FROM THE SCAMMER PERSPECTIVE: PREDISPOSITIONS TOWARDS ONLINE FRAUD MOTIVATION AND RATIONALIZATION

by

Subia Ansari

A Thesis

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Master of Science

Department of Computer and Information Technology
West Lafayette, Indiana
August 2020

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Ida Ngambeki, Chair

Department of Computer and Information Technology

Dr. Kathryn Seigfried-Spellar

Department of Computer and Information Technology

Dr. John Springer

Department of Computer and Information Technology

Approved by:

Dr. John Springer

Dedicated to my mother and my father.

ACKNOWLEDGMENTS

First and foremost, I’d like to thank my mother and father for being a constant source of inspiration to me and for always believing in me. I could not have gotten here without your guidance and support. I will forever be grateful to you for the opportunities you have given. To my brothers thank you for being there and helping me relax when I was under pressure. To the rest of my family and friends, thank you for everything you have done to support me and help me follow my dreams.

To Dr. Ida Ngambeki, thank you for your insight and support during this study. It was with your guidance and constant feedback that I was able to produce a study of this quality. You have inspired me in many ways, I have always been in awe of the amount of knowledge you have, and I have learnt a lot from you. I am extremely grateful that I had the opportunity to work with you.

To Dr. Kathryn Seigfried-Spellar, thank you for helping me improve the quality of this study. The feedback and resources that you shared with me formed an essential part of this study. I’d also like to thank you for teaching me how to conduct statistical analyses, I am not scared of the results section in research papers anymore.

To Dr. John Springer, thank you for your help in this project and for asking me to keep things simple. I will always remember that advice.

TABLE OF CONTENTS

LIST OF TABLES 7

LIST OF FIGURES 8

ABSTRACT 10

CHAPTER 1. INTRODUCTION 11

1.1 Problem Statement 11

1.2 Significance 12

1.3 Scope 13

1.4 Research Design 13

1.5 Assumptions 14

1.6 Limitations 15

1.7 Delimitations 15

1.8 Summary 15

CHAPTER 2. LITERATURE REVIEW 16

2.1 Defining the Scope of Cybercrime 16

2.2 Reviewing the Classification of Cybercrime 17

2.3 Identifying the Scope of Scams 19

2.4 Fraud Motivation Theories 22

2.4.1 Fraud Triangle Theory 22

2.4.2 Fraud Diamond Theory and Further Extensions 23

2.4.3 Towards Mapping Fraud Theory to Cyber-Scammers 25

2.5 Effects of Personality on Fraud Theory 26

2.5.1 The Dark Triad 26

2.5.2 Risk Perception: 28

2.5.3 Spheres of control: 28

2.6 Summary 30

CHAPTER 3. METHODS 31

3.1 Research Design 31

3.2 Sampling Method and Population 32

3.3 Instruments and Scoring 33

3.3.1 Instrument for Fraud Theory 33
3.3.2 Instrument for Dark Triad 33
3.3.3 Instrument for Spheres of Control 34
3.3.4 Instrument for Perceived Risk 34
3.3.5 Instrument to measure Computer Crime Index 34
3.4 Scale Reliability & Validation 35
3.5 Analytical Strategy 35
3.6 Summary 36
CHAPTER 4. RESULTS 37
4.1 Participant Demographics 37
4.2 Data Cleaning 37
4.3 Analytical Strategy 39
4.4 Analysis Results 39
4.5 Results Summary 55
CHAPTER 5. DISCUSSION AND FUTURE WORK 57
5.1 Discussion 57
5.2 Future Work 60
REFERENCES 62
APPENDIX A 71
APPENDIX B. 81

LIST OF TABLES

Table 2.1. A two-level classification of cybercrime. 19

Table 4.1 Demographics for self-reported cyberscamming and non-cyberscamming 38

Table 4.2 Correlation between demographics and variables of interest 40

Table 4.3 Correlation between variables of interest 41

Table 4.4 Analysis Results of Hypothesis 1a.. 43

Table 4.5 Analysis Results of Hypothesis 1b 44

Table 4.6 Analysis Results of Hypothesis 2a.. 45

Table 4.7 Analysis Results of Hypothesis 2b 46

Table 4.8 Analysis Results of Hypothesis 2c.. 47

Table 4.9 Analysis Results of Hypothesis 3a.. 49

Table 4.10 Analysis Results of Hypothesis 3b 50

Table 4.11 Analysis Results of Hypothesis 4a.. 51

Table 4.12 Analysis Results of Hypothesis 4b 52

Table 4.13 Analysis Results of Hypothesis 5 54

Table 4.14 Analysis Results of Hypothesis 6 55

LIST OF FIGURES

Figure 2.1 Fraud Motivation Triangle as proposed by Cressey (1953) 23

Figure 2.2 Fraud Diamond Theory as proposed by Wolfe and Hermanson (2004) 24

Figure 3.1 Hypothesized Model for Fraud Motivation in Cyber-Space 32

Figure 4.1 Factors that affect predilection towards online fraud motivation................................ 42

Figure 5.1 Suggested Model for Future Investigation Based on Linear Regressions................... 61

LIST OF ABBREVIATIONS

AVE	Average Variance Extracted
CCI – R+	Computer Crime Index Revised Plus
CFI	Comparative Fit Index
DOSPERT scale	Domain Specific Risk-Taking Scale
IC3	Internet Crime and Complaint Center
ICT	Information and Communications Technologies
FTC	Federal Trade Commission
FDT	Fraud Diamond Theory
FTT	Fraud Triangle Theory
I-E scale	Internal-External scale
IT	Information Technology
NNFI	Non-normed Fit Index
RMSEA	Root Mean Square Error of Approximation
SRMR	Standardized Root Mean Square Residual
TLI	Tucker-Lewis Index
SEM	Structural Equation Model

ABSTRACT

Cybercrime and online scams are rampant in today’s tech-savvy world. In the past, scammers relied heavily on emails to contact potential victims but today, the presence and widespread usage of social networking platforms and e-commerce businesses has increased the availability of potential victims and made them easily accessible. It could be assumed that since unsuspecting users seek various products or services online - rentals, booking trips, seeking jobs, dating, it makes them easy targets for scammers yet, it is not just individual users who suffer from fraud, but organizations and institutions as well. A study at the Bank of America Merrill Lynch Global Research found that cybercrime costs the global economy up to approximately 540 billion euros annually. There is plenty of research on the technical measures that individuals and organizations may take to prevent themselves from falling prey to fraudsters, however, research trends in the recent past have shifted towards analyzing the human element present in the scenarios. Researchers have argued that identifying the underlying psychological and sociological factors used by fraudsters could help tackle the very root cause of such fraudulent attacks. While there exists some research focusing on the experiences and psychology of victims of these attacks as well as the countermeasures that can be taken to protect them from such attacks, there is little research on the psychology and motivation of those who commit online fraud. This study aims to identify the psychological factors that affect the predilection of scammers to commit online fraud.

CHAPTER 1. INTRODUCTION

This chapter introduces the motivation and objectives of this study and the major research questions that will be investigated. This chapter also defines the scope of the research and addresses the underlying assumptions, limitations and delimitations.

1.1 Problem Statement

Understanding the psychological and sociological techniques used by scammers is an important part of identifying and trying to address the root cause of online fraud attacks. While some research focusing on the experiences and psychology of victims of these attacks as well as the countermeasures that can be taken to protect them from such attacks exists, there is little research on the psychology and motivation of those who commit online fraud. This study aims to uncover motivations of online fraudsters.

The body of research on technical measures to prevent cyber-crime and fraud has made significant advancements in the past few years. These technical measures are being adopted by individuals as well as organizations, yet scams continue to proliferate and cause immense financial losses. The Financial Cost of Fraud 2018 report ("Financial Cost of Fraud 2018 | Crowe UK", 2018) suggests that fraud costs the global economy 3.2 trillion pounds. This is partially because scammers are increasingly using social engineering techniques on their victims to convince individuals and organizations to disclose confidential data or perform some action. They do this by preying on qualities of human nature, such as the assumption that they can trust strangers, or a general belief in courtesy and desire to be helpful to others, or the desire for quick and easy rewards. Therefore, researchers are also shifting towards analyzing the human component in these situations with a lot of research focusing on the techniques used by scammers as well as the personality traits of victims that they exploit (Whitty, 2013; Langenderfer & Shimp, 2001; Kopp, Layton, Sillitoe, & Gondal, 2016; Saad & Norul Huda Sheikh Abdullah, 2018; Fischer, Lea, & Evans, 2013; Abroshan, Devos, & Laermans, 2018).

1.2 Significance

According to the Federal Trade Commission (FTC) report, approximately half of the worlds' population has access to the internet today ("ICT Facts and Figures 2017," n.d.), which puts about 3.5 billion people, most of whom are not cybersecurity experts, on the internet. The internet has brought the world closer by transcending geographical barriers, people from different corners of the world can buy products through e-commerce, as well as socialize and network with strangers with the use of social media and professional networking platforms. The internet has bolstered globalization by giving businesses the ability to operate from remote locations and has also given IT companies the ability to crowdsource. However, this also increases the accessibility of unsuspecting individuals and entities and makes it easier for cybercriminals to prey on them online.

According to FTC ("The top frauds of 2018," 2019), people in the US alone reported losing $1.4 billion to fraud in 2018, a 38% increase from 2017. The most reported types of scams identified by the FTC included imposter scams, debt collection scams and identity theft. They also found that younger people, (43% of people in their 20s) reported losing money to fraud more often than older people, (15% people in their 70s) ("The top frauds of 2018," 2019). However, this could be because older people are less likely report losses because they do not know how to report the fraud, feel embarrassed to report the fraud or simply because of the assumption that law enforcement may not assist them (Dolan 2004). Losses due to romance scams have more than quadrupled in the recent years- from $33 million in 2015 to $143 million in 2018 ("New FTC Data Spotlight Details Big Jump in Losses, Complaints about Romance Scams," 2019). Recently, Google and Facebook paid $23 million and $100 million respectively, to a Lithuanian cybercriminal, who pleaded guilty to wire fraud (Fazzini, 2019). CryptoScamDB, a database that collects reports of scams in the cryptocurrency ecosystem and monitors them, reported 7,131 scams costing up to $9 million a day (Seth, 2019; "Scams | CryptoScamDB," n.d.). These statistics suggest that there is a plethora of scams that exist today that rapidly evolve as scammers are finding innovative and increasingly complex ways to gain financial profits by duping unsuspecting people and businesses. Previous studies have aimed towards strengthening and automating the technical defenses against these attacks, such as the automatic detection of advance fee frauds in emails (Edwards, Peersman & Rashid, 2017), and most of the findings and methods are being adopted and implemented by individuals as well as organizations, yet the scams continue to thrive and cause immense financial losses. Research trends are now shifting towards focusing on the root cause of these attacks – the scammers themselves.

1.3 Scope

This research will investigate the underlying psychological factors that motivate cyber-scammers to commit fraud and how they justify their actions. In the past, researchers have made efforts to identify what motivates fraudsters and how they justify their actions, however, how these theories would apply to cybercriminals who commit fraud remains unclear. This gap in literature is the main focus of this study. Another issue before identifying the motivations of scammers is that there are many different types of scams, and for each of them, conditions change, hence motivations and rationalizations may possibly vary. Chapter 2 provides a description of the types of scams that this study will focus on.

1.4 Research Design

Researchers have made efforts to identify what motivates fraudsters and how they justify their actions with the help of the theoretical framework provided by Cressey – the fraud motivation triangle (1953). This model has been effective in explaining and preventing fraud among insiders in an organization, however, how this theory would apply to scammers in cyberspace remains unclear.

The study will therefore focus on this gap, and aims to investigate the following research questions:

1. How the dark triad traits and spheres of control affect predilection of cyber-scammers towards online fraud motivation?
2. How are cyber-scammers able to justify their actions?

In order to address these questions, I will use the fraud motivation theory which has been used to explain fraud motivation in organizational settings. Fraud motivation theory posits that fraud occurs when the following factors are present – financial pressure that motivates the individual to commit fraud, perceived opportunity that exists with a low risk of being caught, perceived capability of the individual to commit fraud and the willingness to rationalize the act of fraud (Cressey, 1953; Wolfe & Hermanson, 2004). This study will take into consideration the effects of the dark triad of personality (narcissism, psychopathy and machiavellianism), spheres of control (interpersonal control and socio-political control) and risk perception on the fraud motivation theories put forth by Cressey (1953), and Wolfe & Hermanson (2004). In order to examine the effects these different theoretical models have on each other; a set of hypotheses will be developed based on a literature review. These hypotheses will be put together to develop an initial hypothesized model which will attempt to explain how an individual's personality traits and their behavior in interpersonal situations have an effect on motivation to commit fraud in an online setting.

The target population of this study and method of data collection will be further discussed in Chapter 3.

1.5 Assumptions

The assumptions for the study include:

- This study uses Cressey's (1953) fraud motivation theory to analyze what effects certain psychological traits may have on online scammers. The theory put forth by Cressey (1953) was aimed towards understanding the motivation of insiders in an organization to commit fraud. Therefore, our first assumption is that fraud motivation theories alone do not explain the motivations of scammers in cyberspace.
- Another assumption made by this study is that scammers plan their behavior and activities; they consider possible outcomes before deciding if they should commit the act.
- Online scammers have some kind of motivation behind their actions.
- Online scammers make attempts to rationalize their actions.
- Online scammers indulge in similar actions to cybercriminals to facilitate fraud.

1.6 Limitations

The limitations of the study are as follows:

- The study relies on data that has been self-reported so it may be subject to response bias and the limitations of introspective ability and honesty of the participants.
- This study uses scenario-based approach to measure various aspects of fraud, and there were few consequences described, even this helped reduce response fatigue and encourage answers about deceptive practices, a scenario with more severe consequences would complement this study.

1.7 Delimitations

The delimitations of the study are as follows:

- The study will consider the effects of only selected psychological traits; the dark triad and risk perception, on the motivation of cyber scammers.
- The study does not investigate the techniques used by cyber scammers or their effectiveness.
- The study does not provide any suggestions to prevent cyber scams before they occur; the objective is to lay the groundwork towards it.

1.8 Summary

This chapter provided a statement of the problem, its significance, scope and introduced the research questions that will be addressed in this study. It further discussed the assumptions behind the study and its limitations and delimitations.

CHAPTER 2. LITERATURE REVIEW

The impact of cybercrime on individuals and organizations is immense, these crimes vary from identity theft to online pedophilia, cyber-bullying, phishing, cyber-fraud, romance scams, ad fraud, etc. These offences have the potential to cause severe mental strain as well as massive financial losses. In recent years, there has been discussion in the scientific community with regards to the nature of cybercrime and how it should be tackled. Traditional crime was limited by geographical barriers, but cyber-crime is not, owing to the ability of the internet to transcend these barriers. Due to this there is debate over its extent and confusion over its scope. Hence, it is important that before defining the scope of scams that this research considers, we first hash out the definition of cybercrime and identify the different types. From these, we select the crimes that can be categorized as scams and provide a structure to them, so that we can narrow down the scope towards the perpetrators who engage in scams and analyze their motivations.

2.1 Defining the Scope of Cybercrime

The definition of cybercrime is a little nebulous, because of its complex nature. Various research studies and organizations have a series of definitions for cybercrimes, but they differ among researchers and organizations that tackle it. The term cybercrime is often used to describe malicious acts like cyber terrorism and cyber warfare in the information technology domain, and there is not a definition that differentiates cybercrime from these types of threats (Finklea & Theohary, 2012). However, a definition of cybercrime was proposed during the Convention on Cybercrime has become widely accepted, and it states that cybercrime can be defined as – "crimes committed via the internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security." ("Summary to Convention on Cybercrime | Treaty Office", 2001). The accompanying explanatory report during this convention further adds to this definition by stating that cybercrimes are offences in cyberspace that are "either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks, or they consist of the use of such networks or their services to commit traditional offences" ("Explanatory Report to the Convention on Cybercrime | Treaty Office", 2001). In spite of this definition being relatively thorough, when looked at closely, there are still some gaps when it comes to the particular specifics of each feature in the definition (Tsakalidis & Vergidis, 2019). This research places cyber-fraud in a fairly complex domain that has not been differentiated properly and overlaps with other crimes in cyber-space, however, it is out of scope for this review to define cybercrime, the purpose is to merely identify what definition exists in order to map out where fraud in cyber-space lies. Researchers have tried to provide some structure to cyber-crime which we will be exploring in the next sub-section.

2.2 Reviewing the Classification of Cybercrime

Cybercrime is a term that is used to describe a plethora of criminal activities, and these activities are not only complex by their nature but much like everything else in information technology, they also keep evolving and updating and propagate by utilizing the latest technologies. Therefore, it creates a necessity for a classification system that can enable researchers and industry professionals to categorize these different types of cybercrime incidents and match them to their corresponding offences in order to prevent them effectively (Murray, Zeadally, & Flowers, 2012).

The US Department of Justice differentiates cybercrime in three categories depending on: i) if the computer is the medium through which an offence is committed, ii) the target of the offence, and iii) incidental to the offence (Kyl, 1996). Gordon and Ford proposed a simple classification for cybercrime where they categorized cybercrime into two types – Type I: technology crime, as they tend to be almost entirely technical in nature, and Type II: people crime, which tend be people-related at their core (2006). Type I offences are “generally singular, or discrete, events from the perspective of the victim and are facilitated by the introduction of crime-ware programs like keystroke loggers, rootkits, etc. into the users’ computer systems and their introduction can, but may not necessarily, be facilitated by vulnerabilities” (Gordon & Ford, 2006). Type II offences are defined by Gordon and Ford as being “generally facilitated by programs that do not fit under the classification of crimeware, such as conversations taking place using instant messaging clients or file transfer protocols and are generally repeated contacts or events from the users’ perspective” (Gordon & Ford, 2006). Wall proposed a broad classification for cybercrime specifying three different categories (Wall, 2007). The first category is Computer Integrity Crimes, which target the integrity of a computer system and includes activities like denial of service attacks (DoS), hacking, and cracking. The second category is Computer-Assisted Crimes, which use computer systems as merely the medium of committing the crime and includes activities like theft, scams and virtual robberies. The third category defined by Wall is Computer Content Crimes, which includes offensive communication, pornography and violence.

Building further on these classifications, the following more systematic two-level classification for different types of cybercrime offences was introduced as shown in table 1.

i) Type A: Type A offences are the offences against the CIA principle (confidentiality, integrity and availability) of data stored on computer systems and the computer systems themselves. Type A offense consists of acts that involve unauthorized access to and illicit tampering with data, systems or programs. These include a. illegal data acquisition (data espionage), b. Illegal access (hacking, cracking), c. system interference, d. misuse of devices, e. illegal interception, f. data interference,

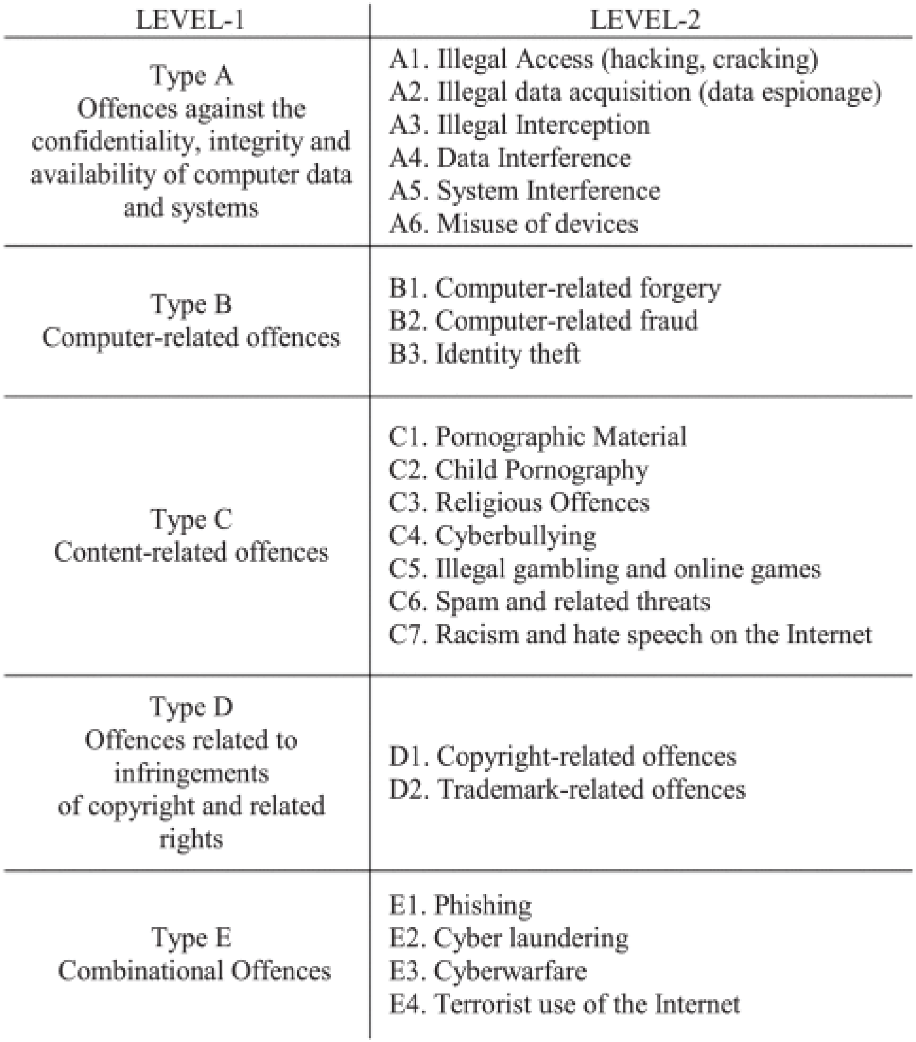
ii) Type B: Type B offense consists of offenses that propagate through the medium of computers and telecommunication systems in order to attack specific legal interests protected by criminal law against traditional means of attacks; this category includes a. identity theft, b. forgery and c. computer-related fraud,

iii) Type C: Type C offense consists of content-related offences where abusive content is facilitated through the medium of computer systems. Offences included in this category are- a. child pornography, b. pornographic material c. cyber-bullying, d. religious offences, e. spam and related threats, f. illegal gambling and online games, g. racism and hate speech on the internet

iv) Type D: Type D offences are related to infringements of copyright and related rights, which include a. copy-right related offences and b. offenses related to trademark

v) Type E: Type E offences are those offences where offenders combine different methodologies and improvise or progress them with new advancements in order to maintain effectiveness, which include a. cyber-laundering, b. phishing c. cyber-warfare and d. cyber-terrorism ("Summary to Convention on Cybercrime | Treaty Office", 2001; Gercke, 2012; Tsakalidis & Vergidis, 2019).

Table 2.1. A two-level classification of cybercrime.
Source: Figure adapted from Tsakalidis & Vergidis (2019).



LEVEL-1	LEVEL-2
Type A Offences against the confidentiality, integrity and availability of computer data and systems	A1. Illegal Access (hacking, cracking) A2. Illegal data acquisition (data espionage) A3. Illegal Interception A4. Data Interference A5. System Interference A6. Misuse of devices
Type B Computer-related offences	B1. Computer-related forgery B2. Computer-related fraud B3. Identity theft
Type C Content-related offences	C1. Pornographic Material C2. Child Pornography C3. Religious Offences C4. Cyberbullying C5. Illegal gambling and online games C6. Spam and related threats C7. Racism and hate speech on the Internet
Type D Offences related to infringements of copyright and related rights	D1. Copyright-related offences D2. Trademark-related offences
Type E Combinational Offences	E1. Phishing E2. Cyber laundering E3. Cyberwarfare E4. Terrorist use of the Internet

2.3 Identifying the Scope of Scams

Based on the classification of cybercrime in section 2.2, the type of scams that we are interested in lie in Type B cybercrime, category B2: Computer-related fraud. In this section, we shall further explore the efforts made to classify scams themselves.

Social media has given fraudsters the ability to hide their true identities and mislead consumers by impersonating trusted sources and making enticing offers. The presence of social media makes it harder to spot scams because they appear to come from trusted sources like friends, family, acquaintances or social communities and brands and they can spread rapidly while propagating content to a wide range of audience. The common scam types propagated with the help of social media include imposter scams, e-commerce scams, clickbait, membership scams, quiz scams, romance scams etc. The Internet Crime Complaint Center (IC3) reported the following scams as of 2019 – auction fraud, parcel courier email scheme, employment/business opportunities, debt elimination, credit card fraud, identity theft, escrow services fraud, investment fraud, lottery fraud, phishing, pyramid schemes, third party receiver of funds, and the classic 419 Nigerian scam among others ("Internet Crime Complaint Center (IC3) | Internet Crime Schemes," n.d.). The long list of never ending and constantly evolving scams creates the need to define how they are classified.

Stabek et. al. proposed a systematic classification of scams after analyzing 250 different scam descriptions for derived static features (Stabek, Brown, & Watters, 2009; Stabek, Watters, & Layton, 2010). Their classification scheme identifies seven different genres of scams –

i. Financial Gain Through Low Level Trickery

This scam genre has the ultimate goal of obtaining money and involves the most basic form trickery. It includes door to door scams that solicit paid services that are never really performed, scams such as psychic and clairvoyant scams, cheque overpayment scams fall under this category.

ii. Financial Gain and Information Gathering Through Developed Story Based Applications

Here, the scammers ultimate goal is to gain money, but they engage in complex planning and providing detail to their pretext. The types of scams that fall under this category are charity scams, Nigerian 419 scams, romance scams and even spam offers.

iii. Participation and Information Gathering through Employment Based Strategies

This genre of scams targets the individual in order to seek participation from them (by seeking a level of victim 'employment') and eventually lead to identity theft or other identity-based crimes.

iv. Financial Gain through Implied Necessary Obligation

These scams require the victim to respond or call-back the perpetrator and aims to make money from the victim by establishing a situation where it may seem necessary. They are different because they do not rely on the internet to propagate, and hence we will not be considering these.

v. Information Gathering through Apparently Authentic Appeal

These scams require a significant amount of knowledge about how systems operate and consists of programs such as spyware and keystroke loggers. They seek information with the intention of causing identity-related crimes like credit card fraud and identity theft.

vi. Financial Gain through Merchant and Customer Based Exploitation

This genre of scams is transaction based and incorporate the roles of both the buyer and the seller leading to offences like bid shielding (manipulating auctions by having other buyers artificially manipulate prices), shill bidding (manipulating auctions by using alternate accounts), payment non-delivery, merchandise non-delivery etc.

vii. Financial Gain and Information Gathering through Marketing Opportunities

The goal here is to make financial gain and sometimes gather information. These scams involve exploitation of investment opportunities, which is the distinctive feature for this genre of scams in order to avoid overlap with the other genres. They include get rich quick scams, Ponzi schemes and pyramid schemes, computer prediction software, 419 advance fee fraud etc.

A detailed description of this classification of scams is provided in Appendix B.

The type of scams this research interested in fall in the categories defined above, with the exception of category iv) Financial gain through implied necessary obligation, as they do not depend on cyber-space to propagate. However, they may be similar in the sense that they require the use of telecommunication and have the ability to transcend geographical barriers.

Now that I have clearly identified the scope of scams in this study; I will proceed to identify the existing literature on what motivates fraudsters and how they rationalize their crimes.

2.4 Fraud Motivation Theories

The motivation to commit fraud has been studied extensively by researchers and a vast body of literature exists in this domain (Thanasak, 2013; Normah & Hesri, 2010; Florenz, 2012; Gbegi & Adebisi, 2013; Sorunke, 2016, Tugas 2012, Coleman, 1987). It is important to identify what the factors that ultimately lead to fraudulent behavior are, and this can be done by making an attempt to understand who the fraudsters are, as well as when and why frauds are committed before making efforts to reduce fraud (Thanasak, 2013). The origins of the Fraud Triangle Theory (FTT) date back to Edwin Sutherland (1939) who came up with the term while-collar crime, and Cressey, who was one of his former students (Dorminey, Fleming, Kranacher, & Riley 2010). Cressey (1953) performed research to identify the factors that lead individuals to indulge in fraud, and the fraud triangle theory he proposed eventually became the foundation of understanding how fraud is committed.

2.4.1 Fraud Triangle Theory

The Fraud Triangle Theory was a perpetrator-centric theory proposed by Cressy in order to explain why the fraudsters commit crime (Cressey, 1953). He argues that three elements must be present in order for fraud to occur:

- Perceived pressure: perpetrator must have a non-shareable financial problem; this financial need is the catalyst that motivates an individual to commit fraud.
- Perceived opportunity: This element consists of the ability to actually commit the fraud, where an opportunity exists that is exploited by the individual; with a low risk of being caught. An opportunity with a low risk of being caught arises when there exist poor conditions within the workplace like weak internal controls. The fewer steps involved in committing the fraud, the more likely it is to occur.
- Rationalization: Here, the individual justifies his behavior, often by seeing themselves as victims of unusual circumstances and develop an explanation to make their illegal actions acceptable.

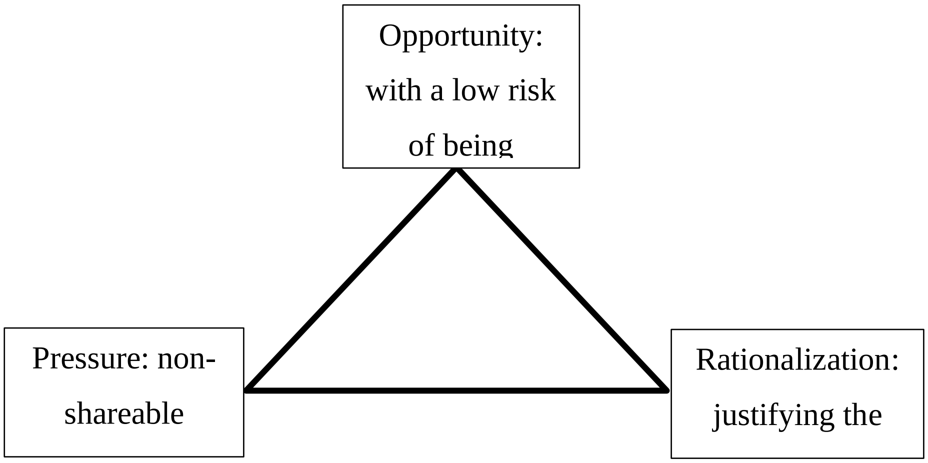

Opportunity: with a low risk of being
Pressure: non-shareable
Rationalization: justifying the

Figure 2.1 Fraud Motivation Triangle as proposed by Cressey (1953)

2.4.2 Fraud Diamond Theory and Further Extensions

Wolfe and Hermanson (2004) proposed a widely accepted extension to the fraud triangle theory by stating that fraud cannot be successfully carried out unless the scammer has a fourth element, capability, i.e., all the abilities and the personal traits in the presence of the other three elements. The perpetrators capability to commit fraud arises from his position in the organization, skills, knowledge or intelligence that he can use to exploit an opportunity, coercion and persuasive skills, ability to manage the stress of committing fraud, ability to lie consistently, and personality traits such as ego or confidence (Wolfe & Hermanson, 2004). The Fraud diamond theory has been examined and discussed and has been identified as an improved version of FTT with the addition of the fourth element (Thanasak, 2013; Normah & Hesri, 2010; Florenz, 2012; Gbegi & Adebisi, 2013).

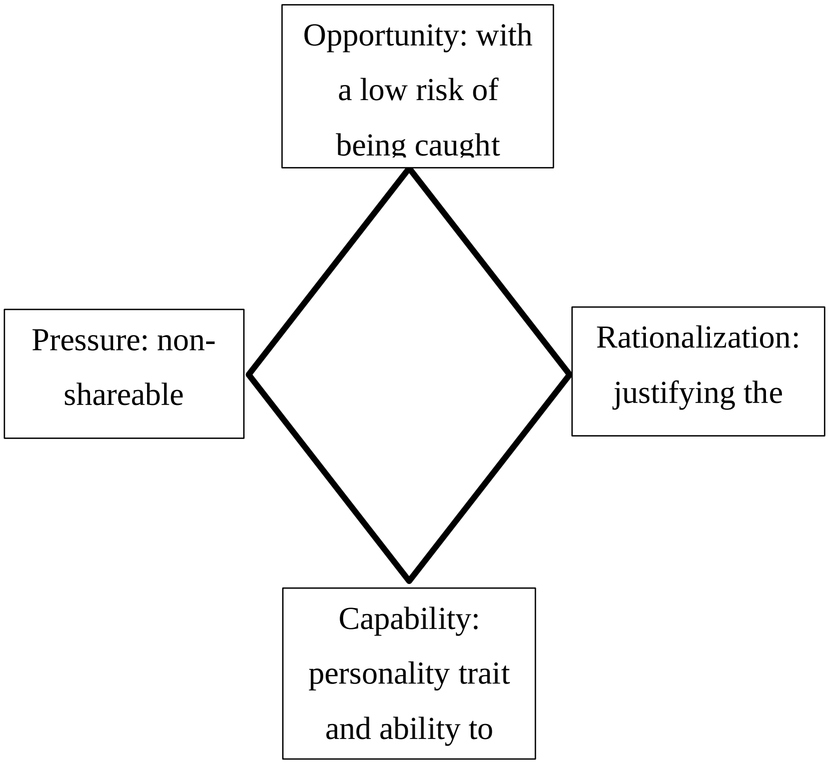

Opportunity: with a low risk of being caught
Pressure: non-shareable
Rationalization: justifying the
Capability: personality trait and ability to

Figure 2.2 Fraud Diamond Theory as proposed by Wolfe and Hermanson (2004)

Further extensions to the FDT have been suggested, many researchers have suggested a fraud pentagon model by adding a fifth dimension. Crowe suggested a 5-dimensional fraud theory in order to extend the FTT by adding fourth and fifth elements of arrogance and competence (Crowe, 2011). Sorunke (2016) theorized a fraud pentagon model with personal ethics being the fifth dimension. He argues that personal ethics have an impact on the perpetrators to commit fraud, and that fraudulent behavior occurs as a result of an individual’s lack of personal integrity that can be attributed to a low level of the individual’s personal ethics (Sorunke, 2016). Another addition to the fraud diamond suggested was the fifth element – external regulation (Tugas 2012). Tugas (2012) argued that fraud cannot occur if regulators were to apply a certain set of strict rules ruthlessly in order to coerce the members of the organization to comply with them. However, there is not a widely accepted fraud pentagon model, neither has it been extensively studied or analyzed.

2.4.3 Towards Mapping Fraud Theory to Cyber-Scammers

The application of the theories of fraud motivation are limited to physical fraud committed in organizational domains unique to societal context of the United States, how these theories explain cyber-crime is still unclear (Czielewski, 2012). Czielewski (2012) suggested that the FTT should be expanded to account for societal factors – social and cultural norms, religious and philosophical religious tradition, political status, socioeconomic conditions and rule of law, to be applicable at an international level. This suggests that researchers would perhaps have a better understanding of the event of fraud if they were to widen the focus of such studies from exclusively the perpetrator alone, to also the environment in which fraud is carried out. This could be a step closer towards explaining the motivations of cyber-scammers as most of them are not limited to one geographical location, have different philosophies and mostly justify their actions due to poor socio-economic conditions (Eichelberger, 2014).

Some attempts have been made to explain the motivations of cyber-scammers. In a recent study, a sales training transcript from the company Alliance for Mature Americans (Alliance) was analyzed to identify how companies motivate their employees to commit fraud (DeLiema, Yon, & Wilber, 2016). Alliance was charged in 1996, for using misrepresentation and deception in order to sell living trusts and annuities worth more than $200 million to adults in California. The study found the following predominant themes: a. indoctrinate sales agents by guaranteeing the product completely, reinforcing ageist stereotypes by stating that old people are simple minded and need to be protected, offering incentives and narratives about power and potential wealth throughout training, encouraging conformity and b. equipping sales agents with persuasive tactics by scapegoating probate attorneys whilst portraying Alliance as protector of the elderly, arousing emotions, building rapport, providing illusion of control, reciprocity, persistence and using distractions when the client started objecting (DeLiema, Yon, & Wilber, 2016). The most remarkable finding of the study was that Alliance actively sanctioned the use of persuasion, distraction, and deception based on stereotypes about the elderly whilst posing as a legitimate business.

Another study suggested that differences between legal systems of countries which ultimately make an investigation and prosecution process difficult, as well as higher per capita income of target countries may also play a role in motivating individuals to commit cyber-fraud ("Economic Impact of Cybercrime Report | McAfee.", 2014). For example, consider the case of Nigeria where socio-economic and political issues have forced some of the citizens to engage in crime as a business and with the advent of internet and social media, scammers migrated to these new platforms (Isacenkova, Thonnard, Costin, Francillon, & Balzarotti, 2014). In a recent article, Eichelberger (2014) interviewed two Nigerian email scammers and made attempts to understand how they rationalize their actions. They justified their actions by scapegoating the government, saying that "they are bad boys" because the government officials, even at the highest-level take peoples' money for personal use instead of investing in the development of the country (Eichelberger, 2014). Researchers have also argued that capitalism and the culture of competition that accompanies it further exacerbates the problem of cyber-fraud; living in a culture that values winning, people feel more pressured to succeed using illegal means (Coleman, 1987). However, these attempts do not provide a proper framework for a theory of motivation to commit fraud in cyber-space. The aim of the study that we will be conducting is to provide a theoretical model to explain the motivation of scammers in cyber-space.

2.5 Effects of Personality on Fraud Theory

2.5.1 The Dark Triad

Since the personality of the fraudsters is an important component of the fraud motivation theory, it is important to examine aspects of personality that may play a role. Researchers have suggested that studies investigating unethical behavior can benefit by examining the influence of dark triad personality traits on such behaviors (Harms & Spain 2015; Wu & Lebreton, 2011).

The term dark triad is used to describe a combination of three psychological personality traits that are socially undesirable– narcissism, machiavellianism and psychopathy (Paulhus & Williams, 2002). These three personality constructs entail a socially destructive character with behavior tendencies such as aggressiveness, grandiosity and manipulation, to varying degrees. When present in combination, these traits are considered to be the predictors of unethical behavior and have been demonstrated affect or facilitate fraudulent behaviors (Johnson, Kuhn, Apostolou, & Hassell, 2012; Jones, 2014; Lee, Ashton, Wiltshire, Bourdage, Visser, & Gallucci, 2013). Individuals that have higher levels of any of the traits which comprise the dark triad are said to be more likely to engage in selfish and unethical behaviors and may also engage in endeavors that are financially risky more often than others (Jones, 2014).

Researchers have noticed that there are certain links between these traits even though they are of different origins. Each of the three dark traits have a strong inverse relationship with modesty and honesty, and this overlap can be traced to callous treatment of others and disagreeableness (Lee & Ashton, 2005; Jakobwitz & Egan, 2006; Jonason, Li, Webster & Schmitt, 2008, Jones & Paulhus, 2011). However, there is evidence that these traits are in fact distinct in other ways, such as the relationship of psychopathy and narcissism with different forms of impulsivity, psychopathy is more compatible with dysfunctional forms of impulsivity whereas narcissism is more compatible with functional forms of impulsivity (Vazire & Funder, 2006; Jones & Paulhus, 2011; Jones & Paulhus, 2010; Vernon, Villani, Vickers & Harris, 2008). Each of the three traits is briefly discussed below.

Machiavellianism is the willingness to use manipulation to act unethically (Christie & Geis, 1970). People who score high in machiavellianism hold a cynical view of others, they perceive others to be gullible and easily fooled and believe that in order to attain goals, manipulation is considered valid and can be useful a method (O’Boyle, Forsyth, Banks, & McDaniel, 2012). Machiavellianism is associated with desire for control and status, amorality and distrust of other (Dahling, Whitaker, Levy, 2009). These individuals are more likely to commit theft, mislead others and cheat (Fehr, Samson, & Paulhus, 1992; Jones & Paulhus 2009; O’Boyle, Forsyth, Banks, & McDaniel, 2012).

Narcissism is characterized by lack of consistent and empathetic childhood interactions and is argued to be the result of a lack of socialization (Kernburg 1975). Researchers have also argued that narcissists have a strong need for validation, they have low self-esteem yet, they emit a sense of grandiosity. They are entitled and self-absorbed and are hence more likely to exploit others. (Emmons 1987, Millon 1990). In short-term interactions, narcissists have been found to gain trust easily; for example during initial encounters or e-commerce transactions, they are generally viewed more favorably as they engage quickly with others and create a positive first impression as compared to subsequent interactions when they are viewed negatively due to their arrogance and impulsivity (Paulhus 1998; Vazire & Funder, 2006; Friedman, Oltmans, Gleason & Turkheimer, 2006). Auditors consider fraud motivation and narcissistic behavior to be significantly positively related to fraud risk assessments (Duchon & Drake 2009, Johnson, Kuhn, Apostolou, & Hassell, 2012, Jones 2014).

Psychopathy is characterized by exhibiting anti-social behaviors stemming from judgments with an elevated importance of self, whilst minimizing others well-being and rights (Levenson 1992). Psychopathic individuals tend to be impulsive, have little concern for other people, lack of guilt and empathy and do not show remorse when their decisions have adverse effects on others (Hare 1991). Therefore, such individuals can demonstrate remorseless and regretless exploitation and manipulation of others (Hare 1991; Lee & Ashton 2005).

Recent studies have made efforts to investigate the effects of the dark triad on fraud theory in the context of fraud and have found that these traits can influence multiple aspects of fraud motivation triangle (Harrison, Summers, & Mennecke, 2018; Gonzalez & Kopp, 2018). In this study, I will be investigating the effects of dark triad in the context of online fraud.

2.5.2 Risk Perception:

Apart from the traits in the dark triad, risk perception of an individual can be one of the factors in whether a potential scammer attempts to scam or not. In an online scenario, scamming can have both potential risks and rewards. According to an earlier study, among various traits, risk tolerance seemed to be the best fraud predictor (Mikulay and Goffin, 1998). In this study, we will consider the effects of risk perception on a scammers motivation to commit fraud.

2.5.3 Spheres of control:

Rotter (1966) conceptualized the Spheres of Control scale (SOC) as internal or external spheres of control measured by the I-E scale. An individual who scores high on internal scale believes that he can control his own life, whereas a high external score indicates a belief that outside factors, which the person cannot influence control their lives (Rotter, 1966). Studies have found that there exists a relation between Machiavellianism and internality/ externality. Some studies have found that Machiavellianism and externality are positively correlated to each other (Christie & Geis, 1970) (Wrightsman & Cook, 1965). While others have found moderate to low correlation with Machiavellianism (Paulhus 1983; Solar & Bruehl, 1971; Russell, 1974; Comer, 1985) when they used diverse groups of participants such as managers, male hockey players, undergraduate students and high school principals. Correlations between Mach scores and internality have been investigated by studies and were found to be negative and of low magnitude across different groups e.g. Italian students (Galli, Nigro & Krampen, 1986), American students (Hunter, Gerbing, & Boster, 1982). These studies have indicated that those who score high in Mach have an external sphere of control; which appears contradictory to the standard that machiavellianism is exhibited by the ability to manipulate others and exert more control over others during interpersonal situations. Paulhus (1983) helped resolve this paradox by further dividing the internality and externality scale and perceived control into the major levels or spheres - personal control, interpersonal control, and socio-political control. According to Paulhus (1983), individuals have different perception of the amount of control they are capable of exerting during their interactions in different domains of the world. The theory posits that there are three different dimensions of perceived control that are conceptually independent, and they are – personal efficacy (PE), interpersonal control (IPC), and socio-political control (SPC). Perceived expectancies of control in personal situations, or the sphere of action that is non-social in nature and does not involve interaction with other humans is measured by personal efficacy and this includes things like personal achievements. The perceived expectancies of control during interpersonal interactions, or behavior when an individual is in a group is determined by interpersonal control and involves influencing others. Socio-political control concerns decisions over the actions of society as a whole. In this study, we will be evaluating the scammers perceived control of the situation i.e. interpersonal control. According to Paulhus (1983), positive correlation between Mach and externality can be attributed to socio-political sphere of perceived control, whereas the interpersonal component comprised the positive relation between machiavellianism and internality. These findings were consistent with certain studies that argue that for Machiavellianism individuals score low on socio-political control because they are cynical about political control and, but they score higher on interpersonal scale because they expect to be in control when interacting with other individuals (Christie and Geis, 1970). Therefore, this study will evaluate the correlation between high Machiavellianism score on the perceived interpersonal control of the online scammers.

2.6 Summary

Based on the research in the domain of cyber-crime presented in this review, it can be concluded that cyber-fraud lies within a fairly complex but moderately defined realm in cyber-space. The research on fraud motivation theory seems to be fairly mature, with the fraud triangle theory being the most widely used theory in regard to understanding fraud motivation in organizational settings. Furthermore, owing to the continuously evolving nature of fraud, theories adding more dimensions to the triangle, the fraud diamond proposed by Wolfe and Hermanson (2004) is an example of a successful attempt at modifying the fraud triangle. However, this review has pointed out that when it comes to understanding the motivations of cyber-fraud perpetrators, there exists a gap, despite a number of research articles that try to understand the same. Hence, the fraud triangle alone cannot not be viewed as the infrastructure to understand and explain the motivation of scammers in cyber-space; this study will make an attempt to investigate the psychological factors that may impact the behavior of online scammers and map them to fraud theory.

CHAPTER 3. METHODS

This chapter will introduce the research design, target population and the method of sampling used in this study. It will then discuss the instruments used to measure the constructs of the theories discussed in the proposed model as well their scoring, validity and reliability.

3.1 Research Design

This study aims to test the following hypotheses:

H1. A. Machiavellianism will have a positive relation with interpersonal control.

H1. B. Machiavellianism will have a negative relation with socio-political control.

H2. A. Perceived risk will be negatively related with Machiavellianism

H2. B. Perceived risk will be negatively related with Psychopathy

H2. C. Perceived risk will be positively related to the scammers perceived opportunity to commit scams.

The literature review conducted in Chapter 2 helped formed the basis of the hypotheses listed above.

A study conducted by Harrison et. al (2018) proposed a model that examined the relationship between the dark triad of personality and fraud motivation theory in online consumer fraud. Their test population comprised of undergraduate students in the management course at a university. This study will test some of their hypotheses as well –

H3. A. Narcissism will be positively related to perceived capabilities of the individual

H3. B. Narcissism will be positively related to motivation of the individual

H4. A. Machiavellianism (Mach) will be negatively related to an individual’s perception of an opportunity to commit an online scam.

H4. B. Mach will be positively related to an individuals’ motivation to commit an online scam.

H5. Psychopathy will be positively related to the willingness to rationalize an act of online fraud.

H6: An individuals' willingness to rationalize an act of fraud will be positively related with their intent to commit fraud.

Based on hypotheses 1a – 6, the model predicting intent to commit fraud was hypothesized and is shown in Figure 3.1.

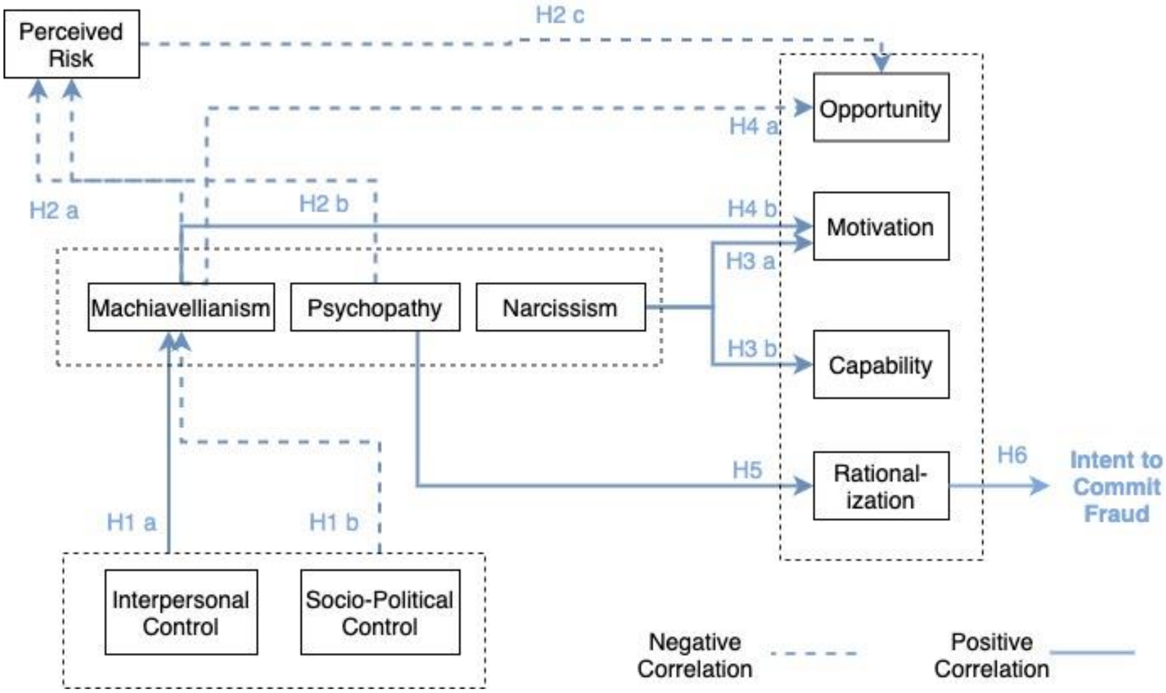


Figure 3.1 Hypothesized Model for Fraud Motivation in Cyber-Space

3.2 Sampling Method and Population

This study aims to recruit 300 participants using Amazon MTurk to sample responses from the general population of internet users residing in the US. The study will collect basic demographics, such as participants' gender, ethnicity and age. Other information that will be collected includes education levels, annual income, computing expertise and time spent online. This study will use the computer crime index survey (Rogers, Seigfried-Spellar, & Bays 2017) to divide the population into cyber scammers and non-cyber scammers.

3.3 Instruments and Scoring

This study will use separate instruments that have been tested for validity and reliability to measure – perceived risk, constructs of the spheres of control, dark triad, and fraud theory. Finally, a computer crime index survey will be used to divide the study populations into cyber scammers and non-cyber scammers. Apart from these questionnaires, the survey will also contain attention check questions to confirm that participants are carefully reading questions and not selecting answers randomly.

3.3.1 Instrument for Fraud Theory

To measure the constructs of Fraud Theory in an online setting, I will use an instrument that provides the user with a scenario and scores them in different constructs of fraud theory using 7-point Likert-scales (Harrison et. al., 2018), the instrument is included in Appendix A1. This instrument measures perceived opportunity, perceived capability, rationalization and motivation using 3 items each. It was developed, validated and tested for reliability by Harrison et.al. (2018) who used it in a similar study to analyze the effects of dark triad on unethical behavior. Harrison et.al. (2018) reported various measures of statistical fit from a confirmatory factor analysis and reported the following values - a χ^2 = 80.204 with degrees of freedom = 48°, a normed χ^2 = 1.671, TLI = 0.980, CFI = 0.985, the SRMR = 0.036, RMSEA = 0.052 and AVE greater than 0.50 for every latent construct indicating validity. They further reported the Cronbach's alpha values for each construct were greater than 0.84, which is well above the recommended value indicating reliability.

3.3.2 Instrument for Dark Triad

In order to measure the dark triad behaviors (narcissism, machiavellianism, and psychopathy) the validated 27-item Dark Triad of Personality D3-Short scale (Paulhus, 2013) will be used and scored using a 5-point Likert-scale (as shown in Appendix A2). Paulhus (2013) reported Cronbach's alphas associated with machiavellianism to be 0.78, narcissism to be 0.77, and psychopathy to be 0.80. The scale intercorrelations varied from 0.20 to 0.37 indicating high internal consistency and the scale has been used by other studies as well (Giammarco, Atkinson, Baughman, Veselka, & Vernon, 2013).

3.3.3 Instrument for Spheres of Control

In order to measure the constructs of spheres of control, the 30-item scale proposed by Paulhus (1990) will be used (on 7-point Likert-scales). The full instrument is included in the Appendix A5. The scale measures personal efficacy, interpersonal control, and socio-political control, and was found by Paulhus et. al (1990) to have reliable alpha scores for each of the constructs, except personal efficacy which showed relatively low levels of reliability due to internal inconsistencies. However, this study is mainly interested in interpersonal control and socio-political control and hence the relatively low levels of reliability in the case of personal efficacy as indicated by Paulhus et. al. (1990) can be ignored.

3.3.4 Instrument for Perceived Risk

In order to measure perceived risk, the validated 30-item DOSPERT scale (Blais & Weber, 2006) will be used and scored using a 7-point Likert-scale (as shown in Appendix A6). DOSPERT is a psychometric scale that assess perceived risk in five domains: financial decisions, health, recreational, ethical and social decisions. This study is more interested in the domains of ethical and financial decisions.

Blais & Weber (2006) reported Cronbach's alphas associated with the scale ranging from 0.74 to 0.83, and scale intercorrelations varied from 0.19 to 0.66 which indicate high internal consistency and the scale has been used by other studies as well (Wilke, Sherman, Curdt, Mondal, Fitzgerald & Kruger, 2014; Foster, Shenesey, & Goff, 2009).

3.3.5 Instrument to measure Computer Crime Index

The Computer crime index – revised plus (CCI – R+) survey measures different types of self-reported computer misbehavior. The questionnaire includes items that target various acts that a cyber-scammer might indulge in ranging from guessing passwords to impersonation without permission to conduct online transactions (e.g., writing a virus, obtaining unauthorized access to a computer or account, stealing credit card information with the intent to sell it to others, obtaining passwords etc.). This survey has been employed by other studies and have reported the Cronbach's alpha value as 0.71 (Withers, 2019). Based on the participants response to items on this questionnaire, they will be classified as either cyber-scammers or non-cyber scammers, i.e., if an individual indulged in any of the computer-deviant behaviors in the questionnaire, they will be classified as cyber-scammers, and if they reported that they never indulged in these behaviors, they will be classified as non-cyber scammers.

3.4 Scale Reliability & Validation

All the instruments used in this study have been validated and tested for reliability as discussed in the section above.

3.5 Analytical Strategy

Preliminary analysis will consist of going through the dataset and deleting incomplete responses in the dataset.

Prior to any analyses, one-tailed statistical significance will be set at alpha level of .05. This will be followed by normality, linearity and homogeneity of variance tests. After the data has passed these tests, a zero-order correlation analysis between demographic variables (age, sex, education level, annual income, computer expertise, time spent online per day on an average) and variables of interest (motivation, perceived opportunity, perceived capability, willingness to rationalize fraud and intent to commit fraud) will be conducted. A zero-order correlation analysis between dark triad elements (machiavellianism, psychopathy, narcissism), constructs of spheres of control (personal control, interpersonal control, socio-political control), risk perception, fraud diamond (motivation, perceived opportunity, perceived capability, willingness to rationalize fraud) and intent to commit fraud will also be conducted. This will be followed by a partial correlation analysis between certain variables while controlling for variables that they have a correlation with. Finally, in order to test the hypotheses and validate the structure of the model proposed model fit statistics will be analyzed with the help of structural equation model using R. The method of estimation that will be used to estimate parameters of the model will be maximum-likelihood estimation.

3.6 Summary

This chapter discussed the experiment setup, identified the study population and procedure for recruitment of participants and presented the instruments and their scoring – for Fraud Theory, the instrument proposed by Harrison et. al., (2018); for the dark triad, the instrument proposed by Paulhus (2013); for spheres of control, the instrument proposed by Paulhus (1990); and for perceived risk the DOSPERT scale (Blais & Weber, 2006). It further discussed the analytical strategies that will be employed.

CHAPTER 4. RESULTS

This chapter will discuss the results of this research. Results are divided into the following sections: demographics of the participants, procedure for data cleaning, and path analysis followed by a summary of this chapter.

4.1 Participant Demographics

This study recruited 318 participants using Amazon MTurk to sample responses from the general population of internet users residing in the US. The participants consist of a group of ethnically diverse people (e.g., Asians, African Americans, Non-Hispanic/White, Hispanic/Latino, Multiracial, Native Americans), of which 185 are males and 103 are females who were of ages 18-70 years. The participants are from different educational backgrounds, with education levels ranging from 12 years of high school to individuals with a doctoral degree. They also had varied annual incomes ranging from below $20,000 a year to above $90,000 a year, and varied computing expertise, from no experience with computers to computer experts.

4.2 Data Cleaning

The dataset initially contained responses from 318 participants, however responses from 28 participants were discarded either because they did not consent to have their data used for the purpose of this research or due to inaccurate responses on attention check questions. This was done to ensure quality results and resulted in the study using responses from 290 participants.

Table 4.1 Demographics for self-reported cyberscamming and non-cyberscamming

Variable		Non-CS	CS	Total
		(*n* = 167)	(*n* = 123)	(*N* = 290)
Sex	Male	64	121	185
	Female	58	45	103
Age (yrs)	18-25	11	22	33
	26-35	47	88	135
	36-45	33	28	61
	46-55	12	18	30
	56-65	14	09	23
	66 and over	06	02	08
Ethnicity	African American	14	26	40
	Asian	9	11	20
	Caucasian	89	99	188
	Hispanic	07	18	25
	Other	04	13	17
Income (in dollars/year)	up to 20,000	26	22	48
	20,000 - 45,000	43	53	96
	45,000 - 70,000	21	57	78
	70,000 - 90,000	15	24	39
	above 90,000	15	09	24
Education	High School	45	37	82
	Bachelor’s Degree	57	88	145
	Diploma	03	03	06
	Master’s Degree	15	35	50
	Doctoral Degree	03	04	07
Computer Expertise	None	00	04	04
	Novice	00	13	13
	Basic Experience	46	61	107
	Above average	52	73	125
	Expert	25	16	41
Time spent online (per day)	less than 1 hour	02	01	03
	2 - 4 hours	36	101	137
	5 - 6 hours	24	29	53
	over 6 hours	61	36	97

Note. Non-CS = Non-cyberscammer; CS = cyberscammer.

4.3 Analytical Strategy

Prior to any of the analyses, the one-tailed significance was set at alpha level of .05. The author first conducted a zero-order correlation analysis between variables of interest (interpersonal control, socio-political control, machiavellianism, narcissism, psychopathy, perceived risk, opportunity, motivation, capability, willingness to rationalize and intent) with the demographic variables (age, sex, annual income, computer expertise, etc.) to identify if any of these variables should be controlled for. Next, the author conducted a zero-order correlation analysis between the variables of interest for each hypothesis, this was followed by a partial correlation analysis between variables of interest while controlling for other variables that had significant correlations with the variables of interest. A linear regression was also conducted for each hypothesis to predict the dependent variables and examine the amount of variance explained by each variable. The method of entry was chosen as stepwise because the author is not sure about what variables belong in the model. Finally, in order to test the proposed model, the author performed a path analysis using structural equation model based on the hypotheses, the results of which are discussed within each hypothesis.

4.4 Analysis Results

A zero-order correlation analysis revealed that there was a significant correlation between sex and willingness to rationalize fraud (r_s = -.17, p < .01), indicating that males were more likely to be willing to rationalize fraud than females. There was also a statistically significant correlation between age and willingness to rationalize fraud (r_s = -.17, p < .01), as well as age and intent to commit fraud (r_s = -.13, p < .05), i.e., younger age groups were more likely to be willing to rationalize fraud and also more likely to have the intent to commit fraud than older age groups. Individuals with higher education level were more likely to be willing to rationalize fraud and have the intent to commit fraud (r_s = .25, p < .01; r_s = .12, p < .05) than individuals with lower education levels. Individuals who spent less time online on an average per day were less likely to be willing to rationalize fraud (r_s = -.31, p < .01), and less likely to have the intent to commit fraud (r_s = -.19, p < .01), than individuals who spent more time online. There was a statistically significant correlation between an individuals' income and their willingness to rationalize fraud (r_s = .12, p < .05), indicating that individuals with lower annual income were more likely to be willing to justify an act of fraud than an individual with higher annual income. These results are summarized in Table 4.2.

Table 4.2 Correlation between demographics and variables of interest

Variable	Opp	Mot	Cap	Rat	Int	Non vs. CS
Sex	0.35	0.00	-0.05	-0.17**	-0.09	-0.21**
Age	-0.02	-0.08	-0.06	-0.17**	-0.13*	-0.18**
Education	0.08	0.08	0.08	0.25**	0.12*	0.14**
Online Time (hours a day)	-0.01	0.07	-0.09	-0.31**	-0.19**	-0.29**
Computer Expertise	-0.07	0.00	-0.01	-0.07	-0.05	-0.19**
Income	0.05	0.07	0.09	0.12*	0.05	0.02

One-tailed, listwise correlation
**. Correlation is significant at the .01 level
*. Correlation is significant at the .05 level
Note. Opp = Opportunity; Mot = Motivation; Cap = Capability; Rat = Rationalization;
Int = Intention; Non vs. CS = non-cyber scammer vs cyber scammer

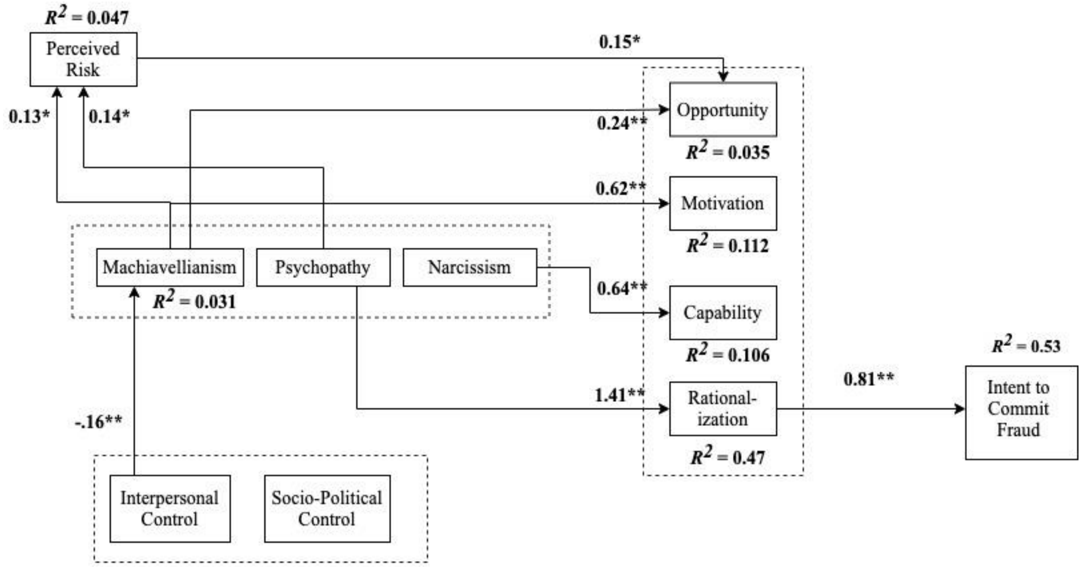
A correlation analysis was done between the variables of interest; interpersonal control, socio-political control, machiavellianism, narcissism, psychopathy, risk perception, perceived opportunity, motivation, perceived capability, willingness to rationalize fraud and intent to commit fraud. All intercorrelations were below |.90| suggesting that there were no issues with multicollinearity as shown in Table 4.3.

Table 4.3 Correlation between variables of interest

Variable	IPC	SPC	Mach	Narc	Psych	RP	Opp	Mot	Cap	Rat
IPC										
SPC	.44**									
Mach	-.15**	-.03								
Narc	.20**	.17**	.54**							
Psych	-.29**	.00	.62**	.61**						
RP	-.12**	.01	.26**	.10*	.25**					
Opp	-.04	-.03	.38**	.15**	.28**	.20**				
Mot	-.14*	.00	.42**	.14**	.27**	.07	.58**			
Cap	.04	.14*	.49**	.34**	.41**	.16**	.64**	.48**		
Rat	-.13*	.10	.55**	.54**	.69**	.26**	.33**	.25**	.52**	
Int	-.07	.09	.44**	.37**	.51**	.32**	.35**	.24**	.44**	.74**

One-tailed, listwise correlation
**. Correlation is significant at the .01 level
*. Correlation is significant at the .05 level
Note. IPC = Interpersonal Sphere of control; SPC = Socio-political sphere of control;
Mach = Machiavellianism; Narc = Narcissism; Psych = Psychopathy; RP = Risk Perception;
Opp = Opportunity; Mot = Motivation; Cap = Capability; Rat = Rationalization; Int = Intention

In order to test the model, a path analysis was done. Results of the structural equation model indicated that the model had a Chi-square value of 258.11 with 32 degrees of freedom. The normed Chi-square value is 7.84 which is above the recommended value of 3.00 and does not provide evidence for a good fit (Hair et. al, 2010). The statistical fit measure test values were as follows – CFI value of 0.74, NNFI/TLI of 0.60, the RMSEA value of 0.17 and SRMR value of 0.19 also do not provide evidence of a good fit (Bentler, 1992; Hu & Bentler, 1999; MacCallum et. al., 1996). The resulting model is shown in figure 4.1.



**. Significant at the .01 level
*. Significant at the .05 level

Figure 4.1 Factors that affect predilection towards online fraud motivation

Hypothesis 1a: Machiavellianism will have a positive correlation with interpersonal control.

The zero-order correlation analysis between Machiavellianism and interpersonal control found that individuals who scored higher on Machiavellianism (r_s = -.15, *p* = .006) scored lower on interpersonal control subscale, indicating that people who have higher levels of Machiavellianism tend to have lower perception of control in interpersonal interactions than people with lower levels of Machiavellianism.

A stepwise linear regression analysis was conducted with interpersonal control as the independent variable and machiavellianism as the dependent variable. The model generated determined that an individuals' perception of control in interpersonal situations was significantly predictive of machiavellianism (*t* = -2.55, *p* = .01). The value of R_2 for this model was .023, which tells us that perception of control in interpersonal situations alone can account for 2.3% of the variation in machiavellianism. The *F*-statistic for this model (*F*(1,284) = 6.53, *p* = .01) suggested that the model significantly improves our ability to predict machiavellianism and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for interpersonal control on machiavellianism level of the individual = -0.16 was significant, *t*-value = -2.75 *p* = 0.01. While the effect of interpersonal control on machiavellianism was significant, the regression results contradict the hypothesis 1a, i.e., machiavellianism is in fact negatively related to perceived interpersonal control of an individual. The results of the hypothesis are summarized in Table 4.4.

Table 4.4 Analysis Results of Hypothesis 1a

Zero Order Correlation	r_2	-0.15**
Linear Regression	R_2	0.02
	t-statistic	-2.55**
	F-statistic	*F* (1,284) = 6.53**
Structural Equation Model	Regression Weight	-0.16**
	t-statistic	-2.75

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation; Stepwise Linear Regression

Hypothesis 1b: Machiavellianism will have a negative correlation with socio-political control.

The zero-order correlation analysis between Machiavellianism and socio-political control revealed that there was no statistically significant correlation between socio-political control and Machiavellianism (r_s = -.03, *p* = .37). This means that those individuals' perception of control in socio-political situations do not have any effect on their levels of machiavellianism.

A stepwise linear regression analysis was conducted with socio-political control added as an independent variable to the previous model along with interpersonal control, the dependent variable remained machiavellianism. The model generated determined that an individuals' perception of control in sociopolitical situations was not significantly predictive of machiavellianism (*t* = .73, *p* = .47). The value of R_2 for this model was .025, which tells us that perception of control in interpersonal situations alone can account for 2.5% of the variation in machiavellianism. The *F*-statistic for this model (*F*(1,277) = 6.99, *p* = .01) suggested that the model significantly improves our ability to predict machiavellianism and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for sociopolitical control on machiavellianism level of the individual = 0.04 was not significant, *t*-value = 0.57, *p* = 0.57. The effect of socio-political control on machiavellianism was not significant, hence the regression results contradict the hypothesis 1b, i.e., there is no evidence that machiavellianism is positively related to perception of socio-political control of an individual. The results of the hypothesis analysis are summarized in Table 4.5.

Table 4.5 Analysis Results of Hypothesis 1b

Zero Order Correlation	r_2	-0.03
Linear Regression	R_2	0.025
	t-statistic	0.07
	F-statistic	*F* (1,277) = 6.99**
Structural Equation Model	Regression Weight	0.04
	t-statistic	0.57

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 2a: Perceived risk will be negatively correlated with Machiavellianism

The zero-order correlation analysis between perceived risk and Machiavellianism indicated that individuals who scored higher on Machiavellianism (r_s = .26, *p* < .001) scored higher on perceived risk, indicating that individuals with higher levels of Machiavellianism tend to perceive higher risk based on their actions in ethical, financial and social situations than individuals with lower levels of Machiavellianism.

A stepwise linear regression analysis was conducted using machiavellianism as the independent variable and perceived risk as the dependent variable. The model generated determined that machiavellianism in individuals was significantly predictive of perceived risk in an individual (t = 4.41, p < .001). The value of R_2 for this model tells us that machiavellianism can account for 6.5% of the variation in perceived risk. The F-statistic for this model (F(1,280) = 19.41, p < .001) suggested that model significantly improves our ability to predict perceived risk and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and independent errors (Durbin-Watson value = 1.91), and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for machiavellianism on perceived risk of the individual = 0.13 was significant, t-value = 2.08, p = 0.04. While the effect of machiavellianism on perceived risk was significant, the regression results contradict the hypothesis 2a, i.e., perceived risk is positively related to machiavellianism in an individual. The results of the hypothesis analysis are summarized in Table 4.6.

Table 4.6 Analysis Results of Hypothesis 2a

Zero Order Correlation	r_2	0.26**
Linear Regression	R_2	0.06
	t-statistic	4.41**
	F-statistic	F (1,280) = 19.41**
Structural Equation Model	Regression Weight	0.13*
	t-statistic	2.08*

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 2b: Perceived risk will be negatively correlated with Psychopathy

The zero-order correlation analysis between perceived risk and psychopathy indicated that individuals who scored higher on psychopathy (r_s = .25, p < .001) scored higher on perceived risk, indicating that individuals with higher levels of psychopathy tend to perceive higher risk based on their actions in ethical, financial and social situations than individuals with lower levels of psychopathy.

A stepwise linear regression analysis was conducted by adding psychopathy as an independent variable along with machiavellianism to the previous model, the dependent variable remained perceived risk. The model generated determined that psychopathy in individuals was significantly predictive of perceived risk in an individual (*t* = 2.04, *p* = .04). The value of R_2 for this model tells us that machiavellianism can account for 7.9% of the variation in perceived risk. However, the *F*-statistic for this model (*F* (1,281) = 11.89, *p* < .001) suggested that model does not significantly improve our ability to predict perceived risk when psychopathy is added.

The structural equation model regression coefficient for psychopathy level on perceived risk of the individual = 0.14 was significant, *t*-value = 2.17, *p* = 0.03. While the effect of psychopathy on perceived risk was significant, the regression results contradict the hypothesis 2b, i.e., perceived risk is positively related to psychopathy levels in an individual. The results of the hypothesis analysis are summarized in Table 4.7.

Table 4.7 Analysis Results of Hypothesis 2b

Zero Order Correlation	r_2	0.25**
Linear Regression	R_2	0.08
	t-statistic	2.04**
	F-statistic	*F* (1,281) = 12.89**
Structural Equation Model	Regression Weight	0.14*
	t-statistic	2.17*

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 2c: Perceived risk will be positively related to the scammers perceived opportunity to commit scams.

The zero-order correlation analysis between perceived risk and perceived opportunity indicated that individuals who scored higher on perceived opportunity (r_s = .20, *p* < .001) also scored higher on perceived risk, indicating that individuals who perceive a higher opportunity to commit fraud, also tend to perceive higher risk based on their actions in ethical, financial and social situations than individuals who perceive lower opportunity to commit fraud.

A stepwise linear regression analysis was conducted with perceived risk as the independent variable and perceived opportunity as the dependent variable. The model generated determined that an individuals' perceived risk was significantly predictive of perceived opportunity to commit online fraud (t = 3.38, p = .001). The value of R_2 for this model tells us that perceived risk can account for 4% of the variation in perceived opportunity to commit fraud online. The F-statistic for this model (F(1,281) = 11.43, p = .001) suggested that model significantly improves our ability to predict perceived opportunity and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and independent errors (Durbin-Watson value = 1.70), and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for perceived risk on perceived opportunity of the individual to commit scam = 0.15 was significant, t-value = 1.98, p < 0.05. The effect of perceived risk on perceived opportunity was significant, the regression results support the hypothesis 2c, i.e., perceived risk is in fact positively related to perceived opportunity to commit scams in an individual. The results of the hypothesis analysis are summarized in Table 4.8.

Table 4.8 Analysis Results of Hypothesis 2c

Zero Order Correlation	r_2	0.20**
Linear Regression	R_2	0.04
	t-statistic	3.38**
	F-statistic	F (1,281) = 11.43**
Structural Equation Model	Regression Weight	0.15*
	t-statistic	1.98*

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 3a: Narcissism will be positively related to perceived capabilities of the individual

The zero-order correlation analysis between narcissism and perceived capability indicated that individuals who scored higher on narcissism (r_s = .34, p < .001) also scored higher on perceived capability, indicating that individuals with higher levels of narcissism tend to have a higher perception of their capability to commit fraud than individuals with lower levels of narcissism. However, a partial correlation analysis revealed that there was no statistically significant relationship between narcissism and perceived capability ($r_{ae.bcd}$ = .08, p = .16) when controlling for machiavellianism and psychopathy. However, partial correlation analysis revealed that there was no statistically significant relationship between narcissism and perceived capability ($r_{ae.bcd}$ = .08, p = .16), when controlling for psychopathy and machiavellianism.

A stepwise linear regression analysis was conducted with narcissism as the independent variable and perceived capabilities as the dependent variable. The model generated determined that narcissism in individuals was significantly predictive of perceived capabilities to commit online fraud (t = 6.23, p < .001). The value of R_2 for this model tells us that narcissism can account for 12% of the variation in perceived capabilities of an individual. The F-statistic for this model (F(1,288) = 38.61, p < .001) suggested that model significantly improves our ability to predict perceived capabilities and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and independent errors (Durbin-Watson value = 1.87), and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for narcissism on perceived capabilities of the individual = 0.64 was significant, t-value = 5.74; p < 0.001. This result supports hypothesis 3a, i.e., narcissism is positively related to an individual's perceived capability to commit fraud. The results of the hypothesis analysis are summarized in Table 4.9.

Table 4.9 Analysis Results of Hypothesis 3a

Zero Order Correlation	r_2	0.34**
Linear Regression	R_2	0.12
	t-statistic	6.23**
	F-statistic	*F* (1,288) = 38.61**
Structural Equation Model	Regression Weight	0.64**
	t-statistic	5.74**

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 3b: Narcissism will be positively related to motivation of the individual to commit online scam

The zero-order correlation analysis between narcissism and motivation to commit fraud indicated that individuals who scored higher on narcissism (r_s = .34, p < .001) also scored higher on motivation, indicating that individuals with higher levels of narcissism tend to have a higher motivation to commit fraud than individuals with lower levels of narcissism. However, partial correlation analysis revealed that there was no statistically significant relationship between narcissism and motivation ($r_{ac.bde}$ = -.07, p = .18), when controlling for psychopathy and machiavellianism.

A stepwise linear regression analysis was conducted with narcissism as the independent variable and motivation to commit online fraud as the dependent variable. The model generated determined that narcissism in individuals was significantly predictive of motivation to commit online fraud (t = 2.45, p = .02). The value of R_2 for this model tells us that narcissism can account for 2% of the variation in motivation of an individual to commit online fraud. The *F*-statistic for this model (*F*(1,288) = 5.99, p = .02) suggested that model significantly improves our ability to predict motivation and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and independent errors (Durbin-Watson value = 1.71), and the assumption of homoscedasticity as well.

However, the structural equation model regression coefficient for narcissism on motivation of the individual to commit scams = -0.12 was not significant, *t*-value = -0.93; *p* = 0.35. This result contradicts hypothesis 3a, i.e., there is no evidence that narcissism is positively related to an individual's perceived capability to commit fraud. The results of the hypothesis analysis are summarized in Table 4.10.

Table 4.10 Analysis Results of Hypothesis 3b

Zero Order Correlation	r_2	0.34**
Linear Regression	R_2	0.02
	t-statistic	2.45*
	F-statistic	*F* (1,288) = 5.99*
Structural Equation Model	Regression Weight	-0.12
	t-statistic	-0.93

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 4a: Machiavellianism will be negatively related to an individual's perception of an opportunity to commit an online scam.

The zero-order correlation analysis between Machiavellianism and the individuals perception of an opportunity to commit fraud indicated that individuals who scored higher on Machiavellianism (r_s = .38, *p* < .001) also scored higher on perceived opportunity, indicating that individuals with higher levels of Machiavellianism tend to have a higher perception of opportunity to commit fraud than individuals with lower levels of Machiavellianism. A partial correlation analysis revealed that there was a statistically significant relationship between machiavellianism and perceived opportunity ($r_{ad.bcde}$ = .25, *p* = .001) when controlling for psychopathy and narcissism.

A stepwise linear regression analysis was conducted with machiavellianism as the independent variable and perceived opportunity as the dependent variable. The model generated determined that machiavellianism in individuals was significantly predictive of perceived opportunity to commit online fraud (*t* = 7.06, *p* < .001). The value of R_2 for this model tells us that machiavellianism can account for 14.8% of the variation in perceived opportunity to commit fraud.

The *F*-statistic for this model (*F*(1,289) = 49.88, *p* < .001) suggested that model significantly improves our ability to predict perceived opportunity and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and independent errors (Durbin-Watson value = 1.81), and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for machiavellianism on perceived opportunity to commit scam = 0.24 was significant, *t*-value = 2.53; *p* = 0.01. This result contradicts hypothesis 4a, i.e., machiavellianism is positively related to an individuals' perceived opportunity to commit fraud. The results of the hypothesis analysis are summarized in Table 4.11.

Table 4.11 Analysis Results of Hypothesis 4a

Zero Order Correlation	r_2		0.38**
Linear Regression	R_2		0.15
	t-statistic		7.06*
	F-statistic	*F* (1,289) = 49.88**	
Structural Equation Model	Regression Weight		0.24**
	t-statistic		2.53**

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 4b: Machiavellianism will be positively related to an individuals' motivation to commit an online scam.

The zero-order correlation analysis between Machiavellianism and motivation to commit fraud indicated that individuals who scored higher on Machiavellianism (r_s = .42, *p* < .001) also scored higher on motivation to commit fraud, indicating that individuals with higher levels of Machiavellianism tend to have a higher motivation to commit fraud than individuals with lower levels of Machiavellianism. A partial correlation analysis revealed that there was a statistically significant relationship between machiavellianism and motivation ($r_{ac.bde}$ = .30, *p* < .001) while controlling for narcissism and psychopathy.

A stepwise linear regression analysis was conducted with machiavellianism added as the independent variable to the model in hypothesis 3b, i.e., along with narcissism as a dependent variable and perceived opportunity as the dependent variable. The model generated determined that machiavellianism in individuals was significantly predictive of perceived opportunity to commit online fraud (t = 7.79, p < .001). The value of R_2 for this model tells us that machiavellianism can account for 17.5% of the variation in perceived opportunity to commit fraud. The F-statistic for this model (F(1,288) = 60.71, p < .001) suggested that model with machiavellianism as a predictor of motivation to commit fraud significantly improves our ability to predict perceived motivation instead of the model with narcissism (F(1,288) = 5.99, p = .02) as a predictor of motivation. The data met the assumption of normality and independent errors (Durbin-Watson value = 1.81), and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for machiavellianism on motivation of the individual to commit scam = 0.62 was significant, t-value = 4.24; p < 0.001. This result supports hypothesis 4b, i.e., machiavellianism is positively related to an individual's motivation to commit fraud. The results of the hypothesis analysis are summarized in Table 4.12.

Table 4.12 Analysis Results of Hypothesis 4b

Zero Order Correlation	r_2	0.42**
Linear Regression	R_2	0.17
	t-statistic	7.79**
	F-statistic	F (1,288) = 60.71**
Structural Equation Model	Regression Weight	0.62**
	t-statistic	4.24**

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 5: Psychopathy will be positively related to the willingness to rationalize an act of online fraud.

The zero-order correlation analysis between psychopathy and rationalizing an act of fraud indicated that individuals who scored higher on psychopathy (r_s = .42, p < .001) also scored higher on rationalization of fraud, indicating that individuals with higher levels of psychopathy tend to have a higher willingness to rationalize fraud than individuals with lower levels of psychopathy. A partial correlation analysis revealed that there was a statistically significant relationship between psychopathy and willingness to rationalize online fraud ($r_{ab.cde}$ = .41, p < .001) when controlling for machiavellianism and narcissism.

A stepwise linear regression analysis was conducted with psychopathy as the independent variable and willingness to rationalize online fraud as the dependent variable. The model generated determined that psychopathy in individuals was significantly predictive of willingness to rationalize online fraud (t = 16.28, p < .001). The value of R_2 for this model tells us that psychopathy can account for 48% of the variation in willingness to rationalize fraud. The F-statistic for this model (F(1,287) = 264.99, p < .001) suggested that model significantly improves our ability to predict willingness to rationalize fraud and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for psychopathy on willingness to rationalize an act of online fraud = 1.41 was significant (t = 19.11; p < 0.001). This result supports hypothesis 5, i.e., psychopathy is positively related to an individual’s willingness to rationalize an act of fraud. The R_2 value at 0.47 suggests that psychopathy alone can account for 47% of variance in willingness to rationalize an act of fraud. The results of the hypothesis analysis are summarized in Table 4.13.

Table 4.13 Analysis Results of Hypothesis 5

Zero Order Correlation	r_2		0.41**
Linear Regression	R_2		0.48
	t-statistic		16.28**
	F-statistic	*F* (1,287) = 264.99**	
Structural Equation Model	Regression Weight		1.41**
	t-statistic		19.11**

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

Hypothesis 6: An individuals' willingness to rationalize an act of fraud will be positively related with their intent to commit fraud

The zero-order correlation analysis between willingness to rationalize an act of fraud and intent to commit fraud indicated that individuals who scored higher on willingness to rationalize fraud (r_s = .74, *p* < .001) also scored higher on intent to commit fraud, indicating that individuals with higher willingness to rationalize fraud tend to have a intent to commit fraud than individuals with lower willingness to rationalize fraud. A partial correlation analysis revealed that there was a statistically significant relationship between willingness to rationalize online fraud and intent to commit fraud ($r_{ab.cde}$ = .66, *p* < .001) when controlling for sex, age, education level, time spent online, motivation, perceived opportunity and perceived capability.

A stepwise linear regression analysis was conducted with willingness to rationalize as the independent variable and intent to commit online fraud as the dependent variable. The model generated determined that willingness to rationalize online fraud was significantly predictive of intent to commit online fraud (*t* = 18.56, *p* < .001). The value of R_2 for this model tells us that psychopathy can account for 54.5% of the variation in willingness to rationalize fraud. The *F*-statistic for this model (*F*(1,287) = 653.89, *p* < .001) suggested that model significantly improves our ability to predict intent to commit fraud and improvements due to fitting regression model are much greater than the inaccuracies within the model. The data met the assumption of normality and the assumption of homoscedasticity as well.

The structural equation model regression coefficient for willingness to rationalize an act of online fraud on intent to commit fraud = 0.81 was significant, *t*-value = 17.34; $p < 0.001$. This result supports hypothesis 6, i.e., willingness to rationalize fraud is positively related to an individuals' intent to commit an act of fraud. The R_2 value at 0.53 suggests that willingness to rationalize alone can account for 53% of variance in intent to commit fraud. The results of the hypothesis analysis are summarized in Table 4.14.

Table 4.14 Analysis Results of Hypothesis 6

Zero Order Correlation	r_2		0.74**
Linear Regression	R_2		0.54
	t-statistic		18.56**
	F-statistic	*F* (1,287) = 653.89**	
Structural Equation Model	Regression Weight		0.81**
	t-statistic		17.34**

**. Significant at the .01 level
*. Significant at the .05 level
One-tailed, listwise correlation;
Stepwise Linear Regression

4.5 Results Summary

The data suggested statistically significant correlations between the variables that the hypothesized model takes into considerations. Specifically, individuals with higher machiavellianism were found to perceive less control in interpersonal situations as compared to individuals with lower machiavellianism. Individuals with higher levels of machiavellianism and psychopathy were found to perceive higher risk than individuals with lower levels of machiavellianism and psychopathy. It was also found that individuals who perceive higher risks also perceive a higher opportunity to commit online fraud. Individuals with higher levels of narcissism were found to perceive higher capabilities to commit online fraud than individuals with lower levels of narcissism, individuals with higher levels of machiavellianism were found to perceive higher opportunity and motivation to commit online fraud than individuals with lower levels of machiavellianism. Individuals with higher levels of psychopathy were found to be more willing to rationalize fraud than individuals with lower levels of psychopathy. Finally, individuals who were more willing to rationalize fraud were also more likely to have the intent to indulge in fraud than individuals who were less willingness to rationalize fraud. However, the results of structured equation model analysis indicated that the model did not provide evidence of a good statistical fit.

CHAPTER 5. DISCUSSION AND FUTURE WORK

This chapter will discuss the results of the study and implications of the research findings in context to the theories that were discussed in the literature review and future work.

5.1 Discussion

The goal of this study was to identify psychological traits and behaviors that affect an individuals' predilection towards committing an act of online fraud. In this study, a set of hypotheses were created based on a literature review of various studies in the IT and psychology domain. This study measured the variables in question with the help of questionnaires that had been previously used and tested for validity and reliability by other studies as well. The self-reported data was collected from a varied demographic of United States residents using Amazon MTurk and analyzed. There were 318 initial responses which were reduced to 290 responses to maintain the accuracy of the dataset.

The proposed model suggests that an individuals' personality traits would be predictive of different elements of the fraud theory and mediated through risk perception. The model also took into consideration an individuals' behavior in interpersonal situations, specifically, it predicted that their perception of control would be related to their personality traits when it comes to the dark triad.

The results showed evidence that most of the hypotheses were supported by statistical evidence. An individual's interpersonal behavior, such as their perception of control in interpersonal situations and their perception of risk is affected by different elements of the dark triad of personality. There was also evidence that indicated different elements of dark triad affected different elements of the fraud diamond.

This research contradicts the notion in traditional fraud detection literature research that suggests focusing on opportunity alone would help swerve the occurrence fraud (Stone, 2015) because the results of this study indicated that in an online setting, focusing on opportunity will not be as effective to prevent fraud when taking into consideration individuals varied psychological traits and their behavior in interpersonal situations. The analysis indicated that every part of the fraud diamond will be affected by different elements of the dark triad, and the dark triad elements will be affected by behavior interpersonal situations. The resulting model suggests that individuals with higher combinations of psychopathy, machiavellianism and narcissism levels possess the psychological traits and interpersonal behaviors that stimulate different phases of the fraud diamond resulting in the intent to commit fraud. Hence, it is also imperative that we analyze the interpersonal behavior of individuals who have a combination of higher levels of these undesirable traits.

The results of this study indicate that individuals who have higher levels of machiavellianism, perceive they exert lower control in socio-political situations which is in accordance with previous research (Christie et. al., 1970; Pauhlus, 1983), but this did not seem to have an effect on dark triad personality traits when it comes to fraudulent decision making. This is perhaps because fraudulent decision making involves interactions in interpersonal space, where they must be able to exert control over other individuals rather than the socio-political space, where they perceive control decisions over the actions of society as a whole. An interesting result of this study was that individuals with higher machiavellianism levels perceived that they exert less control over their peers in interpersonal situations, which is contrary to previous research (Christie et. al., 1970; Pauhlus, 1983), and this result was significant when it came to fraudulent decision making. There has been debate in the scientific research community about the integrity of the dark triad model in itself, where it has been argued that the way the dark triad traits may not be significantly distinct and that their current method of measurement is not complex enough to capture malevolent personality traits (Muris et al., 2017). This factor too perhaps could account for the unexpected result of machiavellianism being negatively related with interpersonal control.

It was also found that individuals with higher levels of machiavellianism and psychopathy also perceived higher risk in financial, ethical and social situations, and individuals who perceived higher risk were more likely to perceive higher opportunity to commit fraud. Psychopathy and machiavellianism have been associated with sensation-seeking and risky behaviors (Crysel et al., 2013; Jones & Paulhus, 2017; Mikulay and Goffin, 1998). These individuals have often been found to indulge in risky sensation seeking behaviors, so it fits that they would also perceive a higher opportunity to commit online fraud.

The effects of machiavellianism on perceived opportunity to commit fraud and the motivation to commit fraud in cyberspace were significant as well in accordance with previous research (Harrison et. al., 2018). Individuals with higher machiavellianism are generally more willing to use manipulation to act unethically (Christie & Geis, 1970). They perceive others to be gullible and easily fooled and believe that when it comes to attaining goals, manipulation is a useful method and a valid tool (O'Boyle, Forsyth, Banks, & McDaniel, 2012). Research also indicates that individuals with machiavellianism have a desire for control that often manifests in aspirations for financial success (McHoskey, 1999). Hence, these aspirations could be the reason machiavellianism motivates individuals to commit fraud, and the perception of others as gullible and easily fooled could dictate a higher perception of opportunity to commit fraud in cyberspace.

The effects of narcissism on capability were significant according to this study and suggested that narcissists perceive higher capabilities to commit online fraud. Narcissism is characterized by an elevated sense of self, they desire to be portrayed as superior in front of others (Kernburg, 1975; Ames et. al., 2004). Narcissists often have low self-esteem, but they often portray themselves more important by exaggerating their abilities even during self-evaluations (Morf & Rhodewalt, 2001; John & Robins; 1994). According to previous research, narcissists also tend to have self-evaluations that are the most unrealistically positive (John & Robins, 1994). Hence, this finding is in accordance with previous research. Narcissism on the other hand, did not have a significant effect on motivation to commit fraud, contrary to previous findings (Harrison et. al., 2018; Johnson et. al., 2012). This is interesting because ego, one of the characteristics of narcissism, is a key non-monetary motivator of fraud (Albrecht et. al., 2012; Dorminey et. al., 2012). They are also said to be entitled and self-absorbed and are hence more likely to exploit others. (Emmons 1987, Millon 1990). However, narcissism is also defined largely by internal insecurities (Kernburg, 1975), which could be a contributor to narcissism not having a significant impact on motivation to commit online fraud. Research suggests that while narcissists do desire power and prestige associated with money, they also fear having to deal with the social consequences of their actions if convicted (Ramamoorti, 2008; Albrecht et. al., 2012). Hence, the results indicate that narcissistic individuals may not be motivated to commit fraud out of fear of social ramifications if caught.

The most statistically significant finding of this study was the effect of psychopathy on willingness to rationalize online fraud and in turn the effect of rationalization on the intention to commit fraud, which is in accordance with the results of the previous research conducted on online fraud (Harrison et. al., 2018). Before a fraud is committed, it must be rationalized by an individual (Albrecht et. al., 2007; Murphy and Dacin, 2011). Individuals who are more willing to rationalize their actions, should also be more willing to take the action. Our results indicate that individuals with higher psychopathy are more willing to rationalize fraud due to their ability to do so without experiencing guilt or remorse and having a higher emphasis on themselves, with no regards for others well-being. These individuals are in turn, more likely to have the intent to commit fraud as well. Psychopathy in individuals is characterized by behaviors based on judgments concerning an elevated importance of self, whilst minimizing others well-being and rights (Levenson 1992). Psychopathic individuals tend to have little concern for other people, lack empathy, guilt and do not regret when their decisions have adverse effects on others (Hare 1991). Therefore, such individuals can demonstrate remorseless manipulation and exploitation of others and rarely experience guilt, regret or shame (Hare 1991; Lee & Ashton 2005; Cleckley, 1976). The findings of this study also contribute towards supporting the unified theory of crime which argues that psychopathy plays a major role and is the most relevant when examining any antisocial behavior, as it mirrors the elemental nature and embodies the essence of antisocial behavior (DeLisi, 2009).

Even though there were significant results from a correlation and linear regression analysis, the structural equation model was tested for goodness of fit, but statistical evidence showed that there was no evidence that the model fit the data well.

5.2 Future Work

Since the SEM model was found to not have enough evidence of a good statistical fit, the results of this study suggest that there is room for improvement of the model to predict predilection towards fraud motivation and rationalization using psychological traits and interpersonal behavior.

Fraud theory suggests that the perception of a higher opportunity to commit fraud may also motivate an individual (Cohen et al., 2010), hence it would be interesting to analyze the effects of different fraud diamond elements on each other in future research. Based on the data collected with the help of surveys described in Chapter 3, several linear regression analyses conducted between collected variables indicated that the model depicted in figure 5.1 may account for a better statistical fit, hence it would be worth investigating if this model would provide for a better statistical fit.

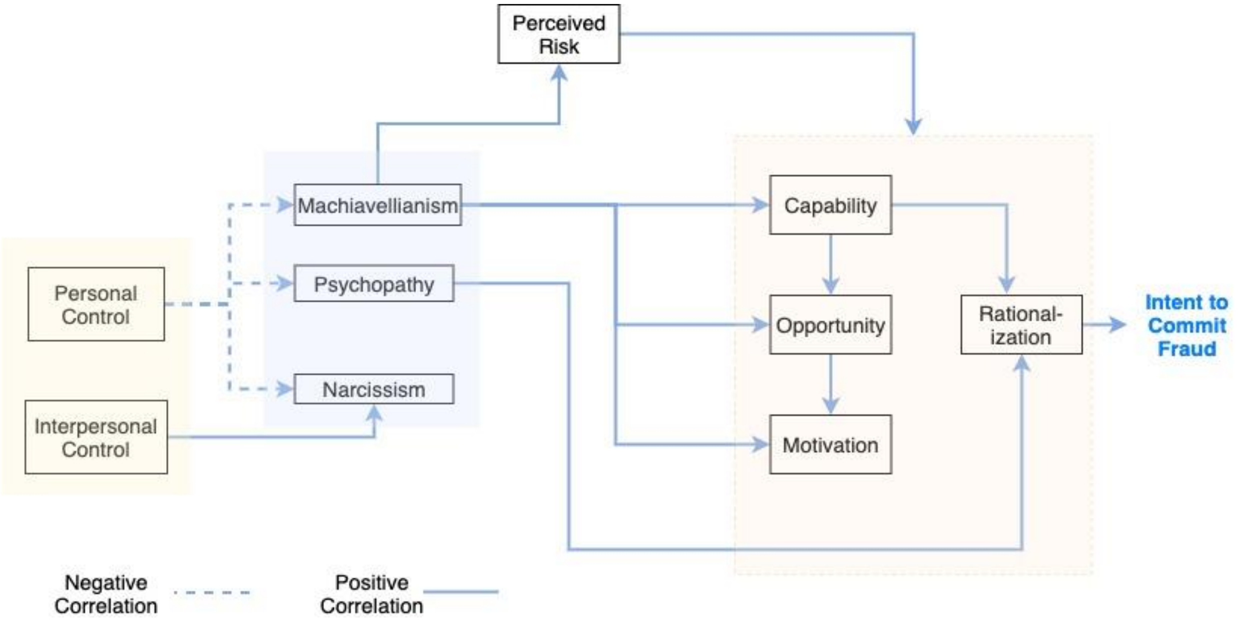


Figure 5.1 Suggested Model for Future Investigation Based on Linear Regressions

Researchers in the field of criminology have talked about the routine activity theory (Cohen & Felson, 1979) which takes a deeper look at opportunity by dividing it into the attractiveness of target, presence of a guardian to protect the target, and the environment. Since this study focuses on psychological traits and interpersonal behavior alone, including the routine activity theory which focuses on the environment of the crime as well would also be interesting future research.

REFERENCES

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2018). Phishing attacks root causes. Risks and Security of Internet and Systems, CRISIS 2017, 10694, 187–202.

Albrecht, W. S., Albrecht, C. C., Albrecht, C., & Zimbelman, M. (2012). Fraud examination (4th ed.). Mason, OH: South-Western Cengage Learning.

Albrecht, C., Albrecht, C. C., Wareham, J., & Fox, P. (2007). The role of power and negotiation in online deception. Journal of Digital Forensics, Security, and Law, 1(4), 29–48.

Ames, Daniel R., Rose, Paul, and Anderson, Cameron P. (2006). The NPI-16 as a short measure of narcissism. *Journal of Research in Personality, 40*, 440-450.

Ames, D. R., & Kammrath, L. K. (2004). Mind-reading and metacognition: Narcissism, not actual competence, predicts self-estimated ability. Journal of Nonverbal Behavior, 28, 187–209

Baughman, H. M., Dearing, S., Giammarco, E., & Vernon, P. A. (2011). Relationships between bullying behaviours and the Dark Triad: A study with adults. *Personality and Individual Differences*, *52*(5), 571–575.

Bentler, P. M. (1992). On the fit of models to covariances and methodology to the Bulletin. *Psychological Bulletin*, *112*(3), 400–404. https://doi.org/10.1037/0033-2909.112.3.400

Christie, R., & Geis, F. (1970). *Studies in Machiavellianism—1st Edition* (1st ed.). Retrieved from https://www.elsevier.com/books/studies-in-machiavellianism/christie/978-0-12-174450-2.

Cieslewicz, J.K. (2012), "The fraud model in international contexts: a call to include societal-influences in the model", Journal of Forensic and Investigative Accounting, Vol. 4 No. 1, pp. 214-254.

Cleckley, H. (1976). The mask of sanity (5th ed.). St. Louis, MO: Mosby

Cohen, J., Ding, Y., Lesage, C., & Stolowy, H. (2010). Corporate fraud and managers' behavior: Evidence from the press. Journal of Business Ethics, 95, 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. (1987). Toward an integrated theory of white-collar crime. American Journal of Sociology, 93 (2). Retrieved from http://www.jstor.org/discover/10.2307/2779590?sid=21106267411483&uid=2&uid=3739920&uid=4&uid=3739256

Comer, J. M. (1985). Machiavellianism and Inner vs Outer Directedness: A Study of Sales Managers. *Psychological Reports*, *56*(1), 81–82. https://doi.org/10.2466/pr0.1985.56.1.81

Council of Europe (2001, November 23), Summary to the Convention on Cybercrime (ETS N° 185) Treaty Office, Nov. 2001, [online] Available: http://www.coe.int/web/conventions/full-list.

Cressey, D.R. (1953), Other People's Money: The Social Psychology of Embezzlement, The Free Press, New York, NY

Crowe, H. (2011). Why the Fraud Triangle is No Longer Enough. Retrieved from www. crowehorwath.co

Crysel, L. C., Crosier, B. S., & Webster, G. D. (2013). The Dark Triad and risk behavior. *Personality and Individual Differences*, *54*(1), 35–40. https://doi.org/10.1016/j.paid.2012.07.029

Dahling, J. J., Whitaker, B. G., & Levy, P. E. (2009). The development and validation of a new Machiavellianism scale. *Journal of Management, 35*, 219–257.

DeLiema, M., Yon, Y., & Wilber, K. H. (2016). Tricks of the Trade: Motivating Sales Agents to Con Older Adults. *The Gerontologist*, *56*(2), 335–344. https://doi.org/10.1093/geront/gnu039

DeLisi, M. (2009). Psychopathy is the Unified Theory of Crime. *Youth Violence and Juvenile Justice*, *7*(3), 256–273. https://doi.org/10.1177/1541204009333834

Dolan, Kyo. (2004). Internet Auction Fraud: The Silent Victims. Journal of Economic Crime Management. vol. 2, no. 1, pp. 1-22.

Dorminey, J., Fleming, A.S., Kranacher, M. and Riley, A. Jr (2012), "The evolution of fraud theory", Issues in Accounting Education, Vol. 27 No. 2, pp. 555-579.

Dorminey, J., Fleming, A., Kranacher, M., & Riley, R. (2010). Beyond the fraud triangle: The CPA Journal, 80(7), 17-23.

Duchon, D., & Drake, B. (2009). Organizational narcissism and virtuous behavior. *Journal of Business Ethics, 85*, 301–308.

Edwards, Matthew & Peersman, Claudia & Rashid, Awais. (2017). Scamming the Scammers: Towards Automatic Detection of Persuasion in Advance Fee Frauds. 26th International World Wide Web Conference 2017, WWW 2017, Companion, 2019, pp.1291-1299. 10.1145/3041021.3053889.

Eichelberger, E. (2014). What I learned hanging out with Nigerian email scammers. *Mother Jones*, *20*.

Emmons, R. A. (1987). Narcissism: Theory and measurement. *Journal of Personality and Social Psychology, 52*(1), 11–17.

Explanatory Report to the Convention on Cybercrime (ETS N° 185) Treaty Office, Nov. 2001, [online] Available: http://www.coe.int/web/conventions/full-list.

Fazzini, K. (2019, March 28). Google and Facebook got tricked out of $123 million by a scam that costs small businesses billions every year—Here's how to avoid it. Retrieved October 16, 2019, from CNBC website: https://www.cnbc.com/2019/03/28/how-to-avoid-invoice-theft-scam-that-cost-google-facebook-123m.html

Fehr, B., Samson, D., & Paulhus, D. L. (1992). The construct of Machiavellianism: Twenty years later. In C. D. Spielberger & J. N. Butcher (Eds.), *Advances in personality assessment* (Vol. 9, pp. 77–116). Hillsdale, NJ: Lawrence Erlbaum Associates.

Financial Cost of Fraud 2018 | Crowe UK. (n.d.). Retrieved October 16, 2019, from https://www.crowe.com/uk/croweuk/insights/financial-cost-of-fraud-2018

Finklea, K. M., & Theohary, C. A. (2012, July 20). Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement [Report]. Retrieved October 16, 2019, from Digital Library website: https://digital.library.unt.edu/ark:/67531/metadc98020/

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology*, *43*(10), 2060–2072. https://doi.org/10.1111/jasp.12158

Foster, J. D., Shenesey, J. W., & Goff, J. S. (2009). Why do narcissists take more risks? Testing the roles of perceived risks and benefits of risky behaviors. *Personality and Individual Differences,* *47*(8), 885–889. https://doi.org/10.1016/j.paid.2009.07.008

Friedman, J. N. W., Oltmanns, T. F., Gleason, M. E. J., & Turkheimer, E. (2006). Mixed impressions: Reactions of strangers to people with pathological personality traits. Journal of Research in Personality, 40, 395–410.

Galli, I., Nigro, G., & Krampen, G. (1986). Multidimensional locus of control and Machiavellianism in Italian and West German students: Similarities and differences. *Applied Psychology*, *35*(4), 453–460. https://doi.org/10.1111/j.1464-0597.1986.tb00945.x

Garofalo, C., Noteborn, M. G. C., Sellbom, M., & Bogaerts, S. (2019). Factor Structure and Construct Validity of the Levenson Self-Report Psychopathy Scale (LSRP): A Replication and Extension in Dutch Nonclinical Participants. *Journal of Personality Assessment*, *101*(5), 481–492. https://doi.org/10.1080/00223891.2018.1519830

Gbegi, D. O., & Adebisi, J. F. (2013). The New Fraud Diamond Model - How can it help forensic accountants in fraud investigation in Nigeria? European Journal of Accounting Auditing and Fiancé Research Vol.1, No. 4, pp.129-138

Gercke, M. (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response. Geneva: International Telecommunications Union.

Gonzalez, George & Kopp, Lori. (2018). The Use of Personality Traits to Predict Propensity to Commit Fraud. 9.

Giammarco, E. A., Atkinson, B., Baughman, H. M., Veselka, L., Vernon, P. A. (2013). The relation between antisocial personality and the perceived ability to deceive. Personality and Individual Differences, 54, 246-250

Gordon, Sarah & Ford, Richard. (2006). On the Definition and Classification of Cybercrime. Journal in Computer Virology. 2. 13-20. 10.1007/s11416-006-0015-z.

Gu, H., Wen, Z., & Fan, X. (2017). Structural validity of the Machiavellian Personality Scale: A bifactor exploratory structural equation modeling approach. *Personality and Individual Differences*, *105*, 116–123. https://doi.org/10.1016/j.paid.2016.09.042

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis: A global perspective (7th ed.). Upper Saddle River, NJ: Pearson.

Hare, R. D. (1991). *The hare psychopathy checklist revised*. Toronto: Multi-Health Systems.

Harms, P. D. and M. S. Spain, 2015. Beyond the bright side: Dark personality at work. Applied Psychology: An International Revie. 64(1): 15–24.

Harrison, A., Summers, J., & Mennecke, B. (2018). The Effects of the Dark Triad on Unethical Behavior. *Journal of Business Ethics*, *153*(1), 53–77. https://doi.org/10.1007/s10551-016-3368-3

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Hunter, J. E., Gerbing, D. W., & Boster, F. J. (1982). Machiavellian beliefs and personality: Construct invalidity of the Machiavellianism dimension. *Journal of Personality and Social Psychology*, *43*(6), 1293–1305. https://doi.org/10.1037/0022-3514.43.6.1293

ICT Facts and Figures 2017. (n.d.). Retrieved October 15, 2019, from https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Isacenkova, J., Thonnard, O., Costin, A., Francillon, A., & Balzarotti, D. (2014). Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security*, *2014*(1), 4. https://doi.org/10.1186/1687-417X-2014-4

Jakobwitz, S., & Egan, V. (2006). The Dark Triad and normal personality traits. Personality and Individual Differences, 40, 331–339.

John, O. P., & Robins, R. W. (1994). Accuracy and bias in self-perception: Individual differences in self-enhancement and the role of narcissism. Journal of Personality and Social Psychology, 66(1), 206–219.

Johnson, E. N., Kuhn, J. R., Jr., Apostolou, B. A., & Hassell, J. M. (2012). Auditor perceptions of client narcissism as a fraud attitude risk factor. Auditing: A Journal of Practice and Theory, 32(1), 203–219.

Johnson, E. N., Kuhn, J. R., Jr., Apostolou, B. A., & Hassell, J. M. (2012). Auditor perceptions of client narcissism as a fraud attitude risk factor. *Auditing: A Journal of Practice and Theory, 32*(1), 203–219.

Jonason, P. K., Li, N. P., Webster, G. D., & Schmitt, D. P. (2008). The Dark Triad: Facilitating a short-term mating strategy in men. European Journal of Personality, 23, 5–18

Jones, D. N., & Paulhus, D. L. (2011). Differentiating the Dark Triad within the interpersonal circumplex. In L. M. Horowitz & S. Strack (Eds.), Handbook of interpersonal psychology (pp. 249–269). New York: Guilford.

Jones, D. N. (2014). Risk in the face of retribution: Psychopathic individuals persist in financial misbehavior among the Dark Triad. *Personality and Individual Differences, 67*, 109–113.

Jones, D. N., Paulhus, D. L. (2010). Differentiating the dark triad within the interpersonal circumplex. In Horowitz, L. M., Strack, S. N. (Eds.), Handbook of interpersonal theory and research (pp. 249–267). New York, NY: Guilford.

Jones, D. N., & Paulhus, D. L. (2009). *Machiavellianism*. New York: Guilford Press.

Jones, D. N., & Paulhus, D. L. (2017). Duplicity among the dark triad: Three faces of deceit. *Journal of Personality and Social Psychology, 113*(2), 329–342. https://doi.org/10.1037/pspp0000139

Kernburg, O. F. (1975). *Borderline conditions and pathological narcissism*. New York: Aronson.

Kopp, Christian & Layton, Robert & Sillitoe, Jim & Gondal, Iqbal & Jaishankar, K. (2016). The Role of Love stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. 9. 10.5281/zenodo.56227.

Kyl, J. (1996, October 4). S.982 - 104th Congress (1995-1996): National Information Infrastructure Protection Act of 1996 [Webpage]. Retrieved October 16, 2019, from https://www.congress.gov/bill/104th-congress/senate-bill/982

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, *18*(7), 763–783. https://doi.org/10.1002/mar.1029

Lee, K., Ashton, M. C., Wiltshire, J., Bourdage, J. S., Visser, B. A., & Gallucci, A. (2013). Sex, power, and money: Prediction from the dark triad and honesty–humility. *European Journal of Personality, 27*(2), 169–184.

Lee, K., & Ashton, M. C. (2005). Psychopathy, Machiavellianism, and narcissism in the five-factor model and the HEXACO model of personality structure. *Personality and Individual Differences, 38*(7), 1571–1582

Levenson, M. R. (1992). Rethinking psychopathy. *Theory and Psychology, 2*, 51–71.

Lynam, D. R., Whiteside, S., & Jones, S. (1999). Self-Reported Psychopathy: A Validation Study. *Journal of Personality Assessment*, *73*(1), 110–132. https://doi.org/10.1207/S15327752JPA730108

M. C. for Strategic and I. Studies. Net Losses: Estimating the Cost of Cybercrime - Economic Impact of Cybercrime ii. http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf , 2014.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods*, *1*(2), 130–149. https://doi.org/10.1037/1082-989X.1.2.130

McHoskey, J. W. (1999). Machiavellianism, intrinsic versus extrinsic goals, and social interest: A self-determination theory analysis. Motivation and Emotion, 23, 267–283.

Millon, T. (1990). The disorders of personality. In L. A. Pervin (Ed.), *Handbook of personality: Theory and Research* (pp. 339–370). New York: Guilford Press.

Morf, C. C., & Rhodewalt, F. (2001). Unraveling the paradoxes of narcissism: A dynamic self-regulatory processing model. Psychological Inquiry, 12, 177–196.

Muris, P., Merckelbach, H., Otgaar, H., & Meijer, E. (2017). The Malevolent Side of Human Nature: A Meta-Analysis and Critical Review of the Literature on the Dark Triad (Narcissism, Machiavellianism, and Psychopathy). *Perspectives on Psychological Science*, *12*(2), 183–204. https://doi.org/10.1177/1745691616666070

Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. Journal of Business Ethics, 101(4), 601–618.

Murray, A., Zeadally, S., & Flowers, A. (2012). *An assessment of U.S. legislation on cybersecurity*. Proc. Int. Conf. Cyber Security Cyber Warfare Digit. Forensic (CyberSec), pp. 289-294, 2012 https://doi.org/10.1109/CyberSec.2012.6246106

New FTC Data Spotlight Details Big Jump in Losses, Complaints about Romance Scams. (2019, February 12). Retrieved October 16, 2019, from Federal Trade Commission website: https://www.ftc.gov/news-events/press-releases/2019/02/new-ftc-data-spotlight-details-big-jump-losses-complaints-about

Normah, B. O, & Hesri, F. M. D. (2010). Fraud Diamond Risk Indicator: An Assessment of Its Importance and Usage, International Conference on Science and Social Research (CSSR 2010), Kuala Lumpur, Malaysia pp. 607-612.

O'Boyle, E. H., Jr., Forsyth, D. R., Banks, G. C., & McDaniel, M. A. (2012). A meta-analysis of the dark triad and work behavior: A social exchange perspective. *Journal of Applied Psychology, 97*(3), 557–579.

Paulhus, D. L. (1998). Interpersonal and intrapsychic adaptiveness of trait self-enhancement: A mixed blessing? *Journal of Personality and Social Psychology, 74*(5), 1197–1208

Paulhus, D. L. and Williams, K. M., 2002. The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. Journal of Research in Personality, 36(6), 556–563.

Paulhus, D. L. (1983). Sphere-specific measures of perceived control. *Journal of Personality and Social Psychology, 44,* 1253-1268.

Paulhus, D. L. (2013). Dark Triad of Personality (D3-Short). Measurement Instrument Database for the Social Science. Retrieved from www.midss.ie

Ramamoorti, S. (2008). The psychology and sociology of fraud: Integrating the behavioral sciences component into fraud and forensic accounting curricula. Issues in Accounting Education, 23(4), 521–533.

Rotter, Julian B (1966). "Generalized expectancies for internal versus external control of reinforcement". Psychological Monographs: General and Applied. **80**: 1 28. doi:10.1037/h0092976

Russell, G. W. (1974). Machiavellianism, Locus of Control, Aggression, Performance and Precautionary Behaviour in Ice Hockey. *Human Relations*, *27*(9), 825–837. https://doi.org/10.1177/001872677402700901

Saad, M. E., & Norul Huda Sheikh Abdullah, S. (2018). Victimization Analysis Based on Routine Activity Theory for Cyber-Love Scam in Malaysia. *2018 Cyber Resilience Conference (CRC)*, 1–3. https://doi.org/10.1109/CR.2018.8626818

Salekin, R. T., Chen, D. R., Sellbom, M., Lester, W. S., & MacDougall, E. (2014). Examining the factor structure and convergent and discriminant validity of the Levenson Self-Report Psychopathy Scale: Is the two-factor model the best fitting model? *Personality Disorders: Theory, Research, and Treatment*, *5*(3), 289–304. https://doi.org/10.1037/per0000073

Scams | CryptoScamDB. (n.d.). Retrieved October 16, 2019, from https://cryptoscamdb.org/scams

Seth, S. (2019, July 25). $9 Million Lost Each Day in Cryptocurrency Scams. Retrieved October 16, 2019, from Investopedia website: https://www.investopedia.com/news/beware-9m-are-lost-each-day-crypto-scams/

Solar, D., & Bruehl, D. (1971). Machiavellianism and Locus of Control: Two Conceptions of Interpersonal Power. *Psychological Reports*, *29*(3_suppl), 1079–1082. https://doi.org/10.2466/pr0.1971.29.3f.1079

Sorunke, Olukayode. (2016). Personal Ethics and Fraudster Motivation: The Missing Link in Fraud Triangle and Fraud Diamond Theories. International Journal of Academic Research in Business and Social Sciences. 6. 10.6007/IJARBSS/v6-i2/2020.

Stabek, A., Watters, P., & Layton, R. (2010). The Seven Scam Types: Mapping the Terrain of Cybercrime. *2010 Second Cybercrime and Trustworthy Computing Workshop*, 41–51. https://doi.org/10.1109/CTC.2010.14

Stabek, A., Brown, S., & Watters, P. (2009). The Case for a Consistent Cyberscam Classification Framework (CCCF). *2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, 525–530. https://doi.org/10.1109/UIC-ATC.2009.77

Stone, Dan N. (2015) Post-Hunton: Reclaiming Our Integrity and Literature. Journal of Information Systems: Summer 2015, Vol. 29, No. 2, pp. 211-227.

Thanasak, R. (2013). The Fraud Factors. International Journal of Management and Administrative Sciences (IJMAS) (ISSN: 2225-7225) Vol. 2, No. 2, pp. 01-05

The top frauds of 2018. (2019, February 28). Retrieved October 16, 2019, from Consumer Information website: https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018

Tsakalidis, G., & Vergidis, K. (2019). A Systematic Approach Toward Description and Classification of Cybercrime Incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(4), 710–729. https://doi.org/10.1109/TSMC.2017.2700495

Tugas, F. C. (2012). Exploring a new element of fraud: A study on selected financial accounting fraud cases in the world. American International Journal of Contemporary Research, 2(6), 112–121.

Vazire, S., & Funder, D. C. (2006). Impulsivity and the self-defeating behavior of narcissists. Personality and Social Psychology Review, 10, 154–165.

Vernon, P. A., Villani, V. C., Vickers, L. C., Harris, J. A. (2008). A behavioral genetic investigation of the dark triad and the Big 5. Personality and Individual Differences, 44, 445–452.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age* (SSRN Scholarly Paper No. ID 1066922). Retrieved from Social Science Research Network website: https://papers.ssrn.com/abstract=1066922

Weiss, B., Sleep, C., & Miller, J. D. (2016). Levenson Self-Report Psychopathy Scale. In V. Zeigler-Hill & T. K. Shackelford (Eds.), *Encyclopedia of Personality and Individual Differences* (pp. 1–6). https://doi.org/10.1007/978-3-319-28099-8_1242-1

Wilke, A., Sherman, A., Curdt, B., Mondal, S., Fitzgerald, C., & Kruger, D. J. (2014). An evolutionary domain-specific risk scale. *Evolutionary Behavioral Sciences*, *8*(3), 123-141. https://doi:10.1037/ebs0000011

Withers, K. (2019). A Psychosocial Behavioral Attribution Model: Examining the Relationship Between the “Dark Triad” and Cyber-Criminal Behaviors Impacting Social Networking Sites. *CCE Theses and Dissertations*. https://nsuworks.nova.edu/gscis_etd/1072

Whitty, M. T. (2013). The Scammers Persuasive Techniques Model Development of a Stage Model to Explain the Online Dating Romance Scam. *The British Journal of Criminology*, *53*(4), 665–684. https://doi.org/10.1093/bjc/azt009

Wolfe, D.T. and Hermanson, D. (2004), “The fraud diamond: considering the four elements of fraud”, The CPA Journal, Vol. 74 No. 12.

Wrightsman, L. S., Jr., & Cook, S. W. (1965). Factor analysis and attitude change. Peabody Papers in Human Development, 3 (No. 2).

Wu, J. and J. M. Lebreton, 2011. Reconsidering the dispositional basis of counterproductive work behavior: The role of aberrant personality. Personnel Psychology 64: 593–626.

APPENDIX A

Appendix A.1. Instrument to measure Fraud Theory Constructs (Harrison et. al., 2018)

Imagine the following scenario:

You are selling a gaming console on an online social media platform like Facebook. If you state the condition of the gaming console to make it appear significantly better than it really is, you could gain additional money from the sale.

Indicate your level of agreement with the following: (on a 7-point Likert scale)

Motivation subscale:

1. I would benefit by selling my gaming console to someone else for than it is worth
2. I have something to gain by overstating the value of the gaming console I am selling
3. I could benefit by selling the gaming console for more than it is worth

Perceived Opportunity subscale:

4. In general, a person could easily sell their gaming console online for more than it is worth
5. It is easy for someone to take advantage of other people buying gaming consoles online
6. In general, it would be easy to persuade people into buying a gaming console for more than it is worth

Perceived Capability subscale:

7. If I wanted to, I am confident I have the skills needed to sell the gaming console for more than it is worth
8. I have the skills necessary to represent this gaming console as being in better condition than it really is
9. I am skillful enough to sell this gaming console for more than it is worth

Willingness to Rationalize subscale:

10. I can justify selling this gaming console for more than it is worth
11. I believe that it is appropriate to sell the gaming console for more than it is worth online
12. In this circumstance, it is acceptable to make the gaming console appear to be in better condition

Intent to commit fraud subscale:

13. If I were going to sell the gaming console online, I would misrepresent the condition of the gaming console
14. I intend to misrepresent the condition of the gaming console if I sell it online
15. If I sell a gaming console online, I plan to misrepresent the condition of the faming console

Appendix A.2. Instrument to measure Dark Triad elements D3-Short (Paulhus, 2013)

Items are scored on a 5-point Likert scale

Machiavellianism subscale

1. It's not wise to tell your secrets.
2. Generally speaking, people won’t work hard unless they have to.
3. Whatever it takes, you must get the important people on your side.
4. Avoid direct conflict with others because they may be useful in the future.
5. It’s wise to keep track of information that you can use against people later.
6. You should wait for the right time to get back at people.
7. There are things you should hide from other people because they don’t need to know.
8. Make sure your plans benefit you, not others.
9. Most people can be manipulated.

Narcissism subscale

1. People see me as a natural leader.
2. I hate being the center of attention. (R)
3. Many group activities tend to be dull without me.
4. I know that I am special because everyone keeps telling me so.
5. I like to get acquainted with important people.
6. I feel embarrassed if someone compliments me. (R)
7. I have been compared to famous people.
8. I am an average person. (R)
9. I insist on getting the respect I deserve.

Psychopathy subscale:

1. I like to get revenge on authorities.

2. I avoid dangerous situations. (R)

3. Payback needs to be quick and nasty.

4. People often say I’m out of control.

5. It’s true that I can be mean to others. (or I enjoy having sex with people I hardly know.)

6. People who mess with me always regret it.

7. I have never gotten into trouble with the law. (R)

8. I like to pick on losers.

9. I’ll say anything to get what I want.

Appendix A.3. Instrument to measure Spheres of Control (Paulhus, 1990)

____ 1. I can usually achieve what I want if I work hard for it.

____ 2. In my personal relationships, the other person usually has more control than I do.

____ 3. By taking an active part in political and social affairs, we the people can influence world events.

____ 4. Once I make plans, I am almost certain to make them work.

____ 5. I have no trouble making and keeping friends.

____ 6. The average citizen can have an influence on government decisions.

____ 7. I prefer games involving some luck over games requiring pure skill.

____ 8. I'm not good at guiding the course of a conversation with several others.

____ 9. It is difficult for us to have much control over the things politicians do in office.

____ 10. I can learn almost anything if I set my mind to it.

____ 11. I can usually develop a personal relationship with someone I find appealing.

____ 12. Bad economic conditions are caused by world events that are beyond our control.

____ 13. My major accomplishments are entirely due to my hard work and ability.

____ 14. I can usually steer a conversation toward the topics I want to talk about.

____ 15. With enough effort we can wipe out political corruption.

____ 16. I usually do not set goals because I have a hard time following through on them.

____ 17. When I need assistance with something, I often find it difficult to get others to help.

____ 18. One of the major reasons we have wars is because people don't take enough interest in politics.

____ 19. Bad luck has sometimes prevented me from achieving things.

____ 20. If there's someone I want to meet, I can usually arrange it.

____ 21. There is nothing we, as consumers, can do to keep the cost of living from going higher.

____ 22. Almost anything is possible for me if I really want it.

____ 23. I often find it hard to get my point of view across to others.

____ 24. It is impossible to have any real influence over what big businesses do.

____ 25. Most of what happens in my career is beyond my control.

____ 26. In attempting to smooth over a disagreement, I sometimes make it worse.

____ 27. I prefer to concentrate my energy on other things rather than on solving the world's problems.

____ 28. I find it pointless to keep working on something that's too difficult for me.

____ 29. I find it easy to play an important part in most group situations.

____ 30. In the long run, we the voters are responsible for bad government on a national as well as a local level.

On all the negatively keyed items listed below, the subject's responses will be reversed (i.e., 7=1, 6=2, 5=3, 4=4, 3=5, 2=6, 1=7). Then I will calculate the score for each scale by summing the 10 items.

Personal Control: Positive 1, 4, 10, 13, 22

Negative 7, 16, 19, 25, 28

Interpersonal Control: Positive 5, 11, 14, 20, 29

Negative 2, 8, 17, 23, 26

Socio-Political Control: Positive 3, 6, 15, 18, 30

Negative 9, 12, 21, 24, 27

Appendix A.4. Instrument to measure Risk Perception (Blais & Weber, 2006)

Domain subscale	Item text
Ethical (E)	6. Taking some questionable deductions on your income tax return. (E)
	9. Having an affair with a married man/woman. (E)
	10. Passing off somebody else's work as your own. (E)
	16. Revealing a friend's secret to someone else. (E)
	29. Leaving your young children alone at home while running an errand. (E)
	30. Not returning a wallet you found that contains $200. (E)
Financial (Investment/Gambling) (F/I, F/G)	12. Investing 5% of your annual income in a very speculative stock. (F/I)
	4. Investing 10% of your annual income in a moderate growth mutual fund. (F/I)
	18. Investing 10% of your annual income in a new business venture. (F/I)
	3. Betting a day's income at the horse races. (F/G)
	14. Betting a day's income on the outcome of a sporting event (F/G)
	8. Betting a day's income at a high-stake poker game. (F/G)
Health/Safety (H/S)	5. Drinking heavily at a social function. (H/S)
	15. Engaging in unprotected sex. (H/S)
	17. Driving a car without wearing a seat belt. (H/S)
	20. Riding a motorcycle without a helmet. (H/S)
	23. Sunbathing without sunscreen. (H/S)
	26. Walking home alone at night in an unsafe area of town. (H/S)
Recreational (R)	2. Going camping in the wilderness. (R)
	11. Going down a ski run that is beyond your ability. (R)
	13. Going whitewater rafting at high water in the spring. (R)
	19. Taking a skydiving class. (R)
	24. Bungee jumping off a tall bridge. (R)
	25. Piloting a small plane. (R)
Social (S)	1. Admitting that your tastes are different from those of a friend. (S)
	7. Disagreeing with an authority figure on a major issue. (S)
	21. Choosing a career that you truly enjoy over a more prestigious one. (S)
	22. Speaking your mind about an unpopular issue in a meeting at work. (S)
	27. Moving to a city far away from your extended family. (S)
	28. Starting a new career in your mid-thirties. (S)

Appendix A.5. Computer Crime Index – Revised Plus CCI – R+, (Rogers, Seigfried-Spellar & Bayes, 2017)

Have you in the past five years indulged in the following:

1. Wrote/programmed a virus or piece of malicious software designed to damage a system or another individual's device. (Virus Writing)
2. Distributed to other individuals a piece of malicious software designed to damage a system or another individual's device. (Virus Distribution)
3. Launched a Distributed Denial of Service (DDoS) attack or any attack designed to prevent a user from accessing a website or system by making it unavailable. (DDoS)
4. Used a botnet or collection of infected systems in order to coordinate an attack against a system. (Botnet)
5. Distributed to other individuals or systems a malicious piece of software designed to encrypt files, or otherwise render files unreadable, until a ransom is paid. (Ransomware)
6. Purchased stolen credit card information. (Data Dump)
7. Stole or harvested credit card information without permission in order to sell to others. (Data Breacher)
8. Guessed another individual's password to gain access to their system, device, or an online account. (Guessing Passwords)
9. Used an automated tool in order to crack a password on another individual's system or device. (Cracking Passwords)
10. Used an automated tool written by others to attack or gain unauthorized access to a system. (Script Kiddies)
11. Sent misleading messages designed to encourage users to enter their login information for a website or system without a specific target. (Phishing)
12. Sent misleading messages personalized to a certain user or group of users designed to encourage them to enter their login information for a website or system. (Spear Phishing)
13. Tampered with a DNS server or setup a malicious website redirect designed to collect users' login information for a website or system. (Pharming)
14. Knowingly made, used, or gave to another person an illegally downloaded copy of commercially sold software or videogame?
15. Accessed another person's computer account or files without their knowledge or permissions just to look at the information or files?
16. Accessed another person's email or social media account without their permission?
17. , deleted, or changed any information in another's computer account without their knowledge or permission?
18. Used someone else's identity online (without their permission) to conduct a commercial transaction, apply for credit, or conduct any other financial transaction?
19. Used a wireless access, or Wi-Fi, access point that you did not have permission or authorization to use?
20. . Monitored or used a sniffer to see network or Internet traffic information without authorization or permission?
21. Defaced, altered, or vandalized a website without authorization or permission?

22. Disclosed passwords, usernames, or other account information without permission?
23. information on a business system or network that you did not have authorization or permission to see?
24. Harassed, annoyed, or stalked someone through emails, Instagram, Facebook, or other technology?
25. Sent unsolicited bulk emails, Facebook messages, or Instagram/Twitter DMs?
26. Without permission, installed a device or piece of software designed to obtain usernames and/or passwords?
27. Without permission, installed software or a device on a network or system designed to circumvent security measures?
28. Contacted an individual pretending to be someone else in order to gain access to information you are unauthorized to access?
29. Used another's password or gave out your own password in order to share access to a multimedia streaming service? (e.g. Hulu, Netflix, HBO Now)

APPENDIX B.

Table B.1.: Scam Genre 1, *(Stabek et. al., 2010)*

Scam Name	Source	Country	Scam Name	Source	Country
Door to door	SW	Aus	Cold calling	ACCC	Aus
Psychic & clairvoyant	SW	Aus	Share promotion & hot tips	ACCC	Aus
Office supply	SW	Aus	Gambling software	ACCC	Aus
Directories & Advertising	SW	Aus	Overpayment	ACCC	Aus
Fake online pharmacies	SW	Aus	Miracle cures	ACCC	Aus
Weight loss	SW	Aus	Weight loss	ACCC	Aus
Miracle cures	SW	Aus	Fake online pharmacies	ACCC	Aus
Domain name renewal	SW	Aus	Psychic & clairvoyant	ACCC	Aus
Cheque overpayment	SW	Aus	Door to door	ACCC	Aus
Cold calling	SW	Aus	Business opportunities	ACCC	Aus
Counterfeit cashiers check	IC3	USA	Small business	ACCC	Aus
Internet extortion	IC3	USA	Direct entry unauthorized advertising	ACCC	Aus
Financial advice	ABS	Aus	Mystery shopper	USPIS	USA
Pyramid schemes	ABS	Aus	Credit card fraud	USPIS	USA
Credit & bank card	ABS	Aus	Child support collection scheme	USPIS	USA
Fake clairvoyant	OFT	UK	Social security schemes	USPIS	USA
Bogus investment	OFT	UK	Unclaimed income tax refund	USPIS	USA
Miracle health cure	OFT	UK	Unclaimed funds	USPIS	USA

Bogus health product	ERG	Can	Property tax exemption	USPIS	USA
Investment fraud	ERG	Can	Cut rate health insurance	USPIS	USA
Advance fee vacation fraud	ERG	Can	Investment fraud	USPIS	USA
Overpayment for sale of merchandise	ERG	Can	Solicitations disguised as invoices	USPIS	USA
Miracle health & slimming	OFT	UK	Oil & gas investment	USPIS	USA
Clairvoyant & psychic mailing	OFT	UK	Land fraud	USPIS	USA
High risk investment	OFT	UK	Illegal sweepstakes	USPIS	USA
Rolling labs	FBI	USA	Government look alike mail	USPIS	USA
Letter of credit fraud	FBI	USA	Free vacations scams	USPIS	USA
Prime bank note	FBI	USA	Receipt for unsolicited merchandise	USPIS	USA
Weight loss claims	OGO	USA	Missing person	USPIS	USA
Cure all products	OGO	USA	Fraudulent health & medical products	USPIS	USA
Check overpayment	OGO	USA	Astrology psychic & clairvoyant	SS	Aus
Pharmacy fraud	L2G2BT	USA	Cheque overpayment	SS	Aus
Investments fraud	L2G2BT	USA	Share trading	SS	Aus
Multiple bidding	L2G2BT	USA	Cold calling	FDO	Aus
Counterfeit cashiers check	L3G2BT	USA	Fake debt invoices	FDO	Aus
Health & diet scams	USC	USA	Fraudulent cheques & credit cards	QPOL	Aus

Table B.2.: Scam Genre 2, (Stabek, Watters, & Layton, 2010)

Scam Name	Source	Country	Scam Name	Source	Country
Charity	SW	Aus	Advance fee scam	L2G2BT	USA
Dating & romance	SW	Aus	Charities fraud	L2G2BT	USA
Fax back	SW	Aus	Nigerian 419	L2G2BT	USA
Spam offers	SW	Aus	Foreign Lottery	L2G2BT	USA
Upfront payment	SW	Aus	Sweepstakes & prizes	L2G2BT	USA
Nigerian 419	SW	Aus	Lottery	ACCC	Aus
Lottery & sweepstakes	SW	Aus	Fake prize	ACCC	Aus
Unexpected prizes	SW	Aus	Chain letters	ACCC	Aus
Chain letters	SW	Aus	Nigerian scam	ACCC	Aus
Lotteries	IC3	USA	Inheritance scam	ACCC	Aus
Nigerian letter 419	IC3	USA	Dating and romance	ACCC	Aus
Advance fee fraud	ABS	Aus	Distributorship & franchise fraud	USPIS	USA
Chain letters	ABS	Aus	900 telephone numbers	USPIS	USA
Lottery	ABS	Aus	Advance fee loan schemes	USPIS	USA
Advance fee	OFT	UK	Charity fraud	USPIS	USA
International sweepstakes	OFT	UK	Chain letters	USPIS	USA
Prize draw pitch	OFT	UK	Free prize schemes	USPIS	USA
Bogus lottery	OFT	UK	Foreign lotteries	USPIS	USA
High pressure sales pitch vacation	ERG	Can	Telemarketing fraud	USPIS	USA
Prize lottery & sweepstakes	ERG	Can	Home improvement & repair	USPIS	USA
West African 419	ERG	Can	Phony inheritance	USPIS	USA
Advance fee loan	ERG	Can	Prison pen pal money order scam	USPIS	USA
Upfront fee for credit card	ERG	Can	Nigerian	SS	Aus
Prize draw & sweepstakes	OFT	UK	Lottery prizes	SS	Aus
Foreign lottery	OFT	UK	Holiday prizes	SS	Aus
Premium rate telephone prize	OFT	UK	Internet bride	SS	Aus
African advance fee frauds foreign money	OFT	UK	Inheritance scam	SS	Aus
Bogus holiday club	OFT	UK	Churches	SS	Aus

Telemarketing	FBI	USA	Bowling clubs	SS	Aus
Nigerian or 419	FBI	USA	Hit man	SS	Aus
Advance fee scheme	FBI	USA	Dating dowry & romance	SS	Aus
Nigerian email	OGO	USA	Donation	SS	Aus
Foreign lotteries	OGO	USA	Nigerian letter and advance fee fraud	FDO	Aus
Pay in advance credit offers	OGO	USA	Lottery scams	FDO	Aus
Debt relief	OGO	USA	Requests to use bank account	QPOL	Aus
Cross border fraud	L2G2BT	USA	Online relationship	QPOL	Aus
Romance scheme	L2G2BT	USA	Charity scam	QPOL	Aus

Table B.3.: Scam Genre 3, (Stabek, Watters, & Layton, 2010)

Scam Name	Source	Country
Business Opportunity	SW	Aus
Guaranteed employment & income	SW	Aus
Work from home	SW	Aus
Transferring money for someone else	SW	Aus
Employment for business opportunities	IC3	USA
Re-shipping	IC3	USA
Third party receiver of funds	IC3	USA
Employment work from home	ERG	Can
Cheque cashing money transfer job fraud	ERG	UK
Work at home & business opportunity scam	OFT	USA
Work at home scams	OGO	USA
Job scams	L2G2BT	USA
Counterfeit money orders	L2G2BT	USA
Bogus business opportunities	USC	USA
Work from home	ACCC	Aus
Guaranteed employment	ACCC	Aus
Phony job opportunities	USPIS	USA
Postal job scams	USPIS	USA
Work at home schemes	USPIS	USA
Employment work from home	SS	Aus
Money transfer	SS	Aus
Fake job email or money transfer schemes	FDO	Aus

Table B.4.: Scam Genre 4, (Stabek, Watters, & Layton, 2010)

Scam Name	Source	Country
SMS competition & trivia	SW	Aus
Missed calls & texts from unknown numbers	SW	Aus
Ring tone	SW	Aus
Modem jacking	SW	Aus
Superannuation	SW	Aus
Premium rate prize draw	OFT	UK
Property investment	OFT	UK
Internet dialer	OFT	UK
Bogus vanity publishers	OFT	UK
Bogus invention promotions	OFT	UK
Bogus model & casting agencies	OFT	UK
Loan scams	OFT	UK
Missed calls	ACCC	Aus
Text messages	ACCC	Aus
SMS competition & trivia	ACCC	Aus
Faxback	ACCC	Aus
Office supply	ACCC	Aus

Table B.5.: Scam Genre 5, (Stabek, Watters, & Layton, 2010)

Scam Name	Source	Country
Spyware and key-loggers	SW	Aus
Free offers on the internet	SW	Aus
Credit card	SW	Aus
Phony fraud alerts	SW	Aus
Requests for account info	SW	Aus
Credit card fraud	SW	Aus
Debt elimination	IC3	USA
Identity theft	IC3	USA
Phishing and spoofing	IC3	USA
Spam	IC3	USA
Phishing and related	ABS	Aus
Identity theft	ABS	Aus
Impersonation or identity fraud	FBI	USA
Phishing	OGO	USA
Hacking	L2G2BT	USA
Identity theft	L2G2BT	USA
Phishing and spoofing	L2G2BT	USA
Spam	L2G2BT	USA
Spyware	L2G2BT	USA
Discount software offers	USC	USA
Phishing email	USC	USA
Trojan horse email	USC	USA
Virus generated email	USC	USA
Phishing	ACCC	Aus
Fake fraud alerts	ACCC	Aus
Spam	ACCC	Aus
Malicious software	ACCC	Aus
Identity theft	SS	Aus
Phishing	SS	Aus
Software	SS	Aus
Virus	SS	Aus
Trojan	SS	Aus
Ransomware	SS	Aus
Spyware	SS	Aus
Malware	SS	Aus
Fake bank emails	FDO	Aus
Social networking fraud	FDO	Aus
Identity theft	FDO	Aus

Table B.6.: Scam Genre 6, (Stabek, Watters, & Layton, 2010)

Scam Name	Source	Country
Online auction and shopping	SW	Aus
Cars skimming	SW	Aus
Product misrepresentation	IC3	USA
Non delivery	IC3	USA
Auction fraud Romania	IC3	USA
Parcel courier email scheme	IC3	USA
Escrow services fraud	IC3	USA
Bill for unsuitable merchandise	ERG	Can
Medical equipment fraud	FBI	USA
Services not performed	FBI	USA
Medicare fraud	FBI	USA
Debt elimination	L2G2BT	USA
Non delivery	L2B2GT	USA
misrepresentation	L2G2BT	USA
Triangulation	L2B2GT	USA
Fee stacking	L2G2BT	USA
Black market or counterfeit goods	L2B2GT	USA
Shill bidding	L2G2BT	USA
International auction fraud	L2B2GT	USA
Escrow services scam	L2G2BT	USA
Card skimming	ACCC	Aus
Online auctions and shopping	ACCC	Aus
Ringtone	ACCC	Aus
Online classifieds	SS	Aus

Table B.7.: Scam Genre 7, (Stabek, Watters, & Layton, 2010)

Scam Name	Source	Country
Identity theft	SW	Aus
Computer prediction software	SW	Aus
Investment seminars and real estate	SW	Aus
Share promotions and hot tips	SW	Aus
Pyramid schemes	SW	Aus
Investment fraud	IC3	USA
Ponzi or pyramid	IC3	USA
Get rich quick	OFT	UK
Bogus racing tipster	OFT	UK
Pyramid selling and chain letter	OFT	UK
Internet matrix scams	OFT	UK
Redemption strawmen or bond	FBI	USA
Ponzi schemes	FBI	USA
Investment schemes	FBI	USA
Ponzi or pyramid	OGO	USA
419 advance fee fraud	L2G2BT	USA
Pyramid scheme	USC	USA
Investment seminar	ACCC	Aus
Charity	ACCC	Aus
Multilevel marketing	USPIS	USA
Affinity fraud	SS	Aus
Pyramid	SS	Aus
Ponzi	SS	Aus
Courses and seminars	SS	Aus
Pump and dump	FDO	Aus
Pyramid schemes	FDO	Aus
Ponzi scheme	FDO	Aus
Affinity fraud	FDO	Aus
Business opportunity	QPOL	Aus