for personal financial gain.                                |
|     | Scheming Attitude: Clark’s involvement in manipulating market prices and prearranged trades shows a calculated and deceitful approach.                        |
|     | Challenge to Beat the System: Participating in complex fraudulent schemes demonstrates an intent to outsmart market regulations.                              |
| 129 | Living Beyond Their Means: Using government funds intended for pandemic relief for personal expenditures suggests living a lifestyle beyond legitimate means. |
|     | Desire for Personal Gain: Misappropriating funds allocated for public health emergency demonstrates a clear motive for personal financial benefit.            |
|     | Scheming Attitude: Diverting funds from a critical public health initiative to personal use indicates a calculated and deceptive approach.                    |
| 130 | Desire for Personal Gain: The deliberate fraud to secure SBA guarantees indicates a motive for financial benefit.   |
|     | Scheming Attitude: The systematic alteration of loan records and business details demonstrates a calculated, deceptive approach.                              |
| 131 | Desire for Personal Gain: Engaging in bid-rigging and price-fixing indicates a clear motive for financial benefit, likely at the expense of fair competition. |
|     | Scheming Attitude: The systematic collusion with competitors to manipulate the bidding process demonstrates a deceptive and unethical approach.               |
| 132 | Desire for Personal Gain: The orchestration of a large-scale fraud scheme demonstrates a strong motivation for financial enrichment.                          |

|     |  |
|-----|--|
|     | Scheming Attitude: Creating an elaborate scheme involving kickbacks, shell companies, and fraudulent orders indicates calculated and deceptive behavior.     |
| 133 | Living Beyond Their Means: The acquisition of high-value assets like a yacht and plane suggests extravagant spending.  |
|     | Desire for Personal Gain: Pursuing inflated contracts through bribery indicates a strong motive for financial gain.  |
|     | Challenge to Beat the System: Engaging in complex schemes of bribery and money laundering shows an intent to outmaneuver legal and ethical standards.        |
| 134 | Living Beyond Their Means: Using city funds for extensive personal expenses indicates a lifestyle beyond her legitimate earnings.                            |
|     | Desire for Personal Gain: Engaging in systematic embezzlement shows a clear motive for financial enrichment.   |
|     | Scheming Attitude: The complex manipulation of financial records demonstrates a calculated and deceptive approach.   |
| 135 | Desire for Personal Gain: The collection of substantial fees and the creation of fraudulent slush funds indicate a motivation for financial benefit.         |
|     | Scheming Attitude: Coordinating complex global transactions for bribery and tax evasion shows a calculated and unethical approach.                           |
| 136 | Desire for Personal Gain: The acceptance of kickbacks in exchange for confidential information indicates a strong motivation for personal financial benefit. |
|     | Scheming Attitude: Orchestrating a bid-rigging scheme and attempting to obstruct justice demonstrate a calculated and manipulative mindset.                  |
| 137 | Desire for Personal Gain: The pursuit of personal commissions through fraudulent loan origination demonstrates a strong motive for financial gain.           |
|     | Scheming Attitude: Manipulating loan applications and instructing borrowers to fabricate information indicates a calculated and unethical approach.          |

|     |   |
|-----|---|
|     | Living Beyond Their Means: Earning substantial commissions through fraudulent means suggests a lifestyle funded by illegitimate activities.                   |
| 138 | Desire for Personal Gain: The act of diverting campaign funds for personal use demonstrates a strong motivation for financial enrichment.                     |
|     | Living Beyond Their Means: Misappropriating funds beyond the agreed-upon salary indicates a lifestyle or spending beyond his legitimate earnings.             |
| 139 | Living Beyond Their Means: Using embezzled funds for personal debts and living expenses indicates spending beyond legitimate means.                           |
|     | Desire for Personal Gain: Embezzling money for personal use reflects a motive for financial gain.   |
|     | Scheming Attitude: Devising a scheme to divert vendor payments and mislead vendors demonstrates a calculated and deceptive approach.                          |
| 140 | Desire for Personal Gain: Xiao's actions to secure additional funding by concealing other grants indicate a motive for personal or professional gain.         |
|     | Scheming Attitude: Deliberately hiding information about other financial sources demonstrates a calculated and dishonest approach.                            |
| 141 | Desire for Personal Gain: Scott's orchestration of the scheme for personal profit demonstrates a clear motive for financial gain.                             |
|     | Scheming Attitude: Creating a complex fraud scheme involving multiple entities shows a deceptive and calculated approach.                                     |
| 142 | Desire for Personal Gain: Brassart's evasion of tax payments indicates a clear motive for financial gain.   |
|     | Scheming Attitude: The creation of nominee corporations and filing of false bankruptcy petitions demonstrate a calculated, deceptive approach to evade taxes. |
| 143 | Desire for Personal Gain: Heredia's involvement in price manipulation indicates a strong motivation for personal and corporate financial benefit.             |

|     |  |
|-----|--|
|     | Scheming Attitude: Orchestrating a scheme to manipulate market prices demonstrates a calculated and dishonest approach.  |
| 144 | Desire for Personal Gain: Ribas's acceptance of multimillion-dollar bribes indicates a clear motivation for personal enrichment.   |
|     | Scheming Attitude: The complex scheme involving intermediaries for bribe payments and money laundering shows calculated deceit.  |
| 145 | Living Beyond Their Means: The purchase of a luxury car and high-end goods suggests spending beyond legitimate income.   |
|     | Desire for Personal Gain: Engaging in fraud for personal financial benefit.  |
|     | Scheming Attitude: Orchestrating a scheme involving kickbacks, bribes, and fraudulent billing.   |
| 146 | Desire for Personal Gain: Rashid's actions, driven by the motive to increase profits through fraudulent medical practices, highlight a strong desire for personal financial gain.  |
|     | Scheming Attitude: Orchestrating a complex scheme involving unnecessary medical procedures and opioid prescriptions demonstrates a calculated and unethical approach to exploit both patients and the healthcare system. |
| 147 | Desire for Personal Gain: Diverting company funds for personal expenses indicates a strong motive for financial gain.  |
|     | Scheming Attitude: Intentionally stopping the payment of employment taxes and using funds for personal benefits shows a deceitful and calculated approach.   |
| 148 | Desire for Personal Gain: The diversion of company funds to personal accounts indicates a clear motive for financial benefit.  |
|     | Scheming Attitude: Actively falsifying records to conceal misappropriation demonstrates calculated deceit and manipulation.  |
| 149 | Desire for Personal Gain: Engaging in the distribution of controlled substances for profit shows a clear motive for financial gain.  |

|     |  |
|-----|--|
|     | Scheming Attitude: The deliberate creation of fake prescriptions and manipulation of the medical system reflects a deceptive and calculated approach.      |
| 150 | Living Beyond Their Means: The utilization of stolen funds for personal expenses indicates spending beyond legitimate means.                               |
|     | Desire for Personal Gain: The systematic fraud for personal financial gain demonstrates a clear motive.  |
|     | Scheming Attitude: Employing deceitful methods to execute fraudulent transfers shows a calculated and deceptive approach.                                  |
| 151 | Desire for Personal Gain: The deliberate inflation of financial performance suggests a motive for personal or corporate gain.                              |
|     | Scheming Attitude: Manipulating financial statements and concealing true financial conditions indicate a calculated and deceptive approach.                |
|     | Challenge to Beat the System: Overriding internal controls to carry out the fraud signifies an intent to outsmart regulatory systems.                      |
| 152 | Desire for Personal Gain: Embezzlement of funds from the Drug Court Foundation indicates a motive for financial enrichment.                                |
|     | Scheming Attitude: Orchestrating the delivery of embezzled funds and planning the destruction of incriminating evidence show calculated deceit.            |
|     | Challenge to Beat the System: Efforts to manipulate a witness and obstruct justice demonstrate a belief in being above the law.                            |
| 153 | Inadequate Attention to Details: Deloitte's failure to identify TBW's fraudulent activities suggests a lack of thoroughness in its auditing process.       |
|     | Challenge to Beat the System: An apparent disregard for strict adherence to auditing standards indicates a mindset of circumventing regulatory compliance. |
| 154 | Desire for Personal Gain: The deliberate forgery and cashing of checks for personal use indicate a strong motivation for financial benefit.                |

|     |   |
|-----|---|
|     | <p>Living Beyond Their Means: The use of embezzled funds for personal expenses suggests spending beyond legitimate financial means.</p> <p>Scheming Attitude: The systematic forgery of checks demonstrates a calculated, dishonest approach.</p>   |
| 155 | <p>Living Beyond Their Means: Hauk's extravagant purchases of luxury vehicles indicate spending far beyond his legitimate income.</p> <p>Desire for Personal Gain: The embezzlement for personal gain, especially for high-value items, highlights a strong motivation for financial enrichment.</p> <p>Scheming Attitude: Complex schemes to divert funds demonstrate a calculated, deceptive approach.</p>  |
| 156 | <p>Living Beyond Their Means: Operating a side business could indicate a lifestyle or financial obligations exceeding their DEA salaries.</p> <p>Desire for Personal Gain: The involvement in a potentially lucrative side business suggests a motive for additional personal income.</p> <p>Challenge to Beat the System: Actively managing a business while not disclosing it, despite understanding the legal and ethical requirements, shows a disregard for rules.</p> |
| 157 | <p>Desire for Personal Gain: Cummings's involvement in selling stolen credit reports for profit indicates a clear motive for personal financial benefit.</p> <p>Scheming Attitude: The systematic misuse of confidential information and participation in a large-scale fraud scheme demonstrates a calculated and deceptive mindset.</p>   |



APPENDIX F:  
ANALYSIS OF ORGANIZATIONAL FLAGS

| Case | Analysis Data  |
|------|--|
| 1    | Placing Too Much Trust in a Few Employees: Stollery controlled investor funds without proper oversight.  |
|      | Lack of Independent Checks on Performance: No verification of the legitimacy of business relationships.  |
|      | Inadequate Attention to Details: Falsified aspects of white papers.  |
|      | Lack of Separation of Duties: Controlled investor funds and diverted them for personal use.  |
|      | Lack of clear lines of authority and responsibilities: Stollery had unchecked control over ICO funds.  |
|      | Lack of regular review by the Internal Auditor: No oversight of fund misappropriation.   |
| 2    | Placing Too Much Trust in a Few Employees: As a mayor, Pérez-Otero likely had significant autonomy and trust, facilitating his ability to engage in bribery. |
|      | Lack of Proper Authorization of Transactions: The ability to expedite payments implies a lack of proper checks and balances in authorizing transactions.     |
|      | Lack of Independent Checks on Performance: His ability to continue this scheme over years suggests inadequate independent oversight.                         |
| 3    | Placing Too Much Trust in a Few Employees: Firlé, as the CFO, was trusted excessively without adequate oversight.  |
|      | Lack of Separation of Duties: Being able to initiate wire transfers and issue checks indicates a lack of separation in financial responsibilities.           |
|      | Inadequate Attention to Details: The prolonged period of embezzlement suggests inadequate attention to financial details by the organization.                |
| 4    | Placing Too Much Trust in a Few Employees: Murray, as the Director of Finance, was given unchecked access to the organization's bank accounts.               |

|   |   |
|---|---|
|   | Inadequate Attention to Details: The fact that the embezzlement continued over several years indicates a lack of detailed financial review.                                 |
|   | Lack of Separation of Duties: Murray's ability to execute and conceal transactions shows a lack of proper financial checks and balances.                                    |
| 5 | Placing Too Much Trust in a Few Employees: Raeford Farms placed significant trust in Hickman and Whiteman, enabling their fraudulent activities.                            |
|   | Lack of Separation of Duties: Hickman's control over sales and Whiteman's responsibility for inventory tracking allowed them to exploit their roles.                        |
|   | Inadequate Attention to Details: The lack of detailed scrutiny of sales transactions and inventory allowed the fraud to continue.   |
| 6 | Placing Too Much Trust in a Few Employees: The prolonged period of embezzlement suggests excessive trust placed in Peterson without adequate oversight.                     |
|   | Lack of Independent Checks on Performance: The fact that the embezzlement continued for several years indicates a lack of independent verification of financial activities. |
|   | Inadequate Attention to Details: The ability to embezzle such a significant amount over time points to a lack of attention to financial details by the organization.        |
| 7 | Placing Too Much Trust in a Few Employees: Arnold, as an accountant, had significant control over financial transactions.   |
|   | Lack of Independent Checks on Performance: Ineffective oversight of Arnold's activities.  |
|   | Inadequate Attention to Details: Failure to detect falsified financial documents.   |
| 8 | Placing Too Much Trust in a Few Employees: Trust in doctors like Payne without proper checks enabled the fraud.   |
|   | No Proper Authorization of Transactions: The lack of checks on the financial transactions related to surgeries.   |
|   | Lack of Independent Checks on Performance: Absence of oversight on the doctors' activities and financial dealings.  |
| 9 | Placing Too Much Trust in a Few Employees: Figg was trusted with significant access to sensitive information.   |

|    |  |
|----|--|
|    | Lack of Separation of Duties: Figg had the ability to manipulate accounts and create loans, indicating inadequate role segregation.                          |
|    | Inadequate Attention to Details: The prolonged duration of the embezzlement suggests a lack of attention to account anomalies.                               |
| 10 | Placing Too Much Trust in a Few Employees: Cherry, as a branch manager, was trusted with significant access to the bank's assets without adequate oversight. |
|    | Lack of Separation of Duties: Her ability to access the vault and manipulate cash drawer totals indicates a failure in segregating duties.                   |
|    | Inadequate Attention to Details: The bank failed to detect the discrepancy in cash supplies and drawer totals for over a year.                               |
| 11 | Inadequate Attention to Details: Failure to detect the inflation of compensation and misuse of corporate credit cards.                                       |
|    | Lack of Independent Checks on Performance: Inability to uncover the falsification of accounting records.   |
|    | Lack of Separation of Duties: Allowing the same individual to handle multiple financial responsibilities without oversight.                                  |
| 12 | Placing Too Much Trust in a Few Employees: Lindberg, as a controlling executive, likely had too much unsupervised control.                                   |
|    | No Proper Authorization of Transactions: The misuse of funds suggests a lack of proper transaction authorization mechanisms.                                 |
|    | Lack of Independent Checks on Performance: The prolonged undetected scheme indicates inadequate independent checks on the company's operations.              |
| 13 | Placing Too Much Trust in a Few Employees: Burley had significant control over financial processes.  |
|    | No Proper Authorization of Transactions: Lack of oversight on transactions she handled.  |
|    | Inadequate Attention to Details: The school districts failed to notice the alterations and misuse of funds.  |
|    | Lack of Independent Checks on Performance: Inadequate verification of her work and financial records.  |

|    |   |
|----|---|
| 14 | Placing Too Much Trust in a Few Employees: Collins had significant control over the church's finances without adequate oversight.                       |
|    | Lack of Separation of Duties: Her role encompassed multiple financial responsibilities, indicating a lack of duty segregation.                          |
|    | Inadequate Attention to Details: The prolonged period of embezzlement suggests a lack of attention to financial details by the church.                  |
| 15 | Placing Too Much Trust in a Few Employees: Ex-players like Dooling and Anderson were trusted by other players, leading to a wider spread of the scheme. |
|    | Lack of Independent Checks on Performance: The success of the scheme indicates a lack of robust verification processes within the Plan.                 |
|    | Inadequate Attention to Details: Failure to detect discrepancies in the claims submitted by the players.  |
|    | No Proper Authorization of Transactions: Lack of adequate authorization procedures for the reimbursement claims.  |
| 16 | Placing Too Much Trust in a Few Employees: Tischer, as the sole trustee, was given excessive control without adequate oversight.                        |
|    | Lack of Separation of Duties: Her role as the sole decision-maker for fund disbursement shows a lack of segregation of duties.                          |
|    | Inadequate Attention to Details: The prolonged period of embezzlement suggests inadequate attention to detail by those overseeing the trust.            |
| 17 | Placing Too Much Trust in a Few Employees: Spadoni, as a high-ranking official, was trusted without sufficient oversight.                               |
|    | No Proper Authorization of Transactions: Lack of thorough review and authorization of the MES contract.   |
|    | Lack of Separation of Duties: Spadoni's ability to influence the contract decision signifies a failure in segregating duties.                           |
|    | Inadequate Attention to Details: Overlooking the conflict of interest in Spadoni's case indicates negligence in detail.                                 |
| 18 | Placing Too Much Trust in a Few Employees: Excessive trust placed in the CEO, Suni Munshani, enabled the fraud.   |

|    |  |
|----|--|
|    | No Proper Authorization of Transactions: The unauthorized transfer of funds indicates a lack of transaction control.   |
|    | Lack of Independent Checks on Performance: The ability to conduct fraud over an extended period suggests inadequate checks and balances.   |
|    | Inadequate Attention to Details: Failure to detect the creation and use of a fake company for fraudulent purposes.   |
| 19 | Placing Too Much Trust in a Few Employees: Carson had sole control over the parish's finances.   |
|    | Lack of Separation of Duties: As the only person managing finances, there was no check on her activities.  |
|    | Inadequate Attention to Details: The prolonged scheme indicates oversight failures.  |
|    | Lack of Independent Checks on Performance: Lack of monitoring allowed the fraud to continue.   |
| 20 | Placing Too Much Trust in a Few Employees: Alexandre's control and operation of EminiFX suggest excessive trust was placed in him without adequate oversight.                    |
|    | Inadequate Attention to Details: The prolonged operation of the fraudulent scheme indicates a lack of attention to operational details by the authorities or other stakeholders. |
|    | Lack of Clear Lines of Authority and Responsibilities: Alexandre's sole control over the investment operations points to a lack of clear organizational structure.               |
| 21 | Placing Too Much Trust in a Few Employees: Excessive trust in Ryan, as CEO, without adequate checks.   |
|    | No Proper Authorization of Transactions: Lack of effective authorization processes for loan approvals and financial statements.  |
|    | Lack of Independent Checks on Performance: Inadequate independent review of bank operations and loan portfolios.   |
|    | Inadequate Attention to Details: Failure to scrutinize the details of borrowers' financial conditions and loan performance.  |
| 22 | Placing Too Much Trust in a Few Employees: Downey, as the business owner, likely had unchecked control.  |
|    | Inadequate Attention to Details: The prolonged undetected scheme indicates a lack of attention to financial details within the organization.                                     |
|    | Lack of Separation of Duties: The ability to manipulate funds without oversight shows a lack of internal controls and segregation of duties.                                     |

|    |  |
|----|--|
| 23 | <p>Inadequate Attention to Details: The failure to detect altered checks and unauthorized salary increase points to inadequate attention to payroll details.</p>       |
|    | <p>Lack of Separation of Duties: The ability of Owens-Sharp to alter checks and manipulate payroll records suggests a lack of adequate internal controls.</p>          |
|    | <p>Lack of Regular Review by the Internal Auditor: The extended period of fraud implies insufficient or ineffective auditing processes.</p>                            |
| 24 | <p>Placing Too Much Trust in a Few Employees: Excessive trust was placed in Woodson and Thompson without adequate oversight.</p>                                       |
|    | <p>Lack of Independent Checks on Performance: The prolonged duration of the fraud suggests a lack of effective checks and balances.</p>                                |
|    | <p>Inadequate Attention to Details: The ability to forge signatures and embezzle funds over years indicates a lack of attention to financial details.</p>              |
|    | <p>Lack of Separation of Duties: The fact that two individuals could write checks to themselves highlights a lack of segregation in financial responsibilities.</p>    |
| 25 | <p>Lack of Separation of Duties: Tigler’s ability to access, create, and cash fraudulent checks indicates a lack of internal control.</p>                              |
|    | <p>Inadequate Attention to Details: The bank’s failure to detect the fraudulent activity over several years suggests a lack of attention to transactional details.</p> |
|    | <p>Lack of Independent Checks on Performance: The absence of independent verification of Tigler's activities enabled the fraud.</p>                                    |
| 26 | <p>Placing Too Much Trust in a Few Employees: Excessive trust in Rivero without adequate supervision facilitated the fraud.</p>  |
|    | <p>Lack of Independent Checks on Performance: The lack of checks allowed Rivero to misappropriate funds without immediate detection.</p>                               |

|    |   |
|----|---|
|    | Inadequate Attention to Details: The firm's failure to promptly identify irregularities in client accounts shows a lack of attention to detail.                                 |
|    | No Proper Authorization of Transactions: Rivero's ability to move client funds without proper authorization indicates a control weakness.                                       |
| 27 | Placing Too Much Trust in a Few Employees: Sharp, as a senior developer with extensive access, was overly trusted.  |
|    | Lack of Independent Checks on Performance: The absence of monitoring or verification of Sharp's activities facilitated the fraud.   |
|    | Inadequate Attention to Details: The failure to detect unusual activities and access patterns indicates a lack of attention to security details.                                |
| 28 | No Proper Authorization of Transactions: Chabaud's ability to access and use the funds post-termination indicates a lack of proper transaction authorization.                   |
|    | Inadequate Attention to Details: The duration of the fraud suggests the band lacked attention to financial details.   |
|    | Lack of Separation of Duties: The fact that she could continue accessing accounts post-termination indicates insufficient separation of financial responsibilities.             |
| 29 | Placing Too Much Trust in a Few Employees: Girardi's ability to conduct extensive fraudulent activities points to excessive trust placed in him and Kamon.                      |
|    | Lack of Independent Checks on Performance: The prolonged undetected scheme indicates inadequate independent checks on the firm's operations.                                    |
|    | Inadequate Attention to Details: Failure to detect the misappropriation of large sums of settlement money over a long period suggests a lack of attention to financial details. |
|    | Lack of Clear Lines of Authority and Responsibilities: The blurred lines between Girardi's and Kamon's roles and responsibilities facilitated the fraud.                        |
| 30 | Placing Too Much Trust in a Few Employees: Cory's ability to misdirect funds indicates excessive trust placed in him.   |

|    |   |
|----|---|
|    | Inadequate Attention to Details: The company's failure to detect false consulting payments shows a lack of attention to financial details.                        |
|    | No Proper Authorization of Transactions: The transfer of funds without proper verification indicates a lack of authorization protocols.                           |
| 31 | Placing Too Much Trust in a Few Employees: Excessive trust in Bowker as the CFO with minimal oversight.   |
|    | No Proper Authorization of Transactions: Ability to bypass two-signature requirements shows a lack of proper transaction controls.                                |
|    | Lack of Independent Checks on Performance: Failure to detect Bowker's embezzlement and tax evasion points to inadequate checks on his activities.                 |
| 32 | Placing Too Much Trust in a Few Employees: Excessive trust was placed in Dunican as CEO, enabling the fraud.  |
|    | No Proper Authorization of Transactions: The redirection of funds without proper checks indicates a lack of transactional oversight.                              |
|    | Lack of Independent Checks on Performance: The scheme's success until its accidental discovery suggests a lack of effective independent verification.             |
| 33 | Placing Too Much Trust in a Few Employees: Dodson's control over fundraising and bank accounts indicates excessive trust without proper oversight.                |
|    | Lack of Separation of Duties: Control over both fundraising and financial information dissemination suggests a lack of internal controls.                         |
|    | No Proper Authorization of Transactions: The unauthorized use of investor funds indicates a failure in transaction authorization processes.                       |
| 34 | Placing Too Much Trust in a Few Employees: Bernardi, as the CEO, had significant control which he abused.   |
|    | No Proper Authorization of Transactions: The lack of oversight in financial statements and legal communications indicates a failure in transaction authorization. |
|    | Lack of Independent Checks on Performance: The fraudulent activities went undetected, suggesting insufficient independent verification.                           |



|    |   |
|----|---|
| 35 | Placing Too Much Trust in a Few Employees: Jackson's unchecked authority and access to the cash vault and accounts indicate excessive trust.              |
|    | Lack of Independent Checks on Performance: The lack of detection of her fraudulent activities for years suggests inadequate independent checks.           |
|    | Inadequate Attention to Details: The failure to notice unauthorized transactions and account anomalies indicates a lack of detail-oriented oversight.     |
| 36 | Inadequate Attention to Details: The ability to manipulate invoices without immediate detection suggests a lack of attention to financial details.        |
|    | Lack of Separation of Duties: As an accounts payable clerk, her ability to manipulate invoices indicates insufficient separation of duties.               |
|    | Lack of Independent Checks on Performance: The duration of the fraud indicates a lack of effective independent reviews and checks.                        |
| 37 | Inadequate Attention to Details: The bank's failure to detect unusual access patterns to customer information.  |
|    | Lack of Regular Review by the Internal Auditor: The scheme's success suggests a lack of effective internal audits.  |
| 38 | Lack of Independent Checks on Performance: The ability to engage in bid-rigging over several years indicates a lack of effective checks and controls.     |
|    | Inadequate Attention to Details: The prolonged period over which the bid-rigging occurred suggests a lack of attention to contract details and oversight. |
|    | No proper authorization of transactions: The manipulation of bids implies a failure in ensuring proper authorization and oversight of contract processes. |
| 39 | Placing Too Much Trust in a Few Employees: Excessive trust in Slingerland as CEO allowed the misappropriation of funds.                                   |
|    | Inadequate Attention to Details: The organization failed to notice the misuse of substantial amounts of money.  |
|    | Lack of Separation of Duties: Slingerland's unchecked control over financial decisions and lack of oversight.   |

|    |  |
|----|--|
|    | Lack of Regular Review by the Internal Auditor: The prolonged period of embezzlement suggests inadequate internal auditing.                                  |
| 40 | Inadequate Attention to Details: The long-term undetected fraud indicates a lack of detail-oriented oversight.   |
|    | Lack of Separation of Duties: As payroll manager, Maurello had control over the payroll system without sufficient checks.                                    |
|    | Lack of Regular Review by the Internal Auditor: The duration of the fraud suggests a lack of effective internal audit procedures.                            |
| 41 | Inadequate Attention to Details: Failure to detect ongoing fraudulent activities over a long period.   |
|    | Lack of Separation of Duties: One individual having extensive access to financial reimbursement systems without adequate checks.                             |
|    | Lack of clear lines of authority and responsibilities: Not promptly revoking access to systems upon termination shows a lack of clear procedural guidelines. |
| 42 | Placing Too Much Trust in a Few Employees: Abboud's unchecked control over finances due to excessive trust in her position.                                  |
|    | Lack of Separation of Duties: Abboud's ability to manipulate financial transactions without oversight indicates insufficient internal controls.              |
|    | Inadequate Attention to Details: Failure to notice the misuse of funds for personal expenses shows a lack of detail-oriented financial oversight.            |
|    | No Proper Authorization of Transactions: The fraudulent transactions indicate a lack of proper checks and authorizations.                                    |
| 43 | Placing Too Much Trust in a Few Employees: Excessive trust in Skidmore's role as Secretary-Treasurer enabled her to perpetrate the fraud.                    |
|    | Lack of Separation of Duties: Skidmore's ability to manage accounts and handle fee collections without oversight.  |
|    | Inadequate Attention to Details: Failure to detect the creation of unauthorized accounts and misuse of funds.  |

|    |   |
|----|---|
|    | No Proper Authorization of Transactions: The ability to transfer and misappropriate funds indicates a lack of transaction authorization controls.                           |
| 44 | Placing Too Much Trust in a Few Employees: Boisture's role as chief financial employee provided her with excessive unsupervised control.                                    |
|    | Lack of Separation of Duties: The ability to divert funds and take loans without oversight indicates a lack of internal control mechanisms.                                 |
|    | No Proper Authorization of Transactions: The unauthorized loans and financial misrepresentations point to a lack of proper transaction authorization processes.             |
| 45 | Placing Too Much Trust in a Few Employees: Excessive trust in Carroll's executive position allowed the misappropriation of funds.   |
|    | No Proper Authorization of Transactions: The lack of thorough verification of the contract and invoices points to weak transaction authorization.                           |
|    | Lack of Independent Checks on Performance: The absence of independent checks enabled Carroll's fraudulent activities to go unnoticed.                                       |
| 46 | Placing Too Much Trust in a Few Employees: Pothos, as a relationship manager, had significant trust and access to sensitive client information.                             |
|    | Lack of Independent Checks on Performance: The failure to detect the change in mailing addresses and phone numbers reflects a lack of independent verification.             |
|    | Inadequate Attention to Details: The bank's systems failed to notice suspicious activities and address changes, indicating a lack of attention to customer account details. |
| 47 | Placing Too Much Trust in a Few Employees: Spilberg, as a manager, was trusted with access to company funds, which he misused.  |
|    | Inadequate Attention to Details: The failure to detect repeated misuse of the company debit card points to a lack of financial oversight.                                   |

|    |  |
|----|--|
|    | Lack of Separation of Duties: Allowing a manager unrestricted access to company funds without adequate checks indicates a lack of internal control.              |
| 48 | Placing Too Much Trust in a Few Employees: Excessive trust was placed in Simkins as CFO, enabling embezzlement.  |
|    | Lack of Independent Checks on Performance: Lack of independent oversight allowed Simkins to misuse funds.  |
|    | Inadequate Attention to Details: Failure to detect large-scale and growing embezzlement indicates insufficient attention to financial details.                   |
| 49 | No Proper Authorization of Transactions: The ability to embezzle and fraudulently obtain loans suggests a lack of effective transaction authorization processes. |
|    | Inadequate Attention to Details: Her former employer's failure to detect embezzlement indicates a lack of attention to financial details.                        |
| 50 | Placing Too Much Trust in a Few Employees: Excessive trust was placed in Chalmers as the bookkeeper, allowing her to embezzle funds.                             |
|    | Lack of Separation of Duties: Her role allowed her to both write checks and manage accounting records, indicating a lack of separation in financial duties.      |
|    | Inadequate Attention to Details: The failure to detect falsified year-end cash-on-hand numbers suggests insufficient attention to financial details.             |
| 51 | Placing Too Much Trust in a Few Employees: Excessive trust placed in C-suite executives, allowing them to manipulate company information.                        |
|    | Lack of Clear Lines of Authority and Responsibilities: Ineffective oversight of executive actions and decisions.   |
|    | Inadequate Attention to Details: Failure to ensure accurate and truthful public disclosures and regulatory submissions.  |
| 52 | Lack of Independent Checks on Performance: Marquez's ability to alter bank statements undetected points to a lack of effective independent checks.               |

|    |  |
|----|--|
|    | Inadequate Attention to Details: The prolonged period of undetected embezzlement suggests a failure in paying attention to financial details.                  |
|    | Lack of Separation of Duties: His role as both accountant and cash manager allowed him to execute and conceal fraudulent transactions.                         |
| 53 | Placing Too Much Trust in a Few Employees: Excessive trust in Collins as CEO allowed the perpetration of the fraud.  |
|    | Inadequate Attention to Details: Failure to detect the submission of false loan information suggests a lack of attention to financial details.                 |
|    | Lack of Independent Checks on Performance: The scheme's success points to a lack of effective independent checks and balances within the company.              |
| 54 | Placing Too Much Trust in a Few Employees: Vicars, as a vice president, was given significant trust and authority without adequate checks.                     |
|    | Lack of Separation of Duties: The ability to approve invoices from his own company points to a failure in segregating financial responsibilities.              |
|    | Inadequate Attention to Details: The prolonged period of undetected embezzlement suggests a lack of attention to financial detail within the company.          |
| 55 | Placing Too Much Trust in a Few Employees: Smith, given significant trust and access as an office manager, exploited this position.                            |
|    | Lack of Independent Checks on Performance: The prolonged period of undetected embezzlement suggests inadequate oversight of her financial activities.          |
|    | Inadequate Attention to Details: Failure to notice the unauthorized salary increases and fund transfers indicates a lack of attention to financial details.    |
| 56 | Lack of Independent Checks on Performance: The employers' failure to verify the legitimacy of Reyes' tax exemption claims indicates a lack of thorough checks. |

|    |  |
|----|--|
|    | Inadequate Attention to Details: Employers not noticing the anomalies in Reyes' W-4 forms suggests inadequate attention to payroll details.                          |
| 57 | Placing Too Much Trust in a Few Employees: Patel, as the owner, had unchecked control over the lab's operations.   |
|    | Inadequate Attention to Details: Lack of scrutiny into the legitimacy of the large volume of claims submitted.   |
|    | Lack of Separation of Duties: Control over operations, including the orchestration of kickbacks, points to a lack of internal checks and balances.                   |
| 58 | Placing Too Much Trust in a Few Employees: As CFO, Bowker was given significant trust and control over company finances.   |
|    | Lack of Independent Checks on Performance: The ability to embezzle and mismanage funds without immediate detection points to a lack of effective independent checks. |
|    | Inadequate Attention to Details: The extended period of fraudulent activities suggests a failure in monitoring and paying attention to financial details.            |
| 59 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Bankman-Fried, enabling misuse of funds.  |
|    | Lack of Independent Checks on Performance: The prolonged undetected scheme suggests a lack of effective independent checks.  |
|    | Inadequate Attention to Details: The organization failed to detect misappropriation of funds, indicating inadequate attention to financial details.                  |
| 60 | Inadequate Attention to Details: The prolonged period of undetected embezzlement indicates a lack of attention to financial details.                                 |
|    | Lack of Separation of Duties: Meeks' role encompassing bill payments, monitoring statements, and record maintenance allowed her to both commit and conceal fraud.    |
|    | Lack of Independent Checks on Performance: The failure to detect unauthorized purchases points to inadequate independent checks on her work.                         |
| 61 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Kewalis as President and CEO enabled her to exploit her position.                               |

|    |  |
|----|--|
|    | Lack of Independent Checks on Performance: The duration of the embezzlement suggests a lack of effective checks on her activities.                                     |
|    | Inadequate Attention to Details: Failure to detect the creation of fraudulent accounts and unauthorized entries indicates insufficient attention to financial details. |
| 62 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Hicks as IT Director, allowing misuse of resources.   |
|    | Lack of Independent Checks on Performance: The prolonged undetected fraud suggests a lack of effective independent monitoring.   |
|    | Inadequate Attention to Details: Failure to notice the misuse of company resources over a long period indicates a lack of attention to financial details.              |
| 63 | Placing Too Much Trust in a Few Employees: Lazzaro, as vault manager, was given significant trust with minimal oversight.  |
|    | Inadequate Attention to Details: Failure to quickly detect discrepancies in cash and records indicates a lack of attention to operational details.                     |
|    | Lack of Independent Checks on Performance: The absence of regular, independent checks enabled her continued theft.   |
| 64 | Placing Too Much Trust in a Few Employees: Excessive trust in McManus as CFO allowed financial misconduct.   |
|    | Inadequate Attention to Details: The organization failed to detect the misuse of funds, indicating inadequate attention to financial monitoring.                       |
|    | Lack of Independent Checks on Performance: The prolonged undetected embezzlement suggests a lack of effective independent checks within the company.                   |
| 65 | Placing Too Much Trust in a Few Employees: Sharar, as CFO, had significant trust and control over financial matters.   |
|    | Lack of Independent Checks on Performance: The prolonged undetected embezzlement indicates a lack of effective independent checks.                                     |

|    |   |
|----|---|
|    | Inadequate Attention to Details: Failure to detect the embezzlement suggests insufficient attention to financial details and reporting.                                 |
| 66 | Inadequate Attention to Details: Overlooking complex fraudulent activities.   |
|    | No Proper Authorization of Transactions: Lack of stringent controls over significant financial decisions.   |
|    | Lack of Clear Lines of Authority and Responsibilities: Potentially blurred lines enabling the CEO to manipulate financial data.   |
|    | Lack of Regular Review by the Internal Auditor: Failure to detect financial discrepancies and irregularities.   |
| 67 | Placing Too Much Trust in a Few Employees: Swanson, in her role as an accountant and controller, was likely given excessive trust and control over financial processes. |
|    | Inadequate Attention to Details: The prolonged period of embezzlement indicates a lack of attention to the details of payroll and accounting processes.                 |
|    | Lack of Separation of Duties: Swanson's ability to manipulate payroll processes suggests a failure in segregating financial responsibilities and duties.                |
| 68 | Placing Too Much Trust in a Few Employees: Kent had significant trust and control over procurement without adequate supervision.  |
|    | Inadequate Attention to Details: The failure to detect falsified receipts and invoices points to a lack of attention to financial details.                              |
|    | Lack of Separation of Duties: Kent's role enabled him to initiate, approve, and execute procurement processes.  |
| 69 | Placing Too Much Trust in a Few Employees: As CEO, Farley had excessive control with little oversight.  |
|    | Lack of Separation of Duties: Her role encompassed both operational and financial responsibilities, enabling the fraud.   |
|    | Inadequate Attention to Details: The organization failed to detect irregularities in bank transactions and tax remittances.   |
| 70 | Placing Too Much Trust in a Few Employees: McGlown's role allowed him significant unsupervised control, enabling the fraud.   |



|    |   |
|----|---|
|    | Inadequate Attention to Details: The ability to pass fake invoices and undetected fraudulent activities indicates a lack of thorough oversight.                 |
|    | Lack of Separation of Duties: The roles of McGlown and Gates enabled them to execute and conceal fraudulent transactions without checks.                        |
| 71 | Lack of Independent Checks on Performance: The ability to manipulate financial records suggests inadequate independent verification.                            |
|    | Inadequate Attention to Details: Failure to detect and prevent the manipulation of financial records and unpaid taxes.  |
| 72 | Placing Too Much Trust in a Few Employees: Excessive trust in Aggarwal as a director in the internal auditing department.                                       |
|    | Inadequate Attention to Details: Lack of sufficient scrutiny in verifying the legitimacy of vendor invoices.  |
|    | Lack of Separation of Duties: Aggarwal's position allowed him to oversee and manipulate financial transactions.   |
| 73 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Allen as a manager enabled his fraudulent actions.   |
|    | Lack of Independent Checks on Performance: The lack of effective checks and balances allowed Allen to divert funds without detection.                           |
|    | Inadequate Attention to Details: Failure to detect the diversion of such a significant amount of funds suggests a lack of detail-oriented financial monitoring. |
| 74 | Placing Too Much Trust in a Few Employees: Ritter, as a bank teller, was entrusted with direct access to customer accounts.                                     |
|    | Inadequate Attention to Details: The bank's failure to immediately detect unauthorized withdrawals from customer accounts.                                      |
| 75 | Placing Too Much Trust in a Few Employees: Steele's ascent to CEO provided her with unchecked control.  |
|    | Inadequate Attention to Details: The prolonged undetected embezzlement indicates a lack of scrutiny in financial monitoring within the organization.            |
|    | Lack of Separation of Duties: Steele's control over financial transactions without oversight.   |

|    |  |
|----|--|
| 76 | Placing Too Much Trust in a Few Employees: Rogas’s control over financial documents and bank statements without adequate oversight.                                |
|    | Lack of Independent Checks on Performance: Inadequate verification of financial information provided by Rogas, leading to undetected fraud.                        |
|    | Inadequate Attention to Details: Failure to detect discrepancies in financial records and reliance on falsified documents.   |
| 77 | Placing Too Much Trust in a Few Employees: As a commissioner, Sutton had a significant level of trust and authority that she misused.                              |
|    | Lack of Clear Lines of Authority and Responsibilities: Possible ambiguity in oversight and responsibilities that allowed such behavior to go unchecked.            |
| 78 | Placing Too Much Trust in a Few Employees: Mensinger, as Chief Lending Officer, held significant trust and authority, which he misused.                            |
|    | No Proper Authorization of Transactions: The unauthorized approval of loans based on false information indicates a failure in transaction authorization processes. |
| 79 | Placing Too Much Trust in a Few Employees: Valentin, as the credit manager, was trusted excessively without adequate oversight.                                    |
|    | Inadequate Attention to Details: The prolonged period of embezzlement suggests a lack of attention to financial monitoring within the organization.                |
|    | Lack of Separation of Duties: Her ability to intercept and redirect customer payments indicates a failure in separating financial responsibilities.                |
| 80 | Placing Too Much Trust in a Few Employees: Both individuals, as directors, were trusted with significant authority, which they exploited.                          |
|    | Lack of Independent Checks on Performance: The ability to approve invoices without independent verification enabled the bribery scheme.                            |
|    | Inadequate Attention to Details: The failure to detect the discrepancies in project certifications and payments.   |

|    |  |
|----|--|
| 81 | Placing Too Much Trust in a Few Employees: Williams’ roles as president of both AESC and FSESC allowed her undue control.  |
|    | Lack of Independent Checks on Performance: The undetected embezzlement indicates a failure in independent verification of financial activities.                    |
|    | Inadequate Attention to Details: The prolonged period of embezzlement suggests a lack of scrutiny in financial management.   |
| 82 | Placing Too Much Trust in a Few Employees: Crawford’s role in finance gave her extensive control without adequate oversight.                                       |
|    | Lack of Separation of Duties: As both manager of invoice approvals and overseer of the credit card program, she had ample opportunity to commit fraud.             |
|    | Inadequate Attention to Details: The college's failure to detect fraudulent invoices and improper credit card use indicates a lack of thorough financial scrutiny. |
| 83 | Placing Too Much Trust in a Few Employees: Excessive control by the CEO and President led to unchecked financial decisions.  |
|    | Inadequate Attention to Details: Failure of the organization to detect and address fraudulent claims made to investors.  |
| 84 | Placing Too Much Trust in a Few Employees: Smith’s executive roles likely provided her with significant unsupervised control.                                      |
|    | Inadequate Attention to Details: The prolonged period of undetected embezzlement suggests a lack of scrutiny in financial management.                              |
| 85 | Placing Too Much Trust in a Few Employees: As the president of the Booster Club, Anthony Sharper had significant unsupervised control.                             |
|    | Lack of Independent Checks on Performance: The embezzlement and tax fraud suggest a failure in independent verification of the Sharpers’ activities.               |
|    | Inadequate Attention to Details: The prolonged undetected misuse of funds indicates a lack of scrutiny in financial management within the Booster Club.            |

|    |  |
|----|--|
| 86 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Coday-Townes as office manager.   |
|    | Inadequate Attention to Details: The failure to detect false accounting entries and unauthorized use of signature stamp.   |
|    | Lack of Independent Checks on Performance: Inadequate verification of accounting entries and payroll data.   |
| 87 | Placing Too Much Trust in a Few Employees: Pike's role as a general manager likely provided him with significant autonomy and trust.   |
|    | Inadequate Attention to Details: The prolonged undetected fraud indicates a lack of scrutiny in invoice verification and approval processes.   |
| 88 | Placing Too Much Trust in a Few Employees: Sweeten's role as a bookkeeper, combined with the trust from knowing the company president, provided her with unsupervised access to financial resources. |
|    | Lack of Separation of Duties: Her ability to access and manage company funds without checks highlights a lack of duty segregation.   |
|    | Inadequate Attention to Details: The failure to detect unauthorized transactions and misuse of company assets indicates a lack of vigilance in financial oversight.                                  |
| 89 | Placing Too Much Trust in a Few Employees: Loconte's dual roles provided him excessive control without sufficient oversight.   |
|    | Inadequate Attention to Details: The prolonged period of fraudulent activities suggests a lack of detailed scrutiny in financial reporting.  |
|    | Lack of Independent Checks on Performance: Insufficient verification of payroll and tax reporting indicates a failure in independent oversight.  |
| 90 | Placing Too Much Trust in a Few Employees: Petrone's position allowed her significant autonomy with minimal oversight.   |
|    | Inadequate Attention to Details: The failure to detect the fraudulent purchase patterns over many years suggests a lack of detailed financial scrutiny.  |

|    |   |
|----|---|
| 91 | <p>Placing Too Much Trust in a Few Employees: Thumann’s role as a bookkeeper with significant control over payments and records.</p>                            |
|    | <p>Inadequate Attention to Details: The failure to detect the embezzlement for an extended period indicates a lack of scrutiny in financial reconciliation.</p> |
|    | <p>Lack of Independent Checks on Performance: The prolonged undetected fraud suggests inadequate independent verification of financial activities.</p>          |
| 92 | <p>Placing Too Much Trust in a Few Employees: Laansma's role as Financial Controller likely gave her significant autonomy and trust.</p>                        |
|    | <p>Lack of Independent Checks on Performance: The prolonged undetected embezzlement suggests insufficient independent verification of financial activities.</p> |
|    | <p>Inadequate Attention to Details: Failure to notice the misuse of a corporate credit card indicates a lack of thorough scrutiny in financial management.</p>  |
| 93 | <p>Placing Too Much Trust in a Few Employees: Burke’s role as a bookkeeper with control over issuing checks allowed significant unsupervised control.</p>       |
|    | <p>Inadequate Attention to Details: The failure to detect the embezzlement over a five-year period indicates a lack of scrutiny in financial management.</p>    |
|    | <p>Lack of Independent Checks on Performance: The prolonged undetected fraud suggests inadequate independent verification of financial activities.</p>          |
| 94 | <p>Placing Too Much Trust in a Few Employees: Burke's control over the company's finances as a controller allowed him significant unsupervised control.</p>     |
|    | <p>Lack of Independent Checks on Performance: The prolonged undetected fraud indicates inadequate independent verification of financial activities.</p>         |
| 95 | <p>Placing Too Much Trust in a Few Employees: Ahmed-Elkilani's role provided him with access to sensitive information, which he exploited.</p>                  |

|    |  |
|----|--|
|    | Inadequate Attention to Details: The prolonged undetected fraud suggests a lack of detailed oversight in transaction monitoring.   |
|    | Lack of Independent Checks on Performance: The absence of effective checks allowed him to manipulate transactions without detection.   |
| 96 | Placing Too Much Trust in a Few Employees: Lee’s position as a controller provided him with substantial control over financial transactions without adequate oversight.          |
|    | Lack of Independent Checks on Performance: The lack of detection of fraudulent activities over several years suggests inadequate independent verification and auditing.          |
| 97 | Placing Too Much Trust in a Few Employees: Carper’s ability to exploit pre-signed checks indicates excessive trust in her role.  |
|    | Inadequate Attention to Details: Failure to detect discrepancies in financial records and the misuse of pre-signed checks.   |
|    | Lack of Independent Checks on Performance: The prolonged undetected fraud suggests a lack of effective independent verification of financial activities.                         |
| 98 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Koch as a supervisor allowed the fraudulent scheme to be executed.  |
|    | Inadequate Attention to Details: The failure to notice the discrepancy in work hours versus actual work done suggests a lack of thoroughness.                                    |
|    | Lack of Separation of Duties: Koch's ability to manipulate time records and login credentials without checks indicates inadequate separation of duties.                          |
| 99 | Placing Too Much Trust in a Few Employees: Latoski’s role as Director of Accounting Services likely provided her with significant autonomy and control over financial processes. |
|    | Inadequate Attention to Details: The ability to charge and pay off large personal expenses unnoticed suggests a lack of scrutiny in financial management.                        |

|     |   |
|-----|---|
|     | Lack of Independent Checks on Performance: The prolonged period of undetected fraudulent activity indicates inadequate independent verification of accounting activities.                 |
| 100 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Kennedy and his colleagues allowed the scheme.   |
|     | Inadequate Attention to Details: Failure to detect the fraudulent activities for an extended period.  |
|     | Lack of Independent Checks on Performance: Inadequate independent verification of vendor relationships and transactions.  |
| 101 | Placing Too Much Trust in a Few Employees: Rigsbee's role as a financial advisor with significant control over client accounts indicates a high level of trust placed in him by the bank. |
|     | Inadequate Attention to Details: The failure of the bank to detect unauthorized transfers over several years points to a lack of thoroughness in monitoring account activities.           |
|     | Lack of Independent Checks on Performance: The prolonged period of undetected fraudulent activities suggests inadequate verification and oversight of employee actions.                   |
| 102 | Placing Too Much Trust in a Few Employees: Ellis's role as Financial Officer likely provided him with significant unsupervised control.   |
|     | Inadequate Attention to Details: The prolonged period of undetected embezzlement suggests a lack of thoroughness in financial oversight.  |
|     | Lack of Independent Checks on Performance: The failure to detect the misappropriation of funds over several years indicates inadequate independent verification of financial activities.  |
| 103 | Placing Too Much Trust in a Few Employees: Hall's long-term position as a manager provided her with excessive control and trust.  |
|     | Inadequate Attention to Details: Failure to detect the embezzlement and creation of fake loans over an extended period indicates a lack of thoroughness in financial oversight.           |
|     | Lack of Independent Checks on Performance: The prolonged period of undetected fraudulent activities suggests insufficient independent verification of financial transactions.             |

|     |  |
|-----|--|
| 104 | Lack of Clear Lines of Authority and Responsibilities: The ability to access and copy a large volume of sensitive files suggests a lack of strict control over employee access to proprietary information. |
|     | Inadequate Attention to Details: Failure to detect the unusual activity of a long-term employee accessing numerous files shortly before resignation.   |
| 105 | Placing Too Much Trust in a Few Employees: Bittner’s managerial role likely provided him with unsupervised control over financial transactions.  |
|     | Inadequate Attention to Details: The failure to detect the fraudulent activities over a lengthy period suggests a lack of thoroughness in financial monitoring.  |
| 106 | Placing Too Much Trust in a Few Employees: Welch's role as a bookkeeper with significant financial control likely provided unsupervised access to company funds.   |
|     | Inadequate Attention to Details: The prolonged period of undetected embezzlement suggests a lack of thoroughness in financial monitoring and reconciliation.   |
|     | Lack of Independent Checks on Performance: The failure to detect the fraudulent activities over several years indicates inadequate independent verification and oversight of financial operations.         |
| 107 | Placing Too Much Trust in a Few Employees: Ricker’s ability to access and misuse company checks suggests excessive trust placed in her without adequate oversight.   |
|     | Inadequate Attention to Details: The prolonged period of undetected embezzlement indicates a lack of thoroughness in monitoring financial transactions.  |
| 108 | Placing Too Much Trust in a Few Employees: Lutamila, as Director of Finance, was given considerable trust and authority.   |
|     | Inadequate Attention to Details: The prolonged period of embezzlement suggests a lack of thorough monitoring and oversight.  |
|     | Lack of Independent Checks on Performance: The fact that the scheme was only detected by a new CFO indicates a previous lack of effective independent verification.  |



|     |   |
|-----|---|
| 109 | Placing Too Much Trust in a Few Employees: Miller's supervisory role provided him with significant control over payroll and procurement.                                |
|     | Inadequate Attention to Details: The prolonged period of undetected fraud indicates a lack of scrutiny in verifying timesheets and invoices.                            |
|     | Lack of Independent Checks on Performance: Insufficient verification of Miller's activities and financial transactions.   |
| 110 | Placing Too Much Trust in a Few Employees: Topping's role as a manager provided him with substantial unsupervised control over financial resources.                     |
|     | Inadequate Attention to Details: The prolonged undetected embezzlement suggests a lack of thoroughness in financial monitoring and oversight.                           |
| 111 | Placing Too Much Trust in a Few Employees: Pylant's position as an office administrator allowed her significant control over financial transactions.                    |
|     | Inadequate Attention to Details: The failure to detect her fraudulent activities for several years indicates a lack of thorough monitoring.                             |
|     | Lack of Independent Checks on Performance: The prolonged undetected embezzlement and tax evasion suggest inadequate independent verification of financial transactions. |
| 112 | Placing Too Much Trust in a Few Employees: Aldi's dual roles provided her with extensive control over financial operations without sufficient oversight.                |
|     | Inadequate Attention to Details: The prolonged period of undetected fraud suggests a lack of thoroughness in monitoring financial transactions.                         |
|     | Lack of Independent Checks on Performance: The absence of effective checks and balances enabled the sustained embezzlement.   |
| 113 | Placing Too Much Trust in a Few Employees: Madison's role in handling expenses and her ability to manipulate this process without oversight.                            |

|     |   |
|-----|---|
|     | Inadequate Attention to Details: Failure to detect falsified claims and invoices over a significant period suggests insufficient attention to financial details.  |
|     | Lack of Independent Checks on Performance: The absence of effective verification of her activities within the accounting department.                              |
| 114 | Placing Too Much Trust in a Few Employees: Jones had broad financial responsibilities and access, indicating excessive trust without adequate oversight.          |
|     | Inadequate Attention to Details: Failure to detect misuse of company funds and fraudulent invoicing over several years.   |
|     | Lack of Independent Checks on Performance: Absence of effective checks on Jones' activities and financial transactions.   |
| 115 | Placing Too Much Trust in a Few Employees: Weston's role as an accountant allowed significant control over financial transactions without adequate oversight.     |
|     | Inadequate Attention to Details: The prolonged period of undetected embezzlement suggests a lack of scrutiny in financial management and auditing.                |
|     | Lack of Independent Checks on Performance: The absence of effective verification of accounting practices within the company.                                      |
| 116 | Placing Too Much Trust in a Few Employees: Cox's high-profile position likely afforded him significant autonomy and trust.  |
|     | Inadequate Attention to Details: Potential conflicts of interest were not adequately monitored or controlled, given his dual roles in business and politics.      |
|     | Lack of Independent Checks on Performance: The lack of oversight that allowed these fraudulent activities to occur over several years.                            |
| 117 | Placing Too Much Trust in a Few Employees: Garrett's role in handling both accounts payable and receivable provided excessive control without adequate oversight. |

|     |  |
|-----|--|
|     | Inadequate Attention to Details: The failure to detect fraudulent transactions over several months points to insufficient scrutiny of financial records.     |
|     | Lack of Independent Checks on Performance: The absence of effective internal checks allowed Garrett to manipulate financial records undetected.              |
| 118 | Placing Too Much Trust in a Few Employees: Abouammo's role at Twitter provided significant access to sensitive user data without sufficient oversight.       |
|     | Inadequate Attention to Details: Lack of detection of Abouammo's unauthorized access to user data indicates a failure in monitoring employee activities.     |
|     | Lack of Independent Checks on Performance: The absence of effective checks on Abouammo's access to confidential user information.                            |
| 119 | Placing Too Much Trust in a Few Employees: Sacco's role as a project manager likely provided him with significant autonomy and trust.                        |
|     | Inadequate Attention to Details: The lack of detection of inflated change orders over several years indicates insufficient attention to financial details.   |
| 120 | Placing Too Much Trust in a Few Employees: Levoff's high-level positions provided him with unsupervised access to sensitive financial information.           |
|     | Inadequate Attention to Details: The prolonged undetected insider trading indicates a lack of thoroughness in monitoring compliance with trading policies.   |
|     | Lack of Independent Checks on Performance: The absence of effective oversight of Levoff's activities within his department.                                  |
| 121 | Placing Too Much Trust in a Few Employees: Chandran's control over multiple companies allowed him to orchestrate the fraud without sufficient checks.        |
|     | Inadequate Attention to Details: Investors and possibly internal personnel failed to scrutinize the legitimacy of Chandran's claims and business operations. |

|     |   |
|-----|---|
| 122 | Placing Too Much Trust in a Few Employees: Broyles and his co-conspirators held significant control over the fraudulent activities.                                     |
|     | Inadequate Attention to Details: Lack of thorough due diligence by investors who did not detect the fraud.  |
|     | No proper authorization of transactions: Unauthorized and unverified investment transactions contributing to the fraud.   |
| 123 | Placing Too Much Trust in a Few Employees: Excessive trust placed in Barnes and DeGroot, leading to the misuse of funds.  |
|     | Lack of Independent Checks on Performance: Inadequate oversight of the activities of senior executives.   |
| 124 | Placing Too Much Trust in a Few Employees: Dodson's executive role likely provided him with unsupervised control over financial transactions.                           |
|     | Lack of Independent Checks on Performance: The prolonged period of undetected fraudulent activities suggests inadequate verification and oversight of Dodson's actions. |
| 125 | Placing Too Much Trust in a Few Employees: Phelps' role and actions indicate significant trust without sufficient oversight.  |
|     | No Proper Authorization of Transactions: Lack of verification and authorization in the credit approval process.   |
|     | Inadequate Attention to Details: Failure to detect falsified financial information used for substantial credit lines.   |
| 126 | Placing Too Much Trust in a Few Employees: Schessel, as CEO, had significant autonomy and trust, allowing him to manipulate public statements.                          |
|     | Inadequate Attention to Details: Failure by the company to verify and scrutinize the authenticity of Schessel's public claims.  |
|     | Lack of Independent Checks on Performance: Lack of effective oversight and verification of Schessel's activities and statements.  |
| 127 | Placing Too Much Trust in a Few Employees: Lucas's control over multiple companies' financial affairs indicates excessive trust without sufficient oversight.           |

|     |  |
|-----|--|
|     | Inadequate Attention to Details: The prolonged tax evasion suggests a lack of thoroughness in financial and tax compliance monitoring.   |
| 128 | Placing Too Much Trust in a Few Employees: Clark's high-level position and unsupervised control over trades and information.   |
|     | Inadequate Attention to Details: Failure of the company to detect Clark's kickback arrangements and misuse of information.   |
|     | Lack of Independent Checks on Performance: Absence of effective oversight or auditing of Clark's trading activities and decisions.   |
| 129 | Placing Too Much Trust in a Few Employees: As the owner, Abbas had significant control and autonomy over the financial aspects of her business.                                |
|     | Inadequate Attention to Details: The lack of oversight and verification of the proper use of allocated funds.  |
| 130 | Placing Too Much Trust in a Few Employees: The roles of these executives provided them with significant control over loan processes.   |
|     | Inadequate Attention to Details: The failure to adhere to SBA guidelines suggests a lack of scrutiny in loan administration.   |
| 131 | Lack of Independent Checks on Performance: The ability of these employees to engage in antitrust activities suggests insufficient oversight and verification of their actions. |
|     | Inadequate Attention to Details: The prolonged period of collusion indicates a lack of thorough monitoring of contract bidding processes.                                      |
| 132 | Placing Too Much Trust in a Few Employees: Harry's role as the owner allowed him significant autonomy and control over the operations.   |
|     | Inadequate Attention to Details: Failure by regulatory bodies to detect the complex scheme suggests a lack of thoroughness in oversight.                                       |
| 133 | Lack of Clear Lines of Authority and Responsibilities: Wakil's ability to orchestrate such a large-scale bribery scheme suggests a lack of clear oversight.                    |

|     |   |
|-----|---|
|     | Inadequate Attention to Details: The prolonged period of undetected illicit activities indicates a failure in monitoring financial transactions and partnerships.                           |
| 134 | Placing Too Much Trust in a Few Employees: Ray's position as City Clerk likely provided her significant control over financial transactions with limited oversight.                         |
|     | Inadequate Attention to Details: The failure to detect the embezzlement over several years suggests a lack of thoroughness in financial monitoring and auditing.                            |
|     | Lack of Independent Checks on Performance: The absence of effective verification of Ray's financial activities and record-keeping.  |
| 135 | Lack of Independent Checks on Performance: Their ability to orchestrate this scheme suggests inadequate oversight in their banking roles.   |
|     | Inadequate Attention to Details: The prolonged, undetected nature of the scheme indicates a lack of thorough monitoring in financial transactions.  |
| 136 | Placing Too Much Trust in a Few Employees: Halilov's ability to access and manipulate sensitive procurement information points to excessive trust placed in him without adequate oversight. |
|     | Lack of Independent Checks on Performance: The prolonged period of undetected corruption suggests a lack of effective monitoring and verification of Halilov's activities.                  |
| 137 | Placing Too Much Trust in a Few Employees: The roles of Han, Hu, and Lu allowed them significant control over loan applications without adequate oversight.                                 |
|     | Lack of Independent Checks on Performance: The absence of effective checks and balances to verify the authenticity of loan applications.  |
|     | Inadequate Attention to Details: Failure to detect falsified documents and irregularities in loan applications over an extended period.   |
| 138 | Placing Too Much Trust in a Few Employees: Barry's role in the campaign allowed him significant control over financial transactions without adequate oversight.                             |

|     |   |
|-----|---|
|     | Inadequate Attention to Details: The failure to detect unauthorized diversions of campaign funds over an extended period indicates a lack of thoroughness in monitoring financial activities. |
| 139 | Placing Too Much Trust in a Few Employees: Lewis's role in managing vendor payments allowed her significant control without adequate oversight.   |
|     | Inadequate Attention to Details: Failure by the company to detect the diversion of funds over an extended period suggests a lack of thorough monitoring.                                      |
|     | Lack of Independent Checks on Performance: Absence of effective verification of Lewis's activities within the accounts payable department.  |
| 140 | Inadequate Attention to Details: The failure to detect Xiao's undisclosed financial affiliations indicates a lack of thoroughness in vetting grant applications.                              |
|     | Lack of Independent Checks on Performance: The absence of effective oversight mechanisms to verify the accuracy and completeness of grant applications.                                       |
| 141 | Lack of Clear Lines of Authority and Responsibilities: The collusion with telemedicine companies and laboratories indicates blurred lines in professional responsibilities.                   |
|     | Inadequate Attention to Details: The ability to execute the scheme undetected suggests a lack of thoroughness in oversight by Medicare.   |
| 142 | Inadequate Attention to Details: Initially, the IRS's failure to detect Brassart's use of nominee corporations and false bankruptcy filings indicates a lack of thoroughness in monitoring.   |
|     | Lack of Independent Checks on Performance: The prolonged period before detection of Brassart's fraudulent activities suggests a lack of effective verification processes.                     |
| 143 | Inadequate Attention to Details: The prolonged undetected manipulation of commodity prices suggests a lack of thoroughness in monitoring trading activities.                                  |
|     | Lack of Independent Checks on Performance: The absence of effective oversight mechanisms to verify the legitimacy of trading activities.  |

|     |   |
|-----|---|
| 144 | Placing Too Much Trust in a Few Employees: Ribas's high-ranking positions provided him with significant control without adequate oversight.                                       |
|     | Inadequate Attention to Details: The failure to identify Ribas's unethical activities over an extended period suggests insufficient monitoring within Seguros Sucre.              |
| 145 | Placing Too Much Trust in a Few Employees: As the owner, Sabet had significant control with little oversight.   |
|     | Lack of Independent Checks on Performance: Inadequate monitoring mechanisms for financial transactions.   |
| 146 | Placing Too Much Trust in a Few Employees: Rashid, as CEO, had significant control over the clinics' operations, suggesting excessive trust was placed in his leadership.         |
|     | Lack of Separation of Duties: The absence of checks and balances in the decision-making process regarding patient treatment and billing practices.                                |
|     | Inadequate Attention to Details: Failure to ensure that medical procedures were necessary and beneficial to patients.   |
| 147 | Placing Too Much Trust in a Few Employees: Sreckovic's role in the company provided him with considerable control over financial decisions without adequate oversight.            |
|     | Inadequate Attention to Details: Lack of internal controls to ensure the proper filing and payment of employment taxes.   |
| 148 | Placing Too Much Trust in a Few Employees: Granting Devillez the sole responsibility and access for vendor payments indicates excessive trust.                                    |
|     | Inadequate Attention to Details: The failure to detect discrepancies in vendor payments over several years suggests a lack of thorough financial monitoring.                      |
|     | Lack of Separation of Duties: Combining the roles of preparing, approving, and executing payments in one individual shows a lack of internal control.                             |
| 149 | Placing Too Much Trust in a Few Employees: Giddens and Bozeman were trusted with access to sensitive medical resources, which they exploited.                                     |
|     | Inadequate Attention to Details: The failure to detect the misuse of prescription pads over an extended period suggests a lack of thoroughness in monitoring employee activities. |



|     |   |
|-----|---|
| 150 | Placing Too Much Trust in a Few Employees: Mercedes' role and the trust placed in her enabled the unauthorized access and transactions.                                       |
|     | Inadequate Attention to Details: The failure to detect the misuse of escrow checks and fraudulent transfers over several years.   |
| 151 | Placing Too Much Trust in a Few Employees: Heavy reliance on the CFO and key finance executives without adequate checks.  |
|     | Lack of Separation of Duties: Concentrated control in the hands of a few executives, leading to potential abuse of authority.   |
|     | Inadequate Attention to Details: Failure to detect discrepancies and irregularities in financial reports.   |
| 152 | Placing Too Much Trust in a Few Employees: Moreland's undue influence over the Drug Court Foundation despite no official position.  |
|     | Inadequate Attention to Details: Failure to detect the embezzlement suggests lack of scrutiny in financial oversight.   |
|     | Lack of Independent Checks on Performance: Absence of effective monitoring mechanisms for the foundation's financial transactions.  |
| 153 | Lack of Independent Checks on Performance: Deloitte's inability to detect TBW's fraudulent scheme suggests a lack of effective internal checks within their auditing process. |
|     | Placing Too Much Trust in a Few Employees: Relying heavily on the auditors' judgments without sufficient oversight or verification mechanisms.                                |
| 154 | Placing Too Much Trust in a Few Employees: As an office manager, Calaiaro likely had unsupervised access to financial documents and processes.                                |
|     | Inadequate Attention to Details: The prolonged undetected embezzlement indicates a lack of thoroughness in monitoring financial transactions.                                 |
| 155 | Placing Too Much Trust in a Few Employees: Hauk's ability to embezzle significant sums suggests excessive trust placed in him without adequate oversight.                     |

|     |  |
|-----|--|
|     | Inadequate Attention to Details: The prolonged period of undetected fraudulent activities indicates a lack of thoroughness in monitoring financial transactions.   |
|     | Lack of Independent Checks on Performance: The absence of effective checks and balances to verify Hauk's financial activities.   |
| 156 | Inadequate Attention to Details: The DEA's inability to initially identify this undisclosed employment highlights a lack of thoroughness in background checks.   |
| 157 | Inadequate Attention to Details: The failure to detect the unauthorized use of passwords and subscriber codes for an extended period points to a lack of thoroughness in monitoring access to sensitive information. |

## 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 Science*, Vol. 1, pp. 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.
- Agnew, R., 1992, 'Foundation for a general strain theory of crime and delinquency,' *Criminology*, Vol. 30 No. 1, pp. 47-87.
- Aguilera, R. V., & Vadera, A. K., 2008, 'The dark side of authority: Antecedents, mechanisms, and outcomes of organizational corruption.' *Journal of Business Ethics*, 77, 431-449.
- Albrecht, C., Albrecht, W., Dunn, J., 2001, 'Conducting a Pro-Active Fraud Audit: A Case Study.' *Journal of Forensic Accounting*, 2, 203-218.
- Albrecht, C., Kranacher, M. & Albrecht, S., 2008, Asset Misappropriation Research White Paper for the Institute for Fraud Prevention.
- Albrecht, C., Turnbull, C., Zhang, Y. & Skousen, C.J., 2010, 'The relationship between South Korean chaebols and fraud,' *Management Research Review*, Vol. 33 No. 3, pp. 257-268.
- Albrecht, W.S. 1991, 'Fraud in government entities: the perpetrators and the types of fraud,' *Government Finance Review*, Vol. 7 No. 6, pp. 27-30.
- Albrecht, W.S. 2014, 'Iconic Fraud Triangle endures: metaphor diagram helps everybody understand fraud,' *Fraud*.
- Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O., 2006, *Fraud examination (2nd ed.)*. Mason, OH: Thomson Higher Education.
- Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F., 2009, *Fraud Examination, 3<sup>rd</sup> edition*. Mason, OH: South-Western Cengage Learning.

Albrecht, W. S., Hill, N. C., & Albrecht, C. C., 2006, 'The ethics development model applied to declining ethics in accounting.' *Australian Accounting Review*, 16(1), 30-40.

Albrecht, W. S., Romney, M. B., Cherrington, D. J., Payne, I. R., & Roe, A. J., 1982, 'How to detect and prevent business fraud.' *Englewood Cliffs, NJ: Prentice-Hall.*

Albrecht, W., Albrecht, C., & Albrecht, C. 2004, 'Fraud and Corporate Executives: Agency, Stewardship and Broken Trust.' *Journal of Forensic Accounting*, 5, 109-130.

Albrecht, W.S., 1996. 'Employee fraud,' *Internal Auditor*, October, p. 26.

Albrecht, W.S., Albrecht, C., & Albrecht, C.C., 2008, 'Current Trends in Fraud and Its Detection: A Global Perspective,' *Information Security Journal* (17).

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

Albrecht, W.S., Williams, T.L. & Wernz, G.W., 1995, *Fraud: Bringing Light to the Dark Side of Business*, Burr Ridge, IL: Irwin.

Albright, S., & Denq, F. 1996, 'Employer attitudes toward hiring ex-offenders,' *Prison Journal*, 76, 118-138.

Allan, R., 2003, 'Fraud-the human face of fraud: understanding the suspect is vital to any investigation,' *CA Magazine-Chartered Accountant*, Vol. 136 No. 4, pp. 39-40.

Alleyne, P., & Howard, M., 2005, 'An exploratory study of auditors responsibility for fraud detection in Barbados,' *Managerial Auditing Journal*, Vol. 20 No. 3, pp. 284-303.

*American Accounting Association Annual Meeting*, San Francisco, CA, 31 July-4 August. Auditing: insights, practice implications, and future research directions.' *Auditing: A Journal of Practice & Theory*, Vol. 30 No. 3, pp. 1-31.

American Psychological Association, 2009, *Teaching tip sheet: self-efficacy*, American Psychological Association, viewed 05 May 2022, (<https://www.apa.org/pi/aids/resources/education/self-efficacy>).

Anand, V, Ashforth, BE, Joshi, M 2004, 'Business as usual: The acceptance and perpetuation of corruption in organizations.' *Academy of Management Executive* 18(2): 39–53.

Anderson, J., Jennings, M. & Reckers, P., 1991, 'An empirical study of hindsight bias in the evaluation of auditor decisions: revelations on the expectations gap,' *Arizona State University, AZ*, 1991.

Anderson, J., Jennings, M., & Reckers, P., 1992, 'The presence of hindsight bias in peer and judicial evaluation in public accounting litigation,' *Arizona State University, AZ*, 1992.

Andress, M. & Fonseca, B. 2000, *Manage People to Protect Data*, InfoWorld 22(46): 48.

Andrews, D. A., & Bonta, J. L. 2001, 'The Level of Service Inventory-Revised: Users' manual,' Toronto: *Multi-Health Systems*.

*Annual report on market fraud and its consequences*, 2020. Securities Exchange Commission.

Apostolou, B. A., Hassell, J. M., Webber, S. A. & Sumners, G. E., 2001, 'The relative importance of management fraud risk factors.' *Behavioral Research in Accounting*, 13(1), 1–24.

Argyris, C., 1964, *Integrating the individual and the organization*, New York, NY: John Wiley.

Ashforth, B., & Anand, V., 2003, 'The Normalization of Corruption in Organizations.' *Research in Organizational Behavior*, 25: 1-52.

Asmuni, A.I.H, Nawawi, A. & Salin, A.S.A.P., 2015, 'Ownership structure and auditor's ethnicity of Malaysian public listed companies,' *Pertanika Journal of Social Science and Humanities*, Vol. 23 No. 3, pp. 603-622.

Association of Certified Fraud Examiners, 2013, *Introduction to contract and procurement fraud*, PowerPoint presentation, Contract and Procurement Fraud, Association of Certified Fraud Examiners.

Atkinson, D., Fenster, C. A., & Blumberg, A. S. 1976, 'Employer attitudes toward work-release programs and the hiring of offenders,' *Criminal Justice and Behavior*, 3, 335-343.

Bao Y., Ke B., Li B., Yu Y. J. & Zhang J., 2020, 'Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach.' *J. Account. Res.* 58, 199–235.

Bartlett, N., Endo, R., Tonkin, E., & Williams, A., 2004, *Audit planning for the detection of fraud*, Milton, QLD: John Wiley & Sons, In R. Johnson (Ed.), Readings on auditing.

Baucus, M. S., 1994, 'Pressure, opportunity, and predisposition: A multivariate model of corporate illegality,' *Journal of Management*, 20(4), 699–721.

Beasley, M, Joseph V., Dana R. & dan Terry L., 2010, 'Fraudulent Financial Reporting.' In: *Proceedings of 23rd International Business Research Conference* 18 – 20, November 2013, Marriott Hotel, Melbourne, Australia, ISBN: 978-1-922069-36-8

Beasley, M., Carcello, J., Hermanson, D., & Lapedes, P. D., 2000, 'Fraudulent financial reporting: Consideration of industry traits and corporate governance mechanisms,' *Accounting Horizons* 14 (4): 441-454.

Beasley, M.S., 1996, 'An Empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud.' *The Accounting Review.* 71(4):443-465.

Beasley, S. M., Carcello, J. V. & Hermanson, D. R., 2010, 'Fraudulent Financial Reporting: 1997–2007: An Analysis of U.S. Public Companies.' *Research Report, Committee of Sponsoring Organizations of the Treadway Commission (COSO).*

Becker, C. L., DeFond, M. L. Jiambalvo, J. & Subramanyan, K.R., 1998, 'The Effect of Audit Quality on Earnings Management.' *Contemporary Accounting Research* 15 (1): 1–24.

Becker, D., Connolly, J., Lentz, P., & Morrison, J., 2006, 'Using the Business Fraud Triangle to Predict Academic Dishonesty among Business Students,' *Academy of Educational Leadership Journal* (10:1), pp. 37–54.

Becker, G., 1976, 'The Economic Approach to Human Behavior,' IL: *University of Chicago Press.* Chicago.

Becker, G.S., 1968, 'Crime and punishment: an economic approach.' *J. Polit. Econ.* 76 (2), 169–217.

Benson M. L., Madensen T. D. & Eck J. E., 2009, *White-collar crime from an opportunity perspective, The Criminology of White-Collar Crime*, New York, NY: Springer, pp.175–193. In: S. S. Simpson, D. Weisburd eds.

Benson, M. L., & Simpson, S. S., 2015, *Understanding white-collar crime: An opportunity perspective.* NY: New York: Routledge.

Beynon, D. 2001, *Talking Heads*, Computerworld 24(33): 19-21.

Black, W. K., 2005, 'Control Frauds' as Financial Super-Predators.' *The Journal of Socio-Economics* 34, 734-55.

Black, W.K., 2006, 'Book review: Control Fraud Theory v. The Protocols,' *Crime, Law and Social Change* 45(3): 241–258.

Bloomfield, R. J., 1997, 'Strategic Dependence and the Assessment of Fraud Risk: A Laboratory Study,' *The Accounting Review* 72 (4): 517-538.

Blumstein, A., 2000, *Some recent trends in US violence, the Crime Drop in America,* New York: Cambridge University Press, In: A. Blumstein and J. Wallman (eds.).

Blumstein, A., Cohen, J., Das, S., & Moitra, S. 1988, 'Specialization and seriousness during adult criminal careers,' *Journal of Quantitative Criminology*, 4, 303-345.

Blumstein, A. & Wallman, J., 2000, *The Crime Drop in America,* Cambridge University Press, New York.

Bolton, R.J., & Hand, D.J. 2001, 'Unsupervised profiling methods for fraud detection,' *Proceedings from, Conference on Credit Scoring and Credit Control*, 7, Edinburgh, UK, September, 5–7.

Bonner, S. E., Palmrose, Z.V. & Young, S. M., 1998, 'Fraud Type and Auditor Litigation: An Analysis of SEC Accounting and Auditing Enforcement Releases,' *The Accounting Review*, 73(4): 503-532.

Borck, J. 2000, *Advice for a Secure Enterprise: Implement the Basics and See That Everyone Uses Them*, InfoWorld 22(46): 90.

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), Elsevier, pp. 578–596, (<https://doi.org/10.1016/J.JACCPUBPOL.2015.05.006>).

Braithwaite, J., 1984, *Corporate Crime in the Pharmaceutical Industry*, Routledge and Kegan Paul: London.

Braithwaite, J. & Petit, C., 1990, *Not Just Deserts: A Republican Theory of Criminal Justice*, Oxford: Oxford University Press.

Braithwaite, J., 1992, *Poverty, power and white-collar crime; Sutherland and the paradoxes of criminological theory, White Collar Crime Reconsidered*. Boston, MA: North-Eastern University Press, pp. 78 – 108, In: K. Schlegel and D. Weisburd (eds.).

Brantingham, P., & Brantingham, P., 1981, 'Introduction: The Dimensions of Crime.' *Environmental Criminology*, Pp. 7-26, edited by P. J. Brantingham and P. L. Brantingham. London: *Waveland Press*.

Breidenbach, S. 2000, 'How Secure Are You?' *InformationWeek* (800): 71-78.

Brown, E. D., & Ibekwe, E. E., 2018, 'Effect of Institutional Factors on Foreign Direct Investment in Nigeria,' *The Economics and Finance Letters*, 5(1), 12-27.

Brownfield, D., & Sorenson, A. M., 1993, 'Self-control and juvenile delinquency: Theoretical and an empirical assessment of selected elements of a general theory of crime,' *Deviant Behavior*, 14, 243-264.

Button, M., Gee, J. & Brooks, G., 2011, 'Measuring the cost of fraud: an opportunity for the new competitive advantage,' *Journal of Financial Crime*, Vol. 19 No. 1, pp. 65-75.

Carcello, J. V., & Nagy, A. L., 2004, 'Audit Firm Tenure and Fraudulent Financial Reporting,' *Auditing: A Journal of Practice and Theory* 23 (September): 55–69.

Carcello, J., & Hermanson, D., 2008, 'Fraudulent Financial Reporting: How Do We Close the Knowledge Gap?' *Institute for Fraud Prevention*, Morgantown, WV.

Carcello, J., Hermanson, D., & Ye, Z., 2011, 'Corporate governance research in accounting and auditing: insights, practice implications, and future research directions,' *Auditing: A Journal of Practice & Theory*, Vol. 30 No. 3, pp. 1-31.



Chen, M., Chen, C. C., & Sheldon, O. J., 2016, 'Relaxing moral reasoning to win: how organizational identification relates to unethical pro-organizational behavior,' *J. Appl. Psychol.* 101, 1082–1096.

Cieslewicz, J., 2010, 'The fraud square: societal influences on the risk of fraud,' paper presented at 2010 *American Accounting Association Annual Meeting*, San Francisco, CA, 31 July-4 August.

Cieslewicz, J.K., 2011, 'Culture and accounting: ramifications for fraud prevention, the development of international accounting, and reporting,' *Dissertation Abstracts International Section A: Humanities and Social Sciences*, Vol. 71, No. 12-A, p. 4446.

Cieslewicz, J.K., 2012, 'The Fraud Model in International Contexts: A Call to Include Societal level Influences in the Model,' *Journal of Forensic & Investigative Accounting* (4:1), pp. 214–254.

Clark-Dickson, P. 2001, *Alarmed and Dangerous*, e-Access December 2023.

Clark, L. D. 2004, 'A civil rights task: Removing barriers to employment of ex-convicts,' *University of San Francisco Law Review*, 38, 193-211

Clarke, R.V. 1997, *Situational Crime Prevention: Successful Case Studies*, 2nd ed., Harrow and Heston Publishers, Guilderland, NY.

Clarke, R. V., 1999, 'Hot Products: Understanding, Anticipating and Reducing Demand for Stolen Goods,' *Police Research series paper* 112. London: Home Office.

Clarke, R.V. & Harris, M. 1992, 'A rational choice perspective on the targets of automobile theft,' *Criminal Behaviour and Mental Health*, Vol. 2 No. 1, pp. 25-42.

Clarke, R.V. & Weisburd, D., 1994, 'Diffusion of Crime Control Benefits,' Pp. 165-83 in *Crime Prevention Studies, vol. 2, Crime Prevention Studies*, edited by R. V. Clarke. Monsey, NY: Criminal Justice Press.

Clarke, R. V. & Cornish, D. B., 1985, 'Modeling Offenders' Decisions: A Framework for Research and Policy,' Pp. 147-85 in *Crime and Justice: An Annual Review of Research*, vol. 6, edited by M. Tonry and N. Morris. Chicago: *University of Chicago Press*.

Clarke, R. V. & Felson, M., 1993, *Introduction: Criminology, Routine Activity, and Rational Choice*, Pp. 259-94 in *Routine Activity and Rational Choice, vol. 5, Advances in*

*Criminological Theory*, edited by R. V. Clarke and M. Felson. New Brunswick: Transaction.

Coenen, T., 2008, *Essentials of Corporate Fraud*, John Wiley and Sons, NJ.

Cohen J., Holder-Webb L., Sharp D., & Pant L., 2007, 'The effects of perceived fairness on opportunistic behavior,' *Contemp. Account. Res.* 24, 1119–1138.

Cohen, J. R., Pant, L. W. & Sharp, D. J., 1998, 'The effect of gender and academic discipline diversity on ethical evaluations, ethical intentions and ethical orientation of potential public accounting recruits,' *Accounting Horizons* 12 (3): 250–270.

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.

Cohen, L. E. & Felson, M., 1979, 'Social Change and Crime Rate Trends: A Routine Activity Approach,' *American Sociological Review* 44:588-608.

Coleman J. W., 1987, 'Toward an integrated theory of white-collar crime,' *Am. J. Sociol.* 93, 406–439.

Connell, J., Ferress, N., & Travaglione, T., 2004, 'Engendering trust in manager-subordinate relationships: Predictors and outcomes,' *Personnel Review*, 32(5), 569–590.

Conolly, P. 2000, *Security Starts from Within*, InfoWorld 22(28): 39-40.

*Contract audits: Role in helping ensure effective oversight and reducing improper payments (GAO-11-331T)*, 2011, Washington, DC: Government Accountability Office. (GAO). (2011a, February).

*Contract management: DoD vulnerabilities to contracting fraud, waste, and abuse*, 2006, Washington, DC: Government Accountability Office. (GAO). (2006, 7 July).

Copes, H., & Vieraitis, L. M. 2009a, 'Bounded rationality of identity thieves: Using offender-based research to inform policy,' *Criminology and Public Policy*, 8, 237–262.

Copes, H., & Vieraitis, L. M. 2009b, 'Understanding identity theft: Offender's accounts of their lives and crimes,' *Criminal Justice Review*, 34, 329–349.

Copes, H., & Vieraitis, L. M. 2012, *Identity thieves: Motives and methods*, Boston: Northeastern University Press.

Coram, P., Ferguson, C. & Moroney, R., 2008, 'Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud,' *Accounting and Finance*, Vol. 0 No. 0, pp. 543-559.

Cornish, D. B. & Clarke, R. V., (eds.) 1986, *The Reasoning Criminal: Rational Choice Perspectives on Offending*, New York: Springer Verlag.

Cornish, D. B., & Clarke, R. V., 1986, 'Crime as a rational choice,' In *Criminological Theory: Past to Present* (eds FT Cullen, R Agnew): 278–83. Roxbury Publishing.

Cressey, D., 1953, *Other People's Money; a Study in the Social Psychology of Embezzlement*. Glencoe, IL, Free Press.

Cressey, D.R., 1953, 'The criminal violation of financial trust,' *American Sociological Review*, Vol. 15 No. 6, pp. 738-743.

Cressey, D.R., 1973, *Other People's Money: A Study in the Social Psychology of Embezzlement*. Patterson Smith.

Cross, C. 2015, 'No laughing matter: Blaming the victim of online fraud,' *International Review of Victimology*, 21(1), 187-204. doi:10.1177/0269758015571

Dabney, D. 1995, 'Neutralization and deviance in the workplace: Theft of supplies and medicine by hospital nurses,' *Deviant Behavior*, 16, 313-331.

Dellaportas, S. 2013, 'Conversations with Inmate Accountants: Motivation, Opportunity and the Fraud Triangle,' *Accounting Forum* (37:1), pp. 29–39.

Dinev, T. & Hart, P. 2010, 'Internet privacy concerns and their antecedents - measurement validity and a regression model,' *Behavior & Information Technology*, 23(5), 357-370. doi:10.1080/01449290410001715723

Doe, J., & Roe, M. 2017, 'The impact of regulatory fines on corporations,' *Journal of Financial Regulation*, 13(2), 234-256.

Donegan, J.J., & Ganon, M.W. 2008, 'Strain, Differential Association, and Coercion: Insights from Criminology Literature on Causes of Accountant's Misconduct,' *Accounting and the Public Interest* (8:1), pp. 1–20.

Dorminey, J.W., Fleming, A.S., Kranacher, M. & Riley, R.A. 2010, 'Beyond the fraud triangle: Enhancing deterrence of economic crimes,' *The CPA Journal*, Vol. 80 No. 7, pp. 17-24.

Dorminey, J.W., Fleming, A.S., Kranacher, M. & Riley, R.A. 2012, 'The Evolution of Fraud Theory,' *Issues in Accounting Education*, vol. 27, no. 2, p. 555-579.

Duffield, G. & Grabosky, P. 2001, 'The Psychology of Fraud Trends and Issues in Crime and Criminal Justice,' Bd. 199, *Australian Institute of Criminology*, Canberra.

Duffin, M., Keats, G., & Gill, M. 2006, 'Identity theft in the UK: The offender and victim perspective,' *Perpetuity Research and Consultancy International Ltd.*

Eifler, S. 1998, *Do opportunities make smokers?* Theoretical and empirical analyses of self-control, opportunities, and tobacco smoking. 90-116.

Elliot, A.J. & Devine, P.G. 1994, 'On the motivational nature of cognitive dissonance: dissonance as psychological discomfort,' *Journal of Personality and Social Psychology*, Vol. 67 No. 3, pp. 382-394.

*Enterprise Risk Management – Integrated Framework*, 2004, The Committee of Sponsoring Organizations of the Treadway Commission.

Enzle, M. E., & Anderson, S. C. 1993, 'Surveillant intentions and intrinsic motivation,' *Journal of Personality and Social Psychology*, 64(2), 257–266.

Fama E. F., & Jensen, M. C. 1983, 'Separation of Ownership and Control,' *Journal of Law and Economics* 26(2): 301-325.

Farrell, G. & Pease, K. 1994, 'Crime Seasonality—Domestic Disputes and Residential Burglary in Merseyside 1988-90,' *British Journal of Criminology* 34:487-98.

Farrington, D. P. 1995, 'The development of offending and antisocial behavior from childhood: The key findings from the Cambridge study in delinquent development,' *Journal of Child Psychology and Psychiatry*, 36, 1-36.

Feldman, Y. & Lobel, O. 2010, 'The incentives matrix: the comparative effectiveness of rewards, liabilities, duties, and protections for reporting illegality,' *Texas Law Review*, Vol. 88 No. 6, pp. 1151-1211

Felson, M. 1995, *Those Who Discourage Crime*. Pp. 53-66 in *Crime and Place*, vol. 4, edited by D. Weisburd and J. E. Eck. Monsey, NY: Criminal Justice Press.

Felson, M. 2002, *Crime and everyday life (3rd ed.)*, Thousand Oaks, CA: Sage.

Felson, M., & Ronald, C. V. 1998, 'Opportunity Makes the Thief: Practical Theory for Crime Prevention,' *Police Research Group: Police Research Series Paper 98:36*.

Festinger, L. A. 1957, *A theory of cognitive dissonance*. Evanston, IL: Peterson.

Festinger, L. A. 1962, *An Introduction to the Theory of Dissonance, A Theory of Cognitive Dissonance*. Stanford University Press, Stanford, CA.

Fetchenhauer, D., & Simon, J. 1998. 'General Theory of Crime', 81, 301-315.

Fisher, K. 2015, *The psychology of fraud: What motivates fraudsters to commit crime?* Texas: Texas Woman's University.

Fitzpatrick, T. 2000, 'Critical cyber policy: Network technologies, massless citizens, virtual rights,' *Critical Social Policy* 20 (3): 375 – 407.

*Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response*, 2006, KPMG International.

*Fraudulent Financial Reporting: 1987-1997 – Analysis of US. Public Companies*, 1999, New York, NY: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Free, C. 2015. 'Looking through the Fraud Triangle: A Review and Call for New Directions,' *Meditari Accountancy Research* (23:2), Emerald Group Publishing Limited, pp. 175–196.

Free, C., & Murphy, P. R. 2015, 'The ties that bind: The decision to co-off end in fraud,' *Contemporary Accounting Research*, 32(1): p.18-54.

Friedrichs, D.O. 2004, *Trusted Criminals: White-Collar Crime in Contemporary Society*, Wadsworth, Belmont, CA.

*From Compliance to Competitive Edge: New Thinking on Internal Control*, 2007, EYGM Limited: Ernst and Young.

Fullerton, R. R., & Durtschi, C. 2010, 'The Effect of Professional Skepticism on The Fraud Detection Skills of Internal Auditors,' *Utah State University Working Paper*.

Furman, B.R. 1995, 'Solid screening procedures minimize workplace crime: Special Report,' *Hotel & Motel Management*, Vol.210, No.10, p.29.

Gao, L., & Srivastava, R. P. 2008, 'The Anatomy of Management Fraud Schemes: Analyses and Implications,' Working paper, *University of Nebraska and University of Kansas*.

Gbegi, D. O., & Adebisi, J. F. 2015, 'Analysis of fraud detection and prevention strategies in the Nigerian public sector,' *Journal of Good Governance and Sustainable Development in Africa (JGGSDA)*, 2(4), 109-128.

Geiger, M.A., 1989, 'The new audit report: an analysis of exposure draft comments,' *Auditing: A Journal of Practice & Theory*, Vol. 8 No. 2, Spring 1989, pp. 40-63.

Geis, G. 2011, 'White-collar and Corporate Crime: a Documentary and Reference Guide,' *ABC-CLIO*, Santa Barbara, CA.

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, 437-444.

*Global Fraud Report*, 2013, viewed 12 March 2022, from <http://fraud.kroll.com/introduction/>

*Global Fraud Study: Report to the nation on occupational fraud and abuse, 2018, Asia-Pacific Edition*. pp. 1-28, Association of Certified Fraud Examiners.

*Global profiles of the fraudster: Technology enables, and weak controls fuel the fraud*, 2016, KPMG International. Retrieved December 13, 2017

Golladay, K. & Holtfreter, K. 2017, *The consequences of identity theft victimization: an examination of emotional and physical health outcomes*, Victims and Offenders, Vol. 12 No. 5, pp. 741-760.

Gottfredson, M.L. & Hirschi, T. 1990, *A General Theory of Crime*, Stanford University Press, Palo Alto, CA.

Gottschalk, P. 2016, *Explaining white-collar crime: The concept of convenience in financial crime investigations*, UK: London: Palgrave Macmillan.

Gottschalk, P. 2017, *Understanding white-collar crime: A convenience perspective*, FL: Boca Raton: CRC Press, Taylor & Francis.

Grasmick, H. G., Tittle, C. R., Bursik, R. J., Jr., & Arneklev, B. J. 1993, 'Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime,' *Journal of Research in Crime and Delinquency*, 30, 5-29.

Great Britain. Companies Act 2006, *Section 1 (c. 46)*, viewed 10 September 2023, (<https://www.legislation.gov.uk/ukpga/2006/35/section/1>)

Green, L. 1995, 'Cleaning Up Drug Hot Spots in Oakland, California: The Displacement and Diffusion Effects.' *Justice Quarterly* 12:737-54.

Greenberg, D. F. 1991, 'Modeling criminal careers' *Criminology*, 29, 17-45.

Greenberg, L., & Barling, J. 1999, 'Predicting employee aggression against coworkers, subordinates and supervisors: The roles of person behaviors and perceived workplace factors,' *Journal of Organizational Behavior*, 20, 897-913.

Greengard, S. 1995, 'Avoid negligent hiring: are you well armed to screen applicants?' *Personnel Journal*, Vol. 74, No. 12, p.84.

Greenwood, P., & Shaw, E. 2022, 'Evaluating the costs and benefits of fraud prevention measures in organizations,' *Journal of Business Ethics*, 160(1), 45-60.

*Guidance on Auditing for Fraud*, 2021, Public Company Accounting Oversight Board, PCAOB.

Hackenbrack, K. 1993, 'The effect of experience with different sized clients on auditor evaluations of fraudulent financial reporting indicators,' *Auditing: J. Practice Theory* 12(1) 99-100.

Harrell, E. & Langton, L. 2013, 'Victims of Identity Theft, 2012,' *Bureau of Justice Statistics*, NCJ243779.

Hauser C. 2019, 'Fighting against corruption: does anti-corruption training make any difference?' *J. Bus. Ethics* 159, 281–299.

Hauser C., Hogenacker J. 2014, 'Do firms proactively take measures to prevent corruption in their international operations?' *Eur. Manag. Rev.* 11, 223–237.

Heiman, V. 1990, 'Auditors' Assessments of the Likelihood of Analytical Review Explanations,' *The Accounting Review* (65): 870-890.

*High risk series: An update (GAO-09-271)*, 2009, Washington, DC: Government Accountability Office. (GAO). (2009, January).

*High risk series: An update (GAO-11-278)*, 2011, Washington, DC: Government Accountability Office. (GAO). (2011b, February).

Hochstetler, A., & Copes, H. 2003, *Managing fear to commit felony theft*. In P. Cromwell (Ed.), *In their own words: Criminals on crime* (pp. 87–98). Los Angeles: Roxbury.

Hogan, C. E., Rezaee, Z. Riley, Jr., R. A. & Velury, U. K. 2008, 'Financial Statement Fraud: Insights from the Academic Literature,' *Auditing: A Journal of Practice & Theory* 27 (2): 231-252.

Hollinger, R.C. & J.P. Clark 1983, *Theft by Employees*, D.C. Heath.

Holtfreter, K. 2008, 'Determinants of fraud losses in nonprofit organizations,' *Nonprofit Management and Leadership*, Vol. 19 No. 1, pp. 45-63.

Holtfreter, K. 2008, 'The effects of legal and extra-legal characteristics on organizational victim decision-making,' *Crime, Law, & Social Change*, Vol. 50 Nos 4/5, pp. 307-330.

Holtfreter, K., Beaver, M., Reising, M.D. & Pratt, T.C. 2010a, 'Low self-control and fraud offending,' *Journal of Financial Crime*, Vol. 17 No. 2, pp. 295-307.

Holtfreter, K., Reising, M.D. & Pratt, T.C. 2008a, 'Low self-control, routine activities, and fraud Victimization,' *Criminology*, Vol. 46 No. 1, pp. 189-220.



Holtfreter, K., Reisig, M.D., Piquero, N.L. & Piquero, A.R. 2010b, 'Low self-control and fraud: offending, victimization, and their overlap,' *Criminal Justice and Behavior*, Vol. 37 No. 2, pp. 188-203.

Holtfreter, K., VanSlyke, S., Bratton, J. & Gertz, M. 2008b, 'Public perceptions of white-collar crime and punishment,' *Journal of Criminal Justice*, Vol. 36 No. 1, pp. 50-60.

Holtfreter, R.E. & Holtfreter, K. 2006, 'Gauging the effectiveness of US identity theft legislation,' *Journal of Financial Crime*, Vol. 13 No. 1, pp. 56-64.

Holtfreter, K., Reisig, M.D., Pratt, T.C. & Holtfreter, R.E. 2015, 'Risky remote purchasing and identity theft victimization among older internet users,' *Psychology, Crime and Law*, Vol. 21 No. 7, pp. 681-698.

Holton, C. 2009, 'Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion-dollar problem,' *Decision Support Systems*, Vol. 46, No. 4, pp. 853-864.

Holzer, H. J. 1996, *What employers want: Job prospects for less-educated workers*, New York: Russell Sage.

Holzer, H. J., Raphael, S., & Stoll, M. A. 2003, 'Employment barriers facing ex-offenders,' *Paper presented at the Urban Institute Re-entry Roundtable on Employment Dimensions of Re-entry: Understanding the Nexus Between Prisoner Re-entry and Work*, New York University Law School, New York.

Hooper, M.J. 2010, 'Detering and Detecting Financial Fraud: A Platform for Action,' *Center for audit quality*.

Howe, M. A., & Malgwi, C. A. 2006, 'Playing the ponies: A \$5 million embezzlement case,' *Journal of Education for Business*, 82(1), 27-33.

Howe, M.A. & Malgwi, C.A. 2006. 'Playing the Ponies: A \$5 Million Embezzlement Case,' *Journal of Education for Business* (82:1), pp. 27-33.

Huang, S. M., Yen, D. C., Yang, L. W., & Hua, J. S. 2008, *An investigation of Zipf's Law for fraud detection*, *Decision Support Systems*, 46(1), 70-83.

Huber, W.D. 2012. 'Is Forensic Accounting in the United States Becoming a Profession?' *Journal of Forensic and Investigative Accounting* (4:1), pp. 255-284.

Huber, W.D. 2016. 'Forensic Accounting, Fraud Theory, and the End of the Fraud Triangle,' *Journal of Theoretical Accounting Research* (12:2), pp. 28–48.

Huber, W.D. 2017, 'Forensic accounting, fraud theory, and the end of the Fraud Triangle,' *Journal of Theoretical Accounting Research*, Vol. 12 No. 2, pp. 28-49.

Hunter P 2002, 'Canal plus versus NDS case,' *Network Security* 4: 9–11.

Husnin, A.I., Nawawi, A. & Salin, A.S.A.P. 2013, 'Corporate governance structure and its relationship with audit fee – Evidence from Malaysian public listed companies,' *Asian Social Science*, Vol. 9 No. 15, pp. 305-317

Husnin, A.I., Nawawi, A. & Salin, A.S.A.P. 2016, 'Corporate governance and auditor quality Malaysian evidence,' *Asian Review of Accounting*, Vol. 24 No. 2, pp. 202 – 230

*Internal control management and evaluation tool (GAO-01-1008G)*, 2001, Washington, DC: Government Accounting Office. (GAO). (2001, August).

*Internal control-integrated framework*, 1992, Committee of Sponsoring Organizations of the Treadway Commission (COSO).

*International Standards for the Professional Practice of Internal Auditing*, 2007, Altamonte Springs, FL: The IIA Research Foundation, Institute of Internal Auditors (IIA).

Jackson, K., Holland, D., Albrecht, C., & Woolstenhulme, D. 2010, 'Fraud Isn't Just for Big Business: Understanding the Drivers, Consequences, and Prevention of Fraud in Small Business,' *Journal of International Management Studies* (5:1), pp. 160–164.

Johansson, E., & Carey, P. 2016, 'Detecting fraud: The role of the anonymous reporting channel,' *Journal of Business Ethics*, 139(2), 391-409.

Johnson, L. 2021, 'Customer trust and corporate fraud: A case study analysis,' *Corporate Reputation Review*, 24(3), 175-189.

Jones, A. 2019, 'Insurance and fraud: Navigating the complex landscape,' *Risk Management Magazine*, 66(5), 22-29.

Karpoff J. M., Koester A., Lee D. S., Martin G. S. 2017, 'Proxies and databases in financial misconduct research,' *Account. Rev.* 92, 129–163.

Kassem, R. & Higson, A. 2012, 'The new fraud triangle model,' *Journal of Emerging Trends in Economics and Management Sciences*, Vol. 3 No. 3, p. 191.

Kelly, P. & Hartley, C. 2010, 'Casino gambling and workplace fraud: a cautionary tale for managers,' *Management Research Review*, Vol. 33 No. 3, pp. 224-239.

Kennedy, K. A. 2012, 'An analysis of fraud: Causes, prevention and notable cases,' *University of New Hampshire Scholars' Repository*.

Kenyon, W., & Tilton, P.D. 2006, *Potential Red Flags and Fraud Detection Techniques: A Guide to Forensic Accounting Investigation*, (First Edit.), New Jersey: John Wiley & Sons Inc.

Kinard, J. & Renas, S. 1991, 'Negligent hiring: are hospitals vulnerable?' *Public Personnel Management*, Vol.20, No.3, p.263.

Krambia Kapardis, M. & Papastergiou, K. 2016, 'Fraud victimization in Greece: room for improvement in prevention and detection,' *Journal of Financial Crime*, Vol. 23, pp. 481-500.

Kranacher, M.J. & Riley, R. 2019, *Forensic accounting and fraud examination*, John Wiley & Sons.

Kranacher, M.J., Riley, R. & Wells, J.T. 2010, *Forensic Accounting and Fraud Examination*, John Wiley and Sons, Hoboken, NJ.

Kranacher, M.J., Riley, R. & Wells, J.T. 2011, *Forensic Accounting and Fraud Examination*, John Wiley & Sons Inc.

Lamnek, S. 1994, *Neue Theorien abweichenden Verhaltens [Developments in criminological theory]*, München, Germany: Fink.

Laycock, G. 2004, 'Evaluation of the UK car theft index,' In: M. Maxfield and R.V. Clarke (eds.) *Understanding and preventing car theft*, *Crime Prevention Studies*, Vol. 17, Monsey, NY: Criminal Justice Press.

Leeson, N. 1996, *Rogue Trader: How I Brought Down Barings Bank and Shook the Financial World*, Boston, MA: Little, Brown & Company.

Levi, M. & Handley, J. 2002, 'Criminal Justice and the Future of Credit Card Fraud,' London: *Institute for Public Policy Research*.

Levi, M. 1994, *Masculinity and white-collar crime*. In: T. Newburn and B. Stanko (eds.) *Just Boys Doing Business*. London: Routledge, pp. 234 – 252.

Levi, M. 2008, *Combating identity and other forms of payment Fraud in the UK: An analytical history*. In: M. McNally and G. Newman (eds.) *Perspectives on Identity Theft, Crime Prevention Studies*, Vol. 23. Cullompton, UK: Willan Publishing, pp. 111 – 131.

Levi, M. 2009, *Financial crime*, In Tonry (ed), *Oxford Handbook of Crime and Public Policy* (pp. 223–246). New York, NY: Oxford University Press.

Levi, M., Burrows, J., Fleming, M. H., & Hopkins, M. 2007, *The Nature, Extent and Economic Impact of Fraud in the UK*. London: ACPO.

Libby, R. & Frederick, D. M. 1990, 'Experience and the Ability to Explain Audit Findings,' *Journal of Accounting Research*, 28, 348-367.

Lister, L.M. 2007, 'A Practical Approach to Fraud Risk,' *Internal Auditor*, pp. 1–30.

Loebbecke, J., Eining, M. & Willingham, J. 1989, 'Auditor's Experience with Material Irregularities: Frequency, Nature, and Detectability,' *Auditing: A Journal of Practice and Theory*, 9, pp. 1-28.

Lokanan, M. 2018, 'Theorizing financial crimes as moral actions,' *European Accounting Review*, Vol. 27 No. 5, pp. 901-938.

Lokanan, M.E. 2014, 'How senior managers perpetuate accounting fraud? Lessons for fraud examiners from an instructional case,' *Journal of Financial Crime*, Vol. 21 No. 4, pp. 411-423.

Lokanan, M.E. 2014, 'The demographic profile of victims of investment fraud: a Canadian perspective,' *Journal of Financial Crime* 21(2): 226–242.

Lokanan, M.E. 2015, 'Challenges to the Fraud Triangle: Questions on Its Usefulness,' *Accounting Forum* (39:3), pp. 201–224.

Longshore, D. 1998, 'Self-control and criminal opportunity: A prospective test of the general theory of crime,' *Social Problems*, 45, 102-113.

Longshore, D., & Turner, S. 1998, 'Self-control and criminal opportunity. Cross-sectional test of the general theory of crime,' *Criminal Justice and Behavior*, 25, 81-98.

Longshore, D., Turner, S., & Stein, J. A. 1996, 'Self-control in a criminal sample: An examination of construct validity,' *Criminology*, 34, 209-228.

Mackevicius, J. & Giriunas, L. 2013, 'Transformational research of the fraud triangle,' *Ekonomika*, Vol. 92 No. 4, pp. 150-163.

*Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention 2005.*  
New York, NY: American Institute of Certified Public Accountants.

Mansor, N., & Abdullahi, R. 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 Science*, 1, 38-45.

Mayhew, P., Clarke, R. V., Sturman, A., & Hough, J. M. 1976, 'Crime as Opportunity,' London: *Her Majesty's Stationery Office*.

Merton, R. K. 1968, *Social theory and social structure*. New York: The Free Press.

Miller, L., & Cross, F. 2022, *Fraud Prevention in Modern Enterprises*, Cambridge University Press.

Milne, G. 2003, 'How well do consumers protect themselves from identity theft?' *Journal of Consumer Affairs*, Vol. 37 No. 2, pp. 388-402.

Mischel W. 2014, *The marshmallow test: Mastering self-control*. New York, NY: Little Brown and Company.

Mitchell, A., Sikka, P., & Willmott, H. 1998, 'Sweeping it under the carpet: The role of accountancy firms in money laundering,' *Accounting Organization & Society*, 23(5/6), 589–607.

Mohamed, M. 2013, 'Countering Fraud in the Insurance Industry: A Case Study of Malaysia' *University of Portsmouth*.

Mohamed, N., Mohd Sanusi, Z., Marjuni, N. S., & Johari, R. J. 2010, 'The Effectiveness of Internal Control System Towards Deterring Fraud In Government Agencies,' *Accounting Research Institute & Faculty of Accountancy*. UiTM.

Moore, T., Clayton, R. & Anderson, R. 2009, 'The economics of online crime,' *The Journal of Economic Perspectives* 23(3): 3–20.

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), pp. 170–194.

Moyes, G., & Baker, C. R. 2003, 'Auditors' beliefs about fraud detection effectiveness of standards audit procedures,' *Journal of Forensic Account*, IV (2), 199–216.

Mukamal, D., & Samuels, P. 2003, 'Statutory limitations on civil rights of people with criminal records,' *Fordham Urban Law Journal*, 30, 1501-1506.

Mukoro, D. O., Yamusa, O., & Faboyede, O. S. 2013, 'The Role of Forensic Accounting in Fraud Detection and National Security,' *B VIMSR's Journal of Management Research*, 5(1), 40-47.

Munchus, G. III. 1992, 'Check references for safer selection; employee selection; Recruitment,' *HR Magazine*, Vol.37, No.6, p.75.

Murphy, P. 2012, 'Attitude, Machiavellianism and the rationalization of misreporting,' *Accounting, Organizations and Society*, Vol. 37 No. 5, pp. 242-259.

Murphy, P.R. & Dacin, T.M. 2011, 'Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations,' *Journal of Business Ethics* (101:4), pp. 601–618.

Murphy, P.R. & Free, C. 2016, 'Broadening the Fraud Triangle: Instrumental Climate and Fraud,' *Behavioral Research in Accounting* (28:1), pp. 41–56.

Murphy, P.R., Free, C. & Branston, C. 2012, 'The role of ethical climate in fraud,' *SSRN Electronic Journal*, doi: 10.2139/ssrn.1986989.

Nelson, M. W., Elliott, J. A. & Tarpley, R. L. 2003, 'How are Earnings Managed?' *Examples from Auditors, Accounting Horizons* (Supplement): 17-35.

Newman, P., Rhoades, S. & Smith, R. 1996, 'Allocating Audit Resources to Detect Fraud,' *Review of Accounting Studies* 1(2): 161-182.

Nosworthy, J. 2000, 'Implementing Information Security in the 21st Century - Do You Have the Balancing Factors?' *Computers and Security* 19(4): 337-347.

Noviani, D. P., & Sambharakreshna, Y. 2014, 'Pencegahan kecurangan dalam organisasi pemerintahan,' *Journal of Auditing, Finance, and Forensic Accounting*, 2(2), 61-70.

Odom, C. 1995, 'Candid candidates: what's behind the resume? Employment screening,' *Security Management*, Vol.39, No.5, p.66.

Okezie, A. 2012, 'An analysis of fraud in Nigerian banks,' *American Charter of Economics and Finance*, 1(2), 60-73.

Omar, N., Said, R. & Johari, Z.A. 2016, 'Corporate crimes in Malaysia: a profile analysis,' *Journal of Financial Crime*, Vol. 23 No. 2, pp. 257-272.

Omar, N.B. & Mohamad Din, H.F. 2010, 'Fraud diamond risk indicator: an assessment of its Importance and usage,' *CSSR 2010 - 2010 International Conference on Science and Social Research*, pp. 607-612.

Othman, R., Aris, N. A., Mardziyah, 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.

Padgett, S. 2015, 'About the association of certified fraud examiners and the report to the nations on occupational fraud and abuse,' *Profiling the Fraudster*, pp. 239-242.

- Palmrose, Z. V. 1987, 'Litigation and independent auditors: The role of business failures and management fraud,' *Auditing: A Journal of Practice & Theory* 6: 90–103.
- Park, Y.J., Matkin, D.S. & Marlowe, J. 2016, 'Internal control deficiencies and municipal borrowing costs,' *Public Budgeting & Finance*, Vol. 37 No. 1, pp. 88-111.
- Peltier-Rivest, D. & Lanoue, N. 2011, 'Thieves from within: occupational fraud in Canada,' *Journal of Financial Crime*, Vol. 19 No. 1, pp. 54-64.
- Peltier-Rivest, D. & Lanoue, N. 2015, 'Cutting fraud losses in Canadian organizations,' *Journal of Financial Crime*, Vol. 22 No. 3, pp. 295-304.
- Perols J. L., Bowen R. M., Zimmermann C. & Samba B. 2017, 'Finding needles in a haystack: using data analytics to improve fraud prediction,' *Account. Rev.* 92, 221–245.
- Perry, L. 1991, 'Background checks on potential workers easing some hospitals' liability concerns,' *Modern Healthcare*, April 15, 1991, Section: Staffing, p.68.
- Peterson, B. 2003, 'Fraud Education for Accounting Students,' *Journal of Education for Business*, 78(5), pp.263-267.
- Pfarrer M. D., Smith K. G., Bartol K. M., Khanin D. M. & Zhang X. 2008, 'Coming forward: the effects of social and regulatory forces on the voluntary restatement of earnings subsequent to wrongdoing,' *Organ. Sci.* 19, 386–403.
- Pincus, K. V. 1989, 'The efficacy of a red flags questionnaire for assessing the possibility of fraud,' *Accounting, Organ. Soc.* 14(1–2) 153–163.
- Piquero, A. R., & Rosay, A. B. 1998, 'The reliability and validity of Grasmick et al.'s self-control scale: A comment on Longshore et al.,' *Criminology*, 36, 157-73.
- Piquero, A. R., & Tibbetts, S. G. 1996, 'Specifying the direct and indirect effect of low self-control and situational factor in offenders decision making: Toward a more complete model of rational offending,' *Justice Quarterly*, 13, 481-510.
- Piquero, A.R., Jennings, W.G. & Farrington, D.P. 2010, 'On the malleability of self-control: theoretical and policy implications regarding a general theory of crime,' *Justice Quarterly*, Vol. 27 No. 6, pp. 803-834.



Piquero, N., Cohen, M. & Piquero, A. 2011, 'How much is the public willing to pay to be protected from identity theft?' *Justice Quarterly*, Vol. 28 No. 3, pp. 437-459.

Piquero, N. L., Schoepfer, A., & Langton, L. 2010, 'Completely out of control or the desire to be in complete control? how low self-control and the desire for control relate to corporate offending,' *Crime & Delinquency*, 56(4), 627–647.

Piquero, N.L., Tibbetts, S.G., & Blankenship, M.B. 2005, 'Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime,' *Deviant Behavior* (26:2), pp. 159–188.

Pontell, H.N. & Geis, G. 2007, 'New times, new crimes: “blocking” financial identity fraud,' In F. Bovenkerk and M. Levi (eds), *The Organized Crime Community* (Vol. 6, pp. 45–58). New York, NY: Springer.

Pusch N., & Holtfreter K. 2021, 'Individual and organizational predictors of white-collar crime: a meta-analysis,' *J. White Collar Corporate Crime* 2, 5–23.

Rae, K. & Subramaniam, N. 2008, 'Quality of Internal Control Procedures: Antecedents and Moderating Effect on Organisational Justice and Employee Fraud,' *Managerial Auditing Journal* (23:2), pp. 104–124.

Rahman, R. A., & Anwar, I. S. K. 2014, 'Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks,' *Procedia-Social and Behavioral Sciences*, 145, 97-102.

Rahman, R. A., & Anwar, I. S. K. 2014, 'Types of Fraud among Islamic Banks in Malaysia,' *International Journal of Trade, Economics and Finance*, 5(2), 176-179.

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), pp. 521–533.

Ramamoorti, S., & Olsen, W. 2007, *Fraud: The human factor*, Financial Executive.

Ramamoorti, S., Morrison, D., & Koletar, J. W. 2009, 'Bringing Freud to Fraud: Understanding the State of Mind of the C-Level Suite/White Collar Offender Through “A-B-C” Analysis,' Working paper, *Institute for Fraud Prevention.*, 1–35.

Ramamoorti, S., Morrison, D., & Koletar, J.W. 2014, 'Bringing Freud to Fraud,' *Journal of Forensic & Investigative Accounting* (6:1), pp. 47–81.

Ramamoorti, S., Morrison, D., Koletar, J.W., & Pope, K. R. 2013, *A.B.C.'s of Behavioral Forensics: Applied Psychology to Financial Fraud Prevention and Detection*, Hoboken, NJ: John Wiley & Sons.

Raphael, S, Michael, S, & Holzer, H. J. 2000, 'Are Suburban Firms More Likely to Discriminate against African Americans?' *Journal of Urban Economics* 48:485–508.

Reed, G. E., & Yeager, P. C. 1996, 'Organizational offending and neoclassical criminology: Challenging the reach of a general theory of crime,' *Criminology*, 34(3), 357–382.

Rengert, George F. & J. Wasilchick. 1985, *Suburban Burglary: A Time and Place for Everything*, Springfield, IL: C.C. Thomas.

*Report to Nations on Occupational Fraud and Abuse, 2008*, Association of Certified Fraud Examiners, Austin, TX: Association of Certified Fraud Examiners.

*Report to the Nation on Occupational Fraud and Abuse, 2016*, Austin, TX: Association of Certified Fraud Examiners.

*Report to the nations on occupational fraud and abuse, 2010*, Austin, TX: Association of Certified Fraud Examiners.

*Report to the Nations on Occupational Fraud and Abuse, 2014*, Austin: Association of Certified Fraud Examiners.

*Report to the Nations on Occupational Fraud and Abuse, 2018*, Austin, TX: Association of Certified Fraud Examiners.

*Report to the Nations on Occupational Fraud and Abuse, 2020*, Association of Certified Fraud Examiners.

*Report to the nations on occupational fraud and abuse: 2012 Global Fraud Study, 2012*, Austin, TX: Association of Certified Fraud Examiners.

*Report to the nations on occupational fraud and abuse: Who is Most Likely to Commit Fraud at Your Company, 2010*, Association of Certified Fraud Examiners. Retrieved from <http://www.acfe.com/press-release.aspx?id=1677>.

*Reports on audited financial statements 1988*, Statement on Auditing Standards No. 58, American Institute of Certified Public Accountants (AICPA), New York, NY, 1988.

Rezaee, Z. 2002. *Financial Statement Fraud: Prevention and Detection*, New York: John Wiley & Sons, Inc

Rezaee, Z. 2002, 'Causes, consequences and deterrence of financial statement fraud,' *Critical Perspectives on Accounting* 16(3):277-298.

Rezaee, Z. 2005, 'Causes, Consequences, and Deterrence of Financial Statement Fraud,' *Critical Perspectives on Accounting*, 16(3), 277-298.

Rodgers, W., Söderbom, A., & Guiral, A. 2015, 'Corporate social responsibility enhanced control systems reducing the likelihood of fraud,' *Journal of Business Ethics*, 131(4), 871-882.

Rose, A., Rose, J., & Dibben, M. 2010, 'The effects of trust and management incentives on audit committee judgments,' *Behavioral Research in Accounting*, 22(2), 87-103.

Rose, J. 2007, 'Attention to evidence of aggressive financial reporting and intentional misstatement judgments: Effects of experience and trust,' *Behavioral Research in Accounting*, 19(1), 215-229. doi:10.2308/bria.2007.19.1.215

Ross, I. 2016, *Exposing fraud: Skills, process, and practicalities*. Chichester, West Sussex: John Wiley & Sons, Inc.

Rossouw, G. J., Mulder, B., & Barkhuysen, B. 2000, 'Defining and understanding fraud: A South African case study,' *Business Ethics Quarterly*, 10(4), 885-895.

Sakurai, Y., & Smith, R. 2003, 'Gambling as a motivation for the commission of finance crime, trends and issues in crime and criminal justice,' No. 25, *Australian Institute of Criminology*, Canberra.

Sampson, R., Eck, J. & Dunham, J. 2010, 'Super controllers and crime prevention: a routine activity explanation of crime prevention success and failure,' *Security Journal*, Vol. 23 No. 1, pp. 37-51.

Sauser, W.I. 2007, 'Employee Theft: Who, How, Why, and What Can Be Done,' *Advanced Management Journal* (72:3), pp. 13–25.

Schuchter, A. & Levi, M. 2013, 'The fraud triangle revisited,' *Security Journal*, Vol. 29 No. 2, pp. 1-15.

Schuchter, A. & Levi, M. 2015, 'Beyond the Fraud Triangle: Swiss and Austrian elite fraudsters,' *Accounting Forum*, Vol. 39 No. 3, pp. 176-187.

Schwarzwalder, R. 1999, 'Intranet Security,' *Database and Network Journal* 22(2): 58-62.

Seipel, C. 1999a, 'Die Bedeutung von Gelegenheitsstrukturen in der General Theory of Crime von Michael R. Gottfredson & Travis Hirschi (1990) [The relevance of opportunity in the general theory of crime of Michael R. Gottfredson and Travis Hirschi (1990)],' *Soziale Probleme*, 10, 144-165.

Seipel, C. 1999b, 'Strategien und Probleme des empirischen Theorienvergleichs in den Sozialwissenschaften. Rational Choice Theorie oder Persönlichkeitstheorie? [Strategies and problems within an empirical comparison of theories],' *Opladen, Germany: Leske + Budrich*.

Seipel, C. 2000, 'Ein empirischer Vergleich zwischen der Theorie geplanten Verhaltens von Icek Ajzen und der Allgemeinen Theorie der Kriminalität von Michael R. Gottfredson und Travis Hirschi [An empirical comparison of the theory of planned behavior of Icek Ajzen and the general theory of crime of Michael R. Gottfrdson and Travis Hirschi],' *Zeitschrift für Soziologie*, 29, 399-412.

Shover, N., Coffey, G.S. & Hobbs, D. 2003, 'Crime on the line. Telemarketing and the changing nature of professional crime,' *British Journal of Criminology* 43(3): 489–505.

Shover, N., Coffey, G.S. & Sanders, C.R. 2004, 'Dialing for dollars: opportunities, justifications, and telemarketing fraud,' *Qualitative Sociology* 27(1): 59–75.

Silver, S.E., Fleming, A.S. & Riley, R.A. 2008, 'Preventing and detecting collusive management fraud,' *The CPA Journal*, Vol. 78, pp. 46-48.

Simpson, S. S., & Koper, C. S. 1992, 'Deterring corporate crime,' *Criminology*, 30(3), 347-375.

Simpson, S.S. & Piquero, N.L. 2002, 'Low self-control, organizational theory, and corporate Crime,' *Law & Society Review*, Vol. 36 No. 3, pp. 509-547.

Singleton, T.W. & Singleton, A.J. 2010, *Fraud Auditing and Forensic Accounting, 4th ed.*, John Wiley and Sons, Hoboken, NJ.

Sizer, R. & J. Clark. 1989, 'Computer Security - A Pragmatic Approach for Managers,' *Information Age* 11(2): 88-98.

Skousen, C., & Wright C. 2008, 'Contemporary risk factors and the prediction of financial statement fraud,' *Journal of Forensic Accounting*, 9(1), 37-62.

Skousen, C., Kevin R., & Charlotte J. 2008, 'Detecting and Predicting Financial Statement Fraud: The Effectiveness of the Fraud Triangle and SAS No. 99.'

Skousen, C.J., Smith, R.K.R. & Wright, C.J. 2009, 'Detecting and Predicting Financial Statement Fraud: The Effectiveness Of The Fraud Triangle and SAS No. 99,' *Corporate Governance And Firm Performance Advance In Financial Economics*, Vol. 13, h.53-81

Smith, G. & Crumbley, D. 2009, 'How Divergent Are Pedagogical Views toward the Fraud/ Forensic Accounting Curriculum?' *Global Perspectives on Accounting Education* (6:1), pp. 1-24.

Smith, G., Button, M., Johnston, L. & Frimpong, K. 2011, *Understanding Fraud: Contemporary Issues in White Collar Crime*, Palgrave, Basingstoke.

Smith, J. F. & Kida, T. 1991, 'Heuristics and Biases: Expertise and Task Realism in Auditing,' *Psychological Bulletin* (109): 472-489.

Smith, R., 2018, 'Legal expenditures and their role in corporate fraud cases,' *Harvard Business Law Review*, 8(2), 309-332.

Smith, T. 2004, 'Low self-control, staged opportunity, and subsequent fraudulent behavior,' *Criminal Justice and Behavior*, Vol. 31 No. 5, pp. 542-563.

Smith, T. 2019, 'The psychological impact of fraud on organizations,' *Journal of Organizational Behavior*, 40(7), 789-802.

Soltani, B. 2014, 'The anatomy of corporate fraud: a comparative analysis of high profile American and European corporate scandals,' *Journal of Business Ethics*, Vol. 120 No. 2, pp. 251-274.

Spathis, C. 2002, 'Detecting false financial statements using published data: some evidence from Greece,' *Managerial Auditing Journal*, 17(4), 179–191.

Spathis, C., Doumpos, M. & Zopounidis, C. 2002, 'Detecting Falsified Financial Statements: A Comparative Study Using Multicriteria Analysis and Multivariate Statistical Techniques,' *The European Accounting Review*, 11(3): 509-535.

Spathis, C., Doumpos, M., & Zopounidis, C. 2003, 'Using client performance measures to identify pre-engagement factors associated with qualified audit reports in Greece,' *The International Journal of Accounting*, 38(3), 267–284.

Sridharan, U. & Hadley, L. 2018, 'Internal Audit, Fraud and Risk Management at Wells Fargo,' *Journal of the Academic Business World* (12:1), pp. 49–53.

*Standards for internal control in the federal government (GAO/AIMD-00-21.3.1)*, 1999, Washington, DC: General Accounting Office. (GAO).

*Statement on Auditing Standards No. 99: Consideration of Fraud in a Financial Statement Audit 2002*. New York, NY: American Institute of Certified Public Accountants.

Stoll, M. A., & Raphael, S. 2000, 'Racial Differences in Spatial Job Search Patterns: Exploring the Causes and Consequences,' *Economic Geography* 76:201–23.

Suh, J. B., Nicolaides, R., & Trafford, R. 2019, 'The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions,' *International Journal of Law, Crime and Justice*, 56, 79-88.

Sutherland, E.H. 1939, *Principles of Criminology*, JB Lippincott, Chicago.

Sutherland, E.H. 1940, 'White collar criminality,' *American Sociological Review*, Vol. 5 No. 1, pp. 1-12.

Sutherland, E.H. 1942, 'The development of the theory of differential association,' *The Ohio Valley Sociologist*, Vol. 15 No. 1, p. 3.

Sutherland, E.H. 1983, *White Collar Crime: The Uncut Version*, Yale University Press.

Svensson, R. 2002, 'Strategic offences in the criminal career context,' *British Journal of Criminology* 42 (2): 395 – 411.

*Taking Data Analytics to the Next Level*, 2013, Association of Certified Fraud Examiners Inc.

Taylor, S., & Brown, D. 2020, 'Operational disruptions and their link to financial fraud,' *Journal of Operational Management*, 38(4), 201-215.

Tedeschi, J., & Felson, R. B., 1994, 'Violence, Aggression and Coercive Act,' *American Psychological Association Books*. Washington.

*The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*, 2009, International Standard on Auditing 240, International Auditing and Assurance Standards Board, New York, NY.

*The Global Economic Crime Survey: Economic Crime in a Downturn: The 5th Biennial Global Economic Crime Survey*, 2009, New York, NY: PricewaterhouseCoopers (PwC).

*The next normal: Preparing for a post-pandemic fraud landscape, 2021*, Association of Certified Fraud Examiners, (<https://www.acfe.com/fraud-resources/covid-19-benchmarking-report>)

Tibbetts, S. G., & Myers, D. L. 1999, 'Low self-control, rational choice, and student test cheating,' *American Journal of Criminal Justice*, 23, 179-200.

Tilley, N. 1993, 'Understanding Car Parks, Crime and CCTV: Evaluation Lessons from Safer Cities,' *Police Research Group: Crime Prevention Unit Series Paper* 42:33.

Tilley, N., & Webb, J. 1994, 'Burglary Reduction: Findings from Safer Cities Schemes,' *Police Research Group: Crime Prevention Unit Paper* No 51:60.

Tillman, R. & Indergaard, M. 2007, *Corporate Corruption in the New Economy. International Handbook of White-Collar and Corporate Crime*, edited by Henry Pontell and Gilbert Geis, Springer.

Tillyer, M.S. & Eck, J.E. 2011, 'Getting a handle on crime: a further extension of routine activities theory,' *Security Journal*, Vol. 24 No. 2, pp. 179-193.

Timofeyev, Y. 2015, 'Analysis of predictors of organizational losses due to occupational corruption,' *International Business Review*, Vol. 24 No. 4, pp. 630-641.

Tinker, T., & Okcabol, F. 1991, 'Fatal attractions in the agency relationship,' *British Accounting Review*, 23, 329–354.

Tittle, C. R., & Botchkovar, E. V. 2005, 'Self-control, criminal motivation and deterrence: An investigation using Russian respondents,' *Criminology*, 43, 307-354.

Tittle, C. R., Ward, D. A., & Grasmick, H. G. 2004, 'Capacity for self-control and individual's interest in exercising self-control,' *Journal of Quantitative Criminology*, 20, 143–172.

Transparency International, 2015, *The Corruption Index Perception. Berlin*, Tersedia di, viewed 02 January 2024, ([www.transparency.org](http://www.transparency.org)).

Trompeter, G., Carpenter, T., Desai, N., Jones, K., & Riley, D. 2013, 'A synthesis of Fraud Related Research,' *Auditing: A Journal of Practice and Theory* (32:1), pp. 769–804.

Trompeter, G., Carpenter, T., Jones, K., & Riley, D. 2014, 'Insights for Research and Practice: What We Learn about Fraud from Other Disciplines,' *Accounting Horizons* (28:4), pp. 769–804.

UN Convention Against Corruption: Progress Report, 2013, Transparency International, viewed 08 July 2023, ([www.transparency.org](http://www.transparency.org)).

Verton, D. 2000, 'Companies Aim to Build Security Awareness,' *Computerworld* 34(48): 24.

Von Solms, B. 2000, 'Information Security - The Third Wave?' *Computers and Security* 19(7): 615-620.

Vona, L. W. 2008, *Fraud risk assessment: Building a fraud audit program*, Hoboken New Jersey: John Wiley and Sons, 1-250.



Vousinas, G.L. 2019, 'Advancing theory of fraud: the S. C. O. R. E. model,' *Journal of Financial Crime*, Vol. 26 No. 1, pp. 372-381.

Walsh, D., 1994, 'The obsolescence of crime forms,' In: R. Clarke (ed.) *Crime Prevention Studies*, Vol. 2, Monsey, NY: Criminal Justice Press.

*Warfighter Support: DoD needs additional steps to fully integrate operational contract support into contingency planning*, 2013, Washington, DC: Government Accountability Office. (GAO). (2013, February 8).

Weisburd, D & Green, L., 1995, *Measuring Immediate Spatial Displacement: Methodological Issues and Problems*, Pp. 349-61 in *Crime and Place*, vol. 4, *Crime Prevention Studies*, edited by J. E. Eck and D. Weisburd. Monsey, NY: Criminal Justice Press.

Weisburd, D. & Waring, E. 2001, *White-collar Crime and Criminal Careers*, Cambridge University Press, Cambridge.

Weisburd, D., Waring, E., & Chayet, E. 1995, 'Specific deterrence in a sample of offenders convicted of white-collar crimes,' *Criminology*, 33(4), 587-607.

Weiss, D., 2014, 'Internal controls in family-owned firms,' *European Accounting Review*, Vol. 23 No. 3, pp. 463-482.

Wells, J. T., 2008, *Principles of Fraud Examination. 2nd edition*. Hoboken, NJ: John Wiley and Sons.

Wells, J., 2004, 'New approaches for fraud deterrence,' *Journal of Accountancy*, Vol. 197 No. 2, pp. 72-76.

Wells, J.T. 2001, 'Why employees commit fraud: It's either greed or need,' *Journal of Accountancy*, Vol. 191 No. 2, pp. 89-91.

Wells, J.T., 2011, *Corporate Fraud Handbook: Prevention and Detection*, Hoboken, New Jersey: John Wiley & Sons Inc.

Wells, J.T. 2017, *Corporate Fraud Handbook: Prevention and Detection*, Hoboken, New Jersey: John Wiley & Sons Inc.

West, J., Bhattacharya, M., & Islam, R., 2015, 'Intelligent Financial Fraud Detection Practices: An Investigation.'

*What Boards Need to Know About Financial Statement Fraud*, 2004, Across the Board, October 5–7. KPMG.

Wilks J., & Zimbelman, M. 2004, 'Decomposition of Fraud Risk Assessments and Auditors' Sensitivity to Fraud Cues,' *Contemporary Accounting Research*, Vol. 21, No. 3, pp. 719-745.

Williams J. W. 2013, 'Regulatory technologies, risky subjects, and financial boundaries: governing 'fraud' in the financial markets,' *Acc. Organ. Soc.* 38, 544–558.

Wimbush, J. C., & Dalton, D. R. 1997, 'Base rate for employee theft: Convergence of multiple methods,' *Journal of Applied Psychology*, 82, 756-763.

Wolfe, D., & Hermanson, D., 2004, 'The fraud diamond: considering the four elements of fraud,' *The CPA Journal*, December, 34-37.

Yeager, P. C., & Reed, G. E. 1998, 'Of corporate people and straw men: A reply to Herbert, Green, and Larragoite,' *Criminology*, 36, 885-897.

Young, M.R., 2000, *Accounting Irregularities and Financial Fraud*, San Diego: Harcourt Inc.

Zahra, S. A., Priem, R. L. & Rasheed, A. A. 2005, 'The Antecedents and Consequences of Top Management Fraud,' *Journal of Management*, 31(6): 803 -828.

Zahra, S. A., Priem, R. L., & Rasheed, A. A. 2007, 'Understanding the causes and effects of top management fraud,' *Organizational Dynamics*, 36(2), 122–139.

Zakaria, K.M., Nawawi, A., & Salin, A.S.A. P. 2016. 'Internal Controls and Fraud – Empirical Evidence from Oil and Gas Company,' *Journal of Financial Crime* (23:4), pp. 1154–1168.

Zikmund, P.E. 2008, 'Reducing the Expectation Gap,' *The CPA Journal* CPA (78:6), pp. 20–25.