EXPLORING THE RELATIONSHIP BETWEEN SELF-ESTEEM, FINANCIAL EGOCENTRISIM, AND FRAUD SUSCEPTIBILITY IN CYBER-ENABLED FRAUD SCHEMES INVOLVING CRYPTO ASSETS

by

James McDowell

Liberty University

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

Liberty University

November, 2023

EXPLORING THE RELATIONSHIP BETWEEN SELF-ESTEEM, FINANCIAL EGOCENTRISIM, AND FRAUD SUSCEPTIBILITY IN CYBER-ENABLED FRAUD SCHEMES INVOLVING CRYPTO ASSETS

by

James McDowell

Liberty University

A Dissertation Presented in Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

Liberty University

November, 2023

APPROVED BY:

_____

Laura Beiler, Ph.D., Committee Chair

_____

Rachel Piferi, Ph.D., Committee Member

ABSTRACT

The propensity to exploit others for one's own benefit is continuously exhibited by bad actors. Unfortunately, this sentiment holds true in emerging asset classes, such as crypto assets. As a result, it is surprising that current research on fraud susceptibility is approached in a binary way. Researchers examine either what makes an individual predisposed to victimization by bad actors or what factors influence one's propensity to perpetrate fraudulent schemes. This study bridged this substantial gap in current research by investigating if specific psychological factors influence when, or if, an individual shifts between these two outcomes. The psychological factors incorporated into this analysis included self-esteem, financial egocentrism, and fraud susceptibility. These variables were measured through self-reported assessments. Secondary analysis additionally explored the efficacy of the threat of punishment as a deterrent for the perpetration of cyber-enabled fraud schemes. The evidence indicated that higher levels of financial egocentrism were linked to higher fraud susceptibility. The study also identified that the threat of punishment did not have a statistically significant impact on the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets.

Keywords: cyber-enabled fraud, crypto assets, cybercrime

Dedication

This dissertation is dedicated to those victimized by cyber-enabled fraud schemes involving crypto assets.

Acknowledgments

The candidate wishes to acknowledge the candidate's personal, academic, and professional mentors who positively influenced the candidate. These individuals include Dr. Gary Mottola, Sarah Gill, Sam Draddy, Yvette Panetta, Gregory Markovich, Joseph Borg, Amanda Senn, Dr. Laura Beiler, and Dr. Rachel Piferi.

TABLE OF CONTENTS

List of Tables

List of Figures

CHAPTER 1: INTRODUCTION TO THE STUDY

Introduction

One of the most prominent and lucrative investments in recent years is crypto assets (Coinmarketcap, 2023; Trozze et al., 2022). Unfortunately, the rise in popularity of crypto assets generated a substantial increase in cyber-enabled fraud schemes that rely on this asset as a means to facilitate the schemes (ASIC, 2022; FBI, 2023; FCA, 2019). This form of crime involves the usage of digital devices to exploit the vulnerabilities of potential victims, such as self-esteem and egocentrism, as a means to solicit potential victims to invest in fraudulent schemes or reveal information that can be used in the furtherance of a scheme (e.g., login credentials, private keys, etc.) (McDowell & Woods, 2022).

Moreover, researchers approach this area of research in a binary way by examining either one's propensity to be victimized or one's predisposition to victimize others. This study aimed to investigate the potential relationship between self-esteem, fraud susceptibility, and financial egocentrism in cyber-enabled fraud schemes involving crypto assets, by exploring the impact of these factors on an individual's ability to shift between these two outcomes. This study provides valuable insights to assist individuals, financial institutions, and law enforcement agencies in enhancing investor protection and market integrity by contributing to the development of effective strategies to aid in the mitigation and prevention of cyber-enabled fraud schemes involving crypto assets, which is based on ample academic and theological support.

Background

Scientific evidence indicates that self-esteem is a fundamental element in social cognition (Fiske & Taylor, 2021). Given the findings related to the adverse impact that low levels of self-esteem have on one's ability to regulate one's emotions and actions (Asp et al., 2012; Aquino et al., 2020; Benson & Giacomin, 2020; Gardner & Pierce, 2011), it is unsurprising that current literature indicates that one's feelings about how one navigates social settings, a key component of self-esteem, plays an important role in one's susceptibility to cyber-enabled fraud (Burton et al., 2021; Coluccia et al., 2020; Hanoch & Wood, 2021; Kircanski et al., 2019; Scheibe et al., 2019; Wen et al., 2022; Whitty, 2019; Zebrowitz et al., 2018) by impacting one's ability to accurately assess whom is worthy of one's trust (DeLiema et al., 2020; DeLiema et al., 2021; Jones et al., 2019; Lichtenberg et al., 2020; Murthy & Gopalkrishnan, 2022; Steinmetz, 2021).

Additional evidence indicates that the way in which one processes one's surroundings is an important aspect in determining one's susceptibility to cyber-enabled fraud schemes (Frauenstein & Flowerday, 2020; Norris & Brookes, 2021; Wang, 2022; Wang & Zhou, 2022). For example, recent evidence indicates that how one perceives the individual offering of a product impacts how persuasive one finds the sales pitch (Baker & Rojeck, 2020; Baryshevtsev & McGlynn, 2020, Esmaeili & Golpayegani, 2020; Judges et al., 2017; Koestner et al., 2016; Wahab & Tao, 2019; Wang & Zhou, 2022; Ye et al., 2022). An important aspect of the way in which one processes information is one's tendency to focus on oneself (i.e., one's egocentrism). Egocentrism is a trait linked to negative psychological traits and a propensity to engage in risky behaviors, including cyber-enabled fraud. These include overconfidence, narcissism, emotional instability, and arrogance (Dambrun, 2017; Geis, 2011; Krancher et al., 2010; Kruger et al., 2005; Speer

et al., 2022; Pedneault et al., 2012; as cited in Vousinas, 2019). This evidence indicates that the propensity to perpetrate a cyber-enabled fraud scheme may be influenced by one's financial egocentrism.

Given that the crypto assets are financial assets, the appeal of leveraging crypto assets as a means to perpetrate cyber-enabled fraud schemes is unsurprisingly correlated to financial exploitation in traditional markets (Kamps & Kleinberg, 2018; Raimundo Júnior et al., 2022). Moreover, the typical user of crypto assets exhibits traits linked to increased fraud susceptibility (Arthur & Delfabbro, 2017; Blanco et al., 2011; Ebner et al., 2020; Faber et al., 2012; Martin et al., 2022; Sudzina et al., 2021).

Research into the psychological factors involved in cyber-enabled fraud is a nuanced endeavour requiring significant precision. This complexity generated a split in current research resulting in a bifurcation into two distinct approaches: studies focused on one's penchant for exploiting others by perpetrating fraudulent schemes (Aguilera & Vadera, 2008; Blickle et al., 2006; Eaton & Korach, 2016; Gottschalk, 2020; Nolasco Braaten & Vaughn, 2021; Palmieri et al., 2021; Van Nguyen, 2022; Ye et al., 2019) or one's susceptibility to exploitation by others (Abdelhamid, 2020; Cheng et al., 2021; Marson & Sabatino, 2012; Modic et al., 2018; Mueller et al., 2020; O'Connor et al., 2021; Parsons et al., 2019; Raimundo Júnior et al., 2022; Sorell & Whitty, 2019; Sur et al., 2021; Wang et al., 2023; Wei et al., 2019; White & Wilkoff, 2023; Xu et al., 2022; Zebrowitz et al., 2018). This generates a substantial gap that must be addressed.

Despite this substantial gap in the literature, the evidence indicates that social psychological factors play an influential role in both of these outcomes. These factors include the role that one's opinion of one's self (i.e., one's self-esteem (Greenhaus &

Callanan, 2006; Rosenberg, 1965)) plays in one's ability to navigate one's surroundings (Kernis, 2005; Moksnes & Espnes, 2013; Stets & Burke, 2014), which consists of how one thinks (Kahneman, 2011; Neff & Vonk, 2009; Orth & Robins, 2014), responds to stimulus (Fiske & Taylor, 2021), and makes financial decisions (McCannon et al., 2016; Twenge & Campbell, 2002).

Additionally, the role of one's focus on one's self (i.e., one's egocentrism (Piaget, 1951; Wink, 1991)) has been linked to sub-optimal financial decisions (Berg et al., 1995; Sanchez & Dunning, 2018). The evidence indicates that egocentrism may be associated with one's decision to perpetrate a cyber-enabled fraud scheme and one's propensity to be exploited by a bad actor perpetrating a cyber-enabled fraud scheme.

Problem Statement

A study that addresses the binary approach that researchers currently take to investigating fraud susceptibility is appropriate for a variety of stakeholders. In order to effectively and efficiently bridge this gap in a comprehensive way, the study must additionally investigate the relationship between key psychological variables (e.g., self-esteem and egocentrism) and these two potential outcomes (i.e., one's propensity to be victimized and one's predisposition to victimize others). Evidence related to the potential for one to shift between being victimized and victimizing others may provide crucial, and more comprehensive, insight into fraud susceptibility. On an individual level, this would be useful to academics, practitioners, and executives when exploring resource allocation related to fraud education and prevention efforts. Given the digitization of classified and proprietary data, the transnational impact of cybercrime, and the exponential growth of this form of exploitation (Steinmetz et al., 2023), the collection of more nuanced and

comprehensive evidence related to cyber-enabled fraud susceptibility may additionally enhance the security of organizations, agencies, and nations.

In the current political climate, the regulation of crypto assets is also a highly contested debate garnering significant attention and consuming substantial resources. Thus, scientific evidence related to the role that the threat of punishment plays in one's decision as to whether or not to exploit others, when provided the opportunity to do so, is a substantial chasm in current research that must be addressed prior to the enactment of legislation in this burgeoning asset class (Middleton, 2005; Rose, 2010). Given the role that self-esteem (McGregor & Jordan, 2007) and egocentrism (Handgraaf et al., 2008) play in one's compliance with authority (Chen et al., 2021), this is an essential variable for inclusion to further analyze the relationship between the target variables.

This study mitigated the identified gap in current academic literature by addressing this bifurcation of research through an evaluation of the impact of self-esteem and fraud susceptibility on one's predisposition to perpetrate fraudulent schemes (i.e., finanical egocentrism). The study additionally examined the influence of the threat of punishment on one's decision to perpetrate a cyber-enabled fraud scheme that is facilitated by crypto assets.

Purpose of the Study

The purpose of this quantitative study was to investigate the role that self-esteem, financial egocentrism, and fraud susceptibility play in cyber-enabled fraud involving crypto assets, including one's propensity to victimize others and one's predisposition to be victimized. This was done through a series of self-assessments and simulated

situations. Additionally, the study explored the efficacy of the threat of punishment as a deterrent to perpetrating cyber-enabled fraud schemes in simulated situations.

Research Question(s) and Hypotheses

Research Questions

RQ1: Does a relationship between financial egocentrism, as measured by a modified version of the trust game (Berg et al., 1995), and fraud susceptibility, as measured by the Brief version of the Susceptibility-to-Persuasion II Scale (StP-II-B)(Modic et al., 2018), exist in participants as moderated by their self-esteem level, as measured by the Rosenberg Self-Esteem Scale (Rosenberg, 1965)?

RQ2: How do financial egocentrism, fraud susceptibility, and self-esteem predict the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets in simulated situations?

RQ3: How do financial egocentrism, self-esteem, and the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets in a simulated situation relate to fraud susceptibility?

RQ4: How does the threat of punishment, as measured by the threat levels of punishment, predict the decision to perpetrate cyber-enabled fraud schemes involving crypto assets in simulated situations?

Hypotheses

Research Hypothesis 1: A statistically significant difference exists between financial egocentrism across the identified levels of self-esteem.

Null Hypothesis 1: A statistically significant difference does not exist between financial egocentrism and self-esteem.

Research Hypothesis 2: Higher self-esteem is associated with a lower level of fraud susceptibility and a higher level of financial egocentrism.

Null Hypothesis 2: Higher self-esteem is not associated with a lower level of fraud susceptibility and a higher level of financial egocentrism.

Research Hypothesis 3: The threat of punishment is an effective deterrent in the perpetration of cyber-enabled fraud schemes involving crypto assets.

Null Hypothesis 3: The threat of punishment is not an effective deterrent in the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets.

Assumptions and Limitations of the Study

Assumptions

A key assumption of the study was that participants will provide honest responses to the survey and scenario prompts incorporated in the study. Additionally, it was assumed that participants will only complete the study one time each. The assumption that the sample of participants also corresponds to a representative sample of the population more broadly was also made. Lastly, the belief that cyber-enabled fraud schemes involving crypto assets operate in a similar fashion to fraud susceptibility of other mediums and asset classes was also assumed in the study.

Limitations

There was a clear lack of related studies to the one proposed in this prospectus, which generates a substantial challenge. Given that cyber-enabled fraud is researched in a binary way (i.e., researchers explore one's susceptibility to fraud victimization or one's predisposition to perpetrating criminal schemes), there is ample opportunity for dissenting opinions related to the value of the study and identified findings. The study

primarily relied on limited extrapolation in order to establish relevancy from previous research to establish the validity and usefulness of the study and the scientific evidence that was collected.

A significant limitation of the study emanated from the previously described challenge that no directly related studies were identified as part of the review of academic literature. This limitation meant that identified evidence should be cautiously interpreted and not be given undue credence as a result of the novel approach described in the proposed study. This was due to the fact that the approach taken during the study must be meticulously evaluated by academics to establish the validity of it. Given that findings generated through extrapolation, even limited extrapolation, may fail to align with future findings generated by comprehensive and nuanced evaluations, it is important that the findings uncovered as a result of the study be treated only as a means to support new opportunities for future research, rather than as a means to establish entirely new doctrines.

Theoretical Foundations of the Study

Academic Perspective

The identified gap in current research stems from the binary approach of researchers in fraud susceptibility research. Researchers conduct studies that either investigate the psychological factors that influence one's propensity to be victimized by fraudulent schemes (Aguilera & Vadera, 2008; Blickle et al., 2006; Eaton & Korach, 2016; Gottschalk, 2020; Nolasco Braaten & Vaughn, 2021; Palmieri et al., 2021; Van Nguyen, 2022; Ye et al., 2019) or one's predisposition to victimize others by perpetrating fraudulent schemes against them (Abdelhamid, 2020; Cheng et al., 2021; Marson &

Sabatino, 2012; Modic et al., 2018; Mueller et al., 2020; O'Connor et al., 2021; Parsons et al., 2019; Raimundo Júnior et al., 2022; Sorell & Whitty, 2019; Sur et al., 2021; Wang et al., 2023; Wei et al., 2019; White & Wilkoff, 2023; Xu et al., 2022; Zebrowitz et al., 2018). No evidence was identified that indicated what factors, if any, may influence an individual to shift between these two outcomes.

The variables of the study were selected based on the gestalt of research related to cyber-enabled fraud schemes involving crypto assets. Evidence indicates that social psychological factors are a key factor related to cyber-enabled fraud susceptibility. These include one's self-esteem and one's egocentrism.

One's opinion of one's self (i.e., one's self-esteem (Greenhaus & Callanan, 2006; Rosenberg, 1965)) plays a key role in one's ability to navigate one's surroundings (Kernis, 2005; Moksnes & Espnes, 2013; Stets & Burke, 2014), including how one thinks (Kahneman, 2011; Neff & Vonk, 2009; Orth & Robins, 2014), responds to stimulus (Fiske & Taylor, 2021), and makes financial decisions (McCannon et al., 2016; Twenge & Campbell, 2002).

Additionally, one's perception of others, including an individual offering a product to another, is associated with one's perception of persuasiveness of the sales pitch (Baker & Rojeck, 2020; Baryshevtsev & McGlynn, 2020, Esmaeili & Golpayegani, 2020; Judges et al., 2017; Koestner et al., 2016; Wahab & Tao, 2019; Wang & Zhou, 2022; Ye et al., 2022). On a more granular level, the evidence further indicates that the extent to which one focuses on one's self (Piaget, 1951; Wink, 1991) plays a pivotal role in the efficacy of one's financial decision-making capability (Berg et al., 1995; Sanchez & Dunning, 2018). This concept includes the way in which one processes one's

surroundings, which is a crucial component in determining one's susceptibility to cyber-enabled fraud schemes (Frauenstein & Flowerday, 2020; Norris & Brookes, 2021; Wang, 2022; Wang & Zhou, 2022).

Biblical Perspective

This study is rooted in three theological principles, which include the importance of abstaining from crime, the seriousness of remaining wary of the adverse implications of greed, and the significance of placing justice as a central tenant in how one comports in interactions with others.

Scripture calls one to refrain from committing crimes in several passages. In a broad sense, one is called to understand that there is no "easy" path in which there are no dangers because these challenges are an essential component of life (*New International Version Bible*, 1978/2011, John 16:33). It can be argued that this includes refraining from pursuing the easy path to wealth and riches (i.e., exploiting others to obtain their wealth). Adherence to the rules of society and governing bodies is additionally provided as a key aspect of what makes one a close follower of Him (Romans 13:1-4). Specifically, the idea of exploiting others for one's personal benefit clearly defies Scripture (Exodus 20:15).

The call to refrain from pursuing the trappings of greed is additionally present in several passages throughout Scripture. Specifically, one is called to remain cognizant of the idea that the pursuit of opulence as a means to obtain joy will only result in one failing to obtain satisfaction with one's life (*New International Version Bible*, 1978/2011, Ecclesiastes 5:10). In fact, one may find that overvaluing the importance of wealth is more detrimental than beneficial (1 Timothy 6:10). It is also evident that greed may cost one's spirit (Proverbs 1:19).

In contrast, justice and the pursuit of it is a central tenant of Christianity, and this notion serves as a cornerstone for several of His teachings (*New International Version Bible,* 1978/2011, Psalm 82:3). This principle is built on the idea that pursuing justice is a beneficial exercise to those who walk with Him and detrimental to those who pursue evil (Proverbs 21:15). In the context of business, the incorporation of these concepts entails the calling to build wealth by treating others in financial transactions with fairness and respect (Proverbs 28:6; Proverbs 13:11; Proverbs 22:7; Proverbs 15:27).

Definition of Terms

The following is a list of definitions of terms that are used in this study.

Crypto Assets – A private digital asset secured through some form of cryptography that may be used to facilitate commerce and is not issued by a public authority (Houben & Snyers, 2020).

Cyber-Enabled Fraud – Financially motivated crimes using technological means to amplify the impact of the crime (Button & Cross, 2017).

Financial Egocentrism – One's propensity for trust and reciprocity in an investment game (Berg et al., 1995).

Self-Esteem – One's definition of self-worth (Rosenberg, 1965).

Significance of the Study

Despite the challenges and limitations described in preceding sections, this study provides clear and substantial value to academia, business, and practice in the field of cyber-enabled fraud prevention and investigation. Given the increasing frequency of cyber-enabled fraud schemes involving crypto assets, the findings uncovered by the study

also provide crucial contextual intelligence to relevant stakeholders in the protection of investors and financial markets.

Moreover, the continuing and pervasive exploitation of technology as a means to disrupt political and economic activities of countries underscores the important potential implications of identified findings of the proposed study. By obtaining a more nuanced understanding of the social psychological factors associated with cyber-enabled fraud susceptibility, academics and practitioners are positioned to more effectively and efficiently allocate resources to the prevention and investigation of cybercrimes, which in turn may prove to enhance the security of individuals, businesses, and countries.

Summary

The study addressed a substantial gap in current literature related to a bifurcation in research concerning cyber-enabled fraud susceptibility, whereby researchers investigate either an individual's predisposition to perpetrate cyber-enabled fraud schemes or one's susceptibility to exploitation via cyber-enabled fraud schemes. By incorporating social psychology principles, the study bridged this gap by investigating what factors, if any, may cause an individual to shift between these two results. These principles are rooted in a comprehensive review of current academic literature associated with cyber-enabled fraud schemes.

Despite the binary approach in current academic literature, three key themes were identified across publications related to cyber-enabled fraud. These principles were the three ways in which victims are groomed, the three factors motivating individuals to

perpetrate cyber-enabled fraud schemes, and the individualistic characteristics that increase susceptibility to cyber-enabled fraud.

After establishing this foundation, the relationship between social psychology and cyber-enabled fraud was examined in the bifurcated literature as a result of the clear evidence supporting the role of social psychology in both an individual's susceptibility to victimization and proclivity to victimize others. In the context of victim susceptibility, one's social network (Mueller et al., 2020; Wei et al., 2019), loneliness (Burton et al., 2021; Coluccia et al., 2020; Hanoch & Wood, 2021; Sur et al., 2021; Wen et al., 2022; Whitty, 2019), ability to ascertain who was worthy of trust (DeLiema et al., 2020; DeLiema et al., 2021; Jones et al., 2019; Lichtenberg et al., 2020; Murthy & Gopalkrishnan, 2022; Steinmetz, 2021;), and the way in which one processed information (Frauenstein & Flowerday, 2020; Norris & Brookes, 2021) were identified as key factors. In the context of offender psychology, social influence (Baker & Rojeck, 2020; Baryshevtsev & McGlynn, 2020, Esmaeili & Golpayegani, 2020; Wahab & Tao, 2019; Wang & Zhou, 2022; Ye et al., 2022), adequate incentivization (Attrill-Smith & Wesson, 2020; Orjiakor et al., 2022;), and hubris (Van Driel, 2018; Yaksic, 2020) were identified as key factors in the decision to perpetrate a cyber-enabled fraud scheme and ensure victim compliance with that scheme.

CHAPTER 2: LITERATURE REVIEW

Overview

Cyber-enabled fraud susceptibility is an essential area for future research given the prevalence of technology in the lives of individuals. There is clear support that psychological factors play a role in both one's susceptibility to victimization in cyber-enabled fraud schemes and one's propensity to perpetrate cyber-enabled fraud schemes as a means to victimize others. No evidence could be identified of a study that evaluated when, or if, an individual may shift between these two outcomes and what psychological factors may play a role in that shift.

Description of Search Strategy

Strict criteria was used to conduct this systematic review of academic literature related to cyber-enabled fraud to ensure that a comprehensive investigation was conducted. Primarily, articles were required to be published in peer-reviewed journals, which allowed for a focus on research that was generally accepted by the scientific community. Given that cyber-enabled fraud susceptibility is a rapidly evolving area of research, the second criterion of this review was that only articles that were published after January 1, 2018, were included in the review. This criterion was necessary to ensure the review was strictly focused on current findings.

Boolean operators were used to query academic databases (e.g., Elsevier, SAGE Journals, SpringerLink, PLOS One, etc.). For example, the term cyber-enabled fraud was searched in quotation marks, followed by the term social relationships, to focus search results to the specific topic of this systematic review, which allowed for twenty-eight articles to be identified and incorporated into this review.

Review of Literature

One's thoughts about oneself in relationship to others play an integral role in the essence of what it means to be human (Fiske & Taylor, 2021). Thus, it is no surprise that one's relationships with oneself and others provides a clear indicator of one's susceptibility to victimization by others. Yet, this is not the only psychological factor supported by the gestalt of literature. Current research also suggests that several psychological factors (e.g., self-esteem, susceptibility to persuasion, and financial egocentrism) are associated with cyber-enabled fraud susceptibility and the propensity to perpetrate cyber-enabled fraud. It is reasonable to extrapolate that one's engagement in such behaviors, and one's feelings about one's engagement in those behaviors, are important components of cyber-enabled fraud susceptibility.

Three Underlying Themes

Three overarching main themes were uncovered during the review of current research. These key themes ultimately informed the variables chosen for the proposed study and the identified gap in current literature that was identified. These concepts were that victims are groomed in three distinct ways, three different factors motivate individuals who perpetrate cyber-enabled fraud, and certain individualized characteristics may increase susceptibility to cyber-enabled fraud.

The Three Ways Victims are Groomed in Cyber-enabled Fraud

Although cyber-enabled fraud is a burgeoning area of research, there is no standardized definition that is accepted by all researchers and practitioners. This notion speaks to the nuances involved in research in this emerging area. A systematic literature review was conducted to uncover that the grooming of cyber-enabled fraud victims may

vary dramatically between different victims of the same scheme. However, one key principle emerged as an important component of all cyber-enabled fraud schemes. This was the concept that persuadability was a fundamental element of susceptibility (Modic et al., 2018).

On its face, this principle is intuitive. It stands to reason that persuading an individual to participate in a cyber-enabled fraud scheme is tantamount to making a convincing sales pitch (Modic et al., 2018). This led researchers to develop the Susceptibility to Persuasion II (StP-II) scale, which was crafted through two experiments to establish the reliability and validity of the scale. The StP-II scale was created to quantify an individual's susceptibility to fraudulent pitches that may be received by the individual.

Given the findings uncovered in Modic et al. (2018), the notion that individuals may be recruited into cyber-enabled fraud schemes (i.e., groomed) in different ways is unsurprising. The evidence indicates that there are three distinct ways in which individuals may be recruited. The three ways that were identified include solicitation through broad communications (e.g., public social media posts) (Bekkers & Leukfeldt, 2022; Mirea et al., 2019), communication targeted at specific groups (Dearden & Scaptura, 2023; O'Connor et al., 2021), and personalized communications tailored specifically to the individual (Murthy & Gopalkrishnan, 2022; Steinmetz, 2021).

The recruitment of victims via broad and generic posts was studied by Mirea et al. (2019). After conducting 17 qualitative interviews with individuals who engage in activity on the Darknet (i.e., the unindexed portion of the internet that requires specialized tools to access), researchers identified that publicly accessible forums are

often leveraged to facilitate a wide variety of criminal activity, including cyber-enabled fraud (e.g., purportedly selling drugs to individuals and then failing to provide the drugs to the purchaser) (Dolliver, 2015, as cited in Mirea et al., 2019).

Another way in which bad actors may recruit victims is through solicitation to specific groups of individuals (e.g., affinity fraud) (Dearden & Scaptura, 2023). By tailoring a message to a subset of the population, bad actors may increase the success rate of the cyber-enabled fraud scheme (O'Connor et al., 2021). Phishing, which involves sending messages that appear targeted to specific individuals (e.g., all employees of a given organization), is one of the most prevalent examples of this form of recruitment. The evidence indicates that this form of communication is often the initial form of contact between fraudsters and victims in a wide variety of crimes (FBI, 2023).

One of the less common forms of recruitment of potential cyber-enabled fraud victims is messages specifically targeted at one individual. While this is one of the least common forms of grooming, the evidence indicates that bespoke communication is one of the most effective forms of victim recruitment (Murthy & Gopalkrishnan, 2022; Steinmetz, 2021). One potential explanation for the efficacy of this form of recruitment is that it allows fraudsters to exert social influence and exploit an individual's need to belong (Suler, 2016).

Three Drivers of Cyber-Enabled Fraudsters

While the evidence suggests that victims are recruited into cyber-enabled fraud in three distinct ways, no consensus appeared as to what psychological factors or theories may explain why individuals choose to perpetrate cyber-enabled fraud schemes. Despite no general consensus, three key factors were identified as potential explanations. These

included convenience (Bekkers & Leukfeldt, 2022; Braaten & Vaughn, 2021; Buil-Gil & Zeng, 2022; Gottschalk, 2020; Nolasco), the way in which the bad actors viewed themselves (Palmieri et al., 2021; Van Nguyen, 2022; Ye et al., 2019), and complex social structures (Leukfeldt & Holt, 2020).

Advancements in technology enhanced the ease with which individuals can interact with others (Suler, 2016). Unfortunately, this includes increasing bad actors access to potential victims (Gottschalk, 2020). For example, the popularization of social media as a means to connect fostered cyber-enabled fraud by allowing bad actors to more readily solicit potential victims (Bekkers & Leukefeldt, 2022), including the perpetration of cyber-enabled fraud schemes involving crypto assets (Nolasco Braaten & Vaughn, 2021). Evidence in support of this assertion is clear due to the uptick in cyber-enabled fraud that occurred during the lockdowns that resulted from the global health crisis caused by COVID-19 (Buil-Gil & Zeng, 2022). This concept provides support for the extrapolation that technology increased the convenience with which bad actors could perpetrate cyber-enabled fraud schemes, which in turn increased the occurrence of cyber-enabled fraud involving crypto assets.

Given that the perpetration of cyber-enabled fraud schemes entails more than a solitary event and is more of a time intensive process, it is unsurprising that sufficient enticement is a necessary prerequisite for fraudsters to engage in the activity (Van Nguyen, 2022). In fact, the time intensive process of obtaining compliance with a fraudulent scheme requires exploitation of the perception of the potential victims, which informed the identity construction of the fraudsters (Ye et al., 2019). Thus, the evidence

supports the assertion that individuals who perpetrate cyber-enabled fraud schemes are enticed to do so by self-interest (Palmieri et al., 2021).

In addition to convenience and self-interest as motives for perpetrating cyber-enabled fraud, there is also a distinct psychological factor involved in meeting one's need to belong (Leukfeldt & Holt, 2020). One example of a broader manifestation of this concept can be viewed when examining fraudulent companies and the ways in which resources are allocated within them (Wang et al., 2021). The social structures of these organizations prioritize short-term incentives over long-term implications, which is a principle that aligns with individual approaches to perpetrating cyber-enabled fraud. Thus, the way in which one views oneself in relation to others (i.e., one's focus on one's need to belong), even in a criminal organization, is an important factor in the study of cyber-enabled fraud.

Certain Behaviors and Traits Increase Cyber-Enabled Fraud Susceptibility

Two specific commonalities were identified in this review as factors that increase susceptibility to cyber-enabled fraud. These included confidence in one's technological ability and openness with others. Taken in the aggregate, these findings support the assertion that one's opinion of oneself is an important component in one's susceptibility to cyber-enabled fraud.

Researchers identified that one's confidence in one's ability to use technology was associated with one's likelihood of cyber-enabled fraud victimization (Cheng et al., 2020; Emami et al., 2019). While this finding may be explained, at least in part, as a result of increased use of technology due to perceived proficiency, the importance of the finding remains the same. There is a clear link between how one perceives oneself or

one's abilities and one's propensity to be victimized by bad actors. Given that individuals who were victimized in the past were also more likely to be re-victimized, there is also scientific evidence supporting the notion that one's perception of one's competence is an essential component of one's susceptibility to cyber-enabled fraud victimization (O'Connor et al., 2021).

Individuals who exhibited more openness when engaging with others online were also shown to be more susceptible to victimization by bad actors (Akdemir & Lawless, 2020; Murthy & Gopalkrishnan, 2022). This finding is further supported by a study that was conducted by Steinmetz (2021), which found that more outgoing and connected individuals were more likely to be targeted by bad actors supporting cyber-enabled fraud schemes.

Social Psychology and Cyber-Enabled Fraud

Given the three key themes identified across current academic literature, there is clear scientific evidence that social psychological factors play a role in both one's propensity to victimize others and one's predisposition to be victimized. Therefore, one must consider that psychology plays a fundamental role in cyber-enabled fraud. Specifically, social network, loneliness, ability to accurately assess the trustworthiness of others, and the way in which one processes information were identified as key psychological factors in determining one's susceptibility to cyber-enabled fraud schemes.

Scientific evidence also points to findings that social psychology plays an influential role in one's decision to perpetrate cyber-enabled fraud. A review of current research related to offender psychology identified that both situational and individual psychological factors play a role in this decision (Mohammed et al., 2020). In the context of offender psychology, the factors from social psychology that were identified were

social influence (Baker & Rojeck, 2020; Baryshevtsev & McGlynn, 2020, Esmaeili & Golpayegani, 2020; Wahab & Tao, 2019; Wang & Zhou, 2022; Ye et al., 2022), sufficient incentives (Attrill-Smith & Wesson, 2020; Orjiakor et al., 2022), and hubris (Van Driel, 2018; Yaksic, 2020).

Psychological Factors Impacting Victim Susceptibility

The evidence indicated that cyber-enabled fraud susceptibility is connected to a wide array of characteristics. These included one's social network (Wei et al., 2019; Mueller et al., 2020), loneliness (Burton et al., 2021; Coluccia et al., 2020; Hanoch & Wood, 2021; Sur et al., 2021; Wen et al., 2022; Whitty, 2019), perceived trustworthiness and executive functioning (DeLiema et al., 2020; DeLiema et al., 2021; Jones et al., 2019; Lichtenberg et al., 2020; Murthy & Gopalkrishnan, 2022; Steinmetz, 2021), and information processing (Frauenstein & Flowerday, 2020; Norris & Brookes, 2021).

Social Network.

Given that humans are social creatures, it is unsurprise that one's perception of one's social network plays an influential role in determining one's ability to successfully navigate various stimuli (Fiske & Taylor, 2021). Several factors were identified, including how one perceives right and wrong (Wei et al, 2019).

A study involving a sample of undergraduate students in China conducted by Wei et al. (2019) uncovered that susceptibility to cyber-enabled fraud schemes was influenced by how one perceives the behavior of others. Specifically, the more one believed others were more susceptible to cyber-enabled fraud, the more one was aware of cyber-enabled fraud. Researchers also identified that the more one observed cyber-enabled fraud, the more one believed oneself and one's network to be susceptible to adverse impact.

Interestingly, researchers found that individuals who perceived cyber-enabled fraud in their network took mitigation measures (i.e., observation of cyber-enabled fraud led to behavioral responses in participants).

The evidence indicates that there is a clear association between one's social network and one's susceptibility to cyber-enabled fraud. This assertion is also supported by findings uncovered in a study that was conducted by Mueller et al. (2020). In a study involving 281 randomly selected participants from Amazon Mechanical Turk with a mean age of 53.4 years old, researchers identified emotional intelligence as an effective mediation factor in fraud susceptibility. These findings provide additional support for the notion that one's ability to successfully navigate social relationships plays an essential role in one's susceptibility to cyber-enabled fraud.

As a result of the identified findings that one's social relationships are an important component in one's susceptibility to cyber-enabled fraud, researchers must additionally consider the inverse of this concept. In other words, researchers must additionally investigate the influence that the perceived absence of a social network (i.e., loneliness) has on one's susceptibility to cyber-enabled fraud in order to obtain a comprehensive image of this area of research.

Loneliness.

Findings supporting the positive impact of a social network that one perceives as strong is not the same thing as identifying support for an adverse impact of a perceived lack of a social network. This is important because these apparently related concepts are not one in the same. Given that the ability to successfully navigate social relationships has been proven to serve as a mitigating factor in cyber-enabled fraud susceptibility, it is

necessary to explore the role that the absence of this factor plays in one's susceptibility to cyber-enabled fraud. Through an investigation of current research focused on loneliness and fraud susceptibility, one is able to obtain a comprehensive image of cyber-enabled fraud susceptibility that supports the assertion that loneliness does, in fact, have an adverse impact on one's predisposition to be victimized by bad actors perpetrating fraudulent schemes. This support was uncovered in six studies.

The first of these studies was a literature review conducted by Coluccia et al. (2020), which examined the psychological factors that influence susceptibility to romance scams. Victims of romance scams, which are a subset of cyber-enabled fraud involving the cultivation and exploitation of a perceived personal relationship between the fraudster and the victim, were found to possess high levels of loneliness across the 12 studies examined by researchers. Additional factors identified in the literature reviewed by Coluccia et al. (2020), included low self-esteem, high need for social connection (i.e., companionship), and high emotional instability (i.e., high levels of neuroticism, impulsiveness, and sensation-seeking behavior).

In a more focused study, researchers identified findings that cyber-enabled fraud susceptibility is linked to social isolation. The lack of a social network also had a significant impact (Burton et al., 2021). Although the study primarily focused on cyber-enabled fraud susceptibility in older individuals, the underlying concepts identified by the researchers were aligned with findings in additional studies, which supports the broader applicability of this principle.

In fact, Hanoch & Wood (2021) also examined the psychological factors associated with fraud susceptibility. Researchers found evidence supporting that one's

perception of one's success in social relationships plays an influential role in one's susceptibility to cyber-enabled fraud. Specifically, researchers identified that one's perception of how socially isolated one is played a role in one's propensity to victimization by bad actors.

In a comprehensive study involving 2,272 individuals who were at least 65 years of age, Sur et al. (2021) found evidence supporting the principle that one's perception of oneself is an integral factor in one's susceptibility to cyber-enabled fraud, which further aligns with the findings identified by Hanoch & Wood (2021) and Burton et al. (2021). Sur et al. (2021) uncovered that one who self-reported higher levels of perceived social support from a social network had a decreased level of fraud susceptibility.

Additionally, a study that was conducted by Wen et al. (2022) examined the relationships between loneliness, susceptibility, and vulnerability in a sample of 252 Chinese adults with an average age of 67.94 years old. Researchers used a questionnaire to collect evidence indicating that loneliness was positively correlated with fraud susceptibility. This finding further supports the idea that one's perception of one's social network plays a substantial role in one's susceptibility to cyber-enabled fraud.

Using a sample of 11,780 individuals, including 728 of whom self-identified as victims of cyber-enabled fraud and 329 of whom self-identified as chronic victims, Whitty (2019) identified individuals who possessed adverse social traits (e.g., loneliness, anxiety, and stress) were more susceptible to cyber-enabled fraud schemes. Whitty (2019) also uncovered support for the relationship between emotional instability (e.g., high levels of neuroticism) and cyber-enabled fraud. Additionally, researchers found that individuals who possessed low levels of conscientiousness were more susceptible to

cyber-enabled fraud, which is indicative of the potential relationship between self-esteem, egocentrism, and cyber-enabled fraud susceptibility.

Loneliness as a Consequence of Cyber-enabled Fraud Victimization

The implications of loneliness as a consequence of fraud victimization are also an important area of research to consider as part of a comprehensive review of cyber-enabled fraud research. The adverse implications of loneliness, as it relates to victimization in cyber-enabled fraud schemes, is especially evident in romance scams. Romance scams are scams where victims are tricked into believing they are engaged in a romantic relationship with an individual when in actuality the victim is engaging with a fraudster who is soliciting funds from the victim (Coluccia et al. 2020; Sorell & Whitty, 2019; Wang, 2022). Given the nature of this type of cyber-enabled fraud, it is unsurprising that victims of this form of exploitation often suffer sever adverse psychological implications.

Primarily, a qualitative study investigating romance scam victimization found that victims often suffered from self-doubt, shame, and adverse mental health consequences, such as increased levels of anxiety, depression, and cynicism (Sorrell & Whitty, 2019). Researchers conducted this study by reviewing transcripts of romance scam victim interviews and identified instances of chronic fraud victimization (i.e., victims were exploited multiple times).

In a study involving 15,322 individuals in China, researchers found additional support for the association between fraud victimization and depressive symptoms in middle-aged and older adults (Wang et al., 2023). These findings were further supported by a qualitative study involving the interview of 20 individuals that identified eight

common themes related to the psychological impact of cyber-enabled fraud victimization (Wang, 2022). The most relevant of these notions was that victimization resulted in a shift in one's perception of oneself. Given that this concept was identified and supported across several studies, one could hypothesize that this shift is related to one's self-esteem and that a self-perpetuating cycle of chronic fraud victimization may exist.

The potential that a self-perpetuating cycle of chronic fraud victimization exists is unsurprising given that the same psychological factors that increase fraud susceptibility are the symptoms of being victimized. These findings are unsurprising given the nature of cyber-enabled fraud. The exploitation of social relationships is a fundamental element of cyber-enabled fraud schemes, which aligns with the concept that individuals who are lonely may be more susceptible to cyber-enabled fraud. However, one must consider that loneliness is simply a trait that is more readily exploitable, not a precursor to susceptibility. Given the findings that one's level of trust (Whitty, 2019) and executive functioning (Coluccia et al., 2020) may be related to one's fraud susceptibility, one must consider the potential relationship between one's ability to appropriately perceive who is worthy of trust and one's susceptibility to cyber-enabled fraud (DeLiema et al., 2020; DeLiema et al., 2021; Jones et al., 2019; Lichtenberg et al., 2020; Murthy & Gopalkrishnan, 2022; Steinmetz, 2021).

Perceived Trustworthiness and Executive Functioning.

A key tenant of cyber-enabled fraud is the exploitation of a victim's trust by a bad actor. It also stands to reason that one who is more open and trusting will inevitably trust someone who is not worthy of that trust (e.g., a bad actor). This underlying principle informs an additional area of research related to the role that one's ability to discern who

is worthy of trust plays in one's susceptibility to cyber-enabled fraud. Additionally, the gestalt of research does not support that one should be distrusting of others as a means to protect against exploitation. In fact, the evidence supports the opposite. As is evidenced by current research, one must consider that the way in which one processes context when determining who is worthy of trust is the important aspect of susceptibility. In other words, one's ability to discern the intention of others in a social interaction is the important component (i.e., shifting between automated and controlled cognition (Fiske & Taylor, 2021)). Six studies were identified in this review of current academic literature on the role of trust in cyber-enabled fraud susceptibility.

Primarily, DeLiema et al. (2020) examined the psychological profile of an investment fraud victim in a sample of 1,027 individuals who self-reported to be investors, 214 of whom self-reported to be victims of investment fraud. Researchers found that overconfidence, increased risk tolerance, and high impulsivity were associated with increased susceptibility. Cognitive biases (e.g., illusory control and hindsight) were also linked to higher fraud susceptibility, which supports the assertion that the shift between automatic and controlled cognition (Fiske & Taylor, 2021) is an important area for further research. Additionally, DeLiema et al. (2020) found that individuals who were more trusting of investment recommendations from individuals outside of their social network, as opposed to a reliance on information from their social network, were more susceptible to investment fraud. This idea supports the notion that one's ability to appropriately discern individuals worthy of trust is an important component in fraud susceptibility.

In a later study conducted by DeLiema et al. (2021), researchers expanded on several principles identified in DeLiema et al. (2020). Specifically, DeLiema et al. (2021) examined scam compliance across various forms of fraud using a sample of 1,175 individuals who previously reported a scam to the Better Business Bureau in the United States of American and Canada. This analysis led to the determination that scams that were perceived as official were more likely to lead to individuals engaging with the scheme, which ultimately resulted in individuals losing more money to these scams. These findings highlight the importance that one's ability to appropriately and accurately discern who is trustworthy plays in one's fraud susceptibility.

In a study investigating the potential relationship between one's perception of various parts of one's life and fraud susceptibility, Lichtenberg et al. (2020) collected a survey of 242 individuals in order to create the Financial Exploitation Vulnerability Scale (FEVS). A key principle of the FEVS is the incorporation of context into the scale. This allowed researchers to identify that higher levels of insecurity (e.g., financial and relationship) were associated with higher levels of fraud susceptibility. As a result of assessing context as part of the FEVS, researchers were also able to hypothesize that the increased fraud susceptibility was likely attributable to a decrease in executive functioning due to increased levels of stress. This evidence further supports the assertion that one's ability to appropriately ascertain information in a social interaction (e.g., the trustworthiness of an individual) is essential in determining fraud susceptibility.

Researchers also investigated the various psychological factors that increase susceptibility to a specific type of cyber-enabled fraud, social engineering (Steinmetz, 2021). By conducting 37 interviews with 30 information technology professionals and

seven nonprofessionals, researchers uncovered five criteria that created the ideal victim. One of the criterion identified by Steinmetz (2021) was “connected”, which was defined as an individual who participated in a social network. Individuals who were both under-connected or over-connected were identified as more susceptible to cyber-enabled fraud. This finding, which is supported by the other studies discussed in preceding sections, also highlights that one’s ability to sufficiently navigate various social settings is an essential component in one’s overall susceptibility to cyber-enabled fraud. Extrapolation of this finding supports the notion that one’s ability to accurately assess the intention of others (e.g., who is worthy of trust) is predicated on one’s ability to appropriately shift between automated and controlled cognition as a result of a given stimulus (Fiske & Taylor, 2021).

The second relevant criterion identified by Steinmetz (2021) was “controlled”, which was defined as one’s ability to adequately manage one’s behavior (i.e., appropriately control one’s impulses). Unsurprisingly, the evidence indicated that individuals who were less controlled were more susceptible to cyber-enabled fraud, which aligns with findings by the other relevant studies discussed in preceding sections. The inevitable conclusion that one draws from these findings is that the ability to manage one’s relationships, including one’s relationship with oneself, is the cornerstone of one’s susceptibility to fraud. Additionally, it is reasonable to assume that one must be able to understand oneself in order to successfully navigate relationships with others, which includes understanding the needs that one is seeking to satisfy from the interaction with another person (Fiske & Taylor, 2021).

In a study involving a sample of 135 individuals, Murthy & Gopalkrishnan (2022) used a survey to examine the relationship between one's susceptibility to cyber-enabled fraud and one's willingness to provide information online (i.e., online openness). The evidence indicated that individuals who possessed higher levels of openness when interacting with others online were more susceptible to cyber-enabled fraud.

Although slight extrapolation of this principle is required, it is reasonable to assess that openness is connected to one's willingness to trust the intentions of others, which is supported by the findings described in preceding sections. Thus, Murthy & Gopalkrishnan (2022) provide evidence that one's willingness to provide personal information to others is an important aspect of one's willingness to trust others. This was identified as a key part of fraud susceptibility in the additional studies discussed in this chapter and was a central part of the investigation conducted by Jones et al. (2019).

Phishing, which is a subset of cyber-enabled fraud schemes involving electronic mail, was the focus of a study conducted by Jones et al. (2019) involving a sample of 224 participants. Researchers uncovered that participants who were less cynical were more susceptible to cyber-enabled fraud. In other words, researchers found that individuals who were more trusting of others were more susceptible to cyber-enabled fraud, which is a concept in alignment with the principle that one's ability to accurately discern the intentions of others is a crucial component in one's ability to protect oneself from exploitation by individuals perpetrating cyber-enabled fraud schemes.

As a result of the findings uncovered by Jones et al. (2019), it is reasonable to hypothesize that the dual-process theory (Kahneman, 2011) may play a role in cyber-enabled fraud susceptibility. Specifically, the evidence suggests that dual mode cognition

(Fiske & Taylor, 2021) may be the underlying principle that explains this phenomena. Given that the stimulus that initiates a shift in one's mode of cognition may be the essential component in determining the cyber-enabled fraud susceptibility of an individual, the evidence suggests that the way in which one processes information is an important area of fraud susceptibility, which was a principle explored in studies conducted by Norris & Brookes (2021) and Frauenstein & Flowerday (2020).

Information Processing.

Given that the scientific evidence described throughout this chapter supports the notion that the way in which one derives and assesses important information from the world around them (e.g., social interactions) is an essential aspect in one's susceptibility to cyber-enabled fraud, it is unsurprising that this extrapolation is backed by two recent studies conducted by Norris & Brookes (2021) and Frauenstein & Flowerday (2020).

Norris & Brookes (2021) conducted an academic literature review in order to explore the impact that various psychological factors have on cyber-enabled fraud susceptibility. Interestingly, researchers identified the way in which one processes information is a key element in identifying one's susceptibility to cyber-enabled fraud. This was done through a unique approach assessing the influence of one's emotional state on one's susceptibility. The evidence indicated that individuals who process information deeper are less susceptible to cyber-enabled fraud. The researchers additionally identified that one's emotional state impacts one's susceptibility as a result of the impact that one's emotional state has on one's ability to focus and assess specific stimulus. These findings further support the importance of the dual mode of cognition as it relates to cyber-enabled fraud susceptibility (Fiske & Taylor, 2021).

Frauenstein & Flowerday (2020) further examined this concept through a study where survey data were collected from 215 participants at a university in South Africa to investigate the association between the way in which one processes information on a social networking site and one's susceptibility to a specific cyber-enabled fraud schemes, phishing. The study uncovered that information processing is a key component in determining cyber-enabled fraud susceptibility. Specifically, the evidence indicated that the perception of the relationship with the fraudster played an influential role in the victim's decision as to whether or not to engage with the fraudster. This finding further supports the concept from Fiske & Taylor (2021) that the way in which one processes information is an important component in one's ability to shift between the two modes of cognition.

As a result of the binary approach that researchers take to this topic, it is necessary to also explore the psychological factors that make one predisposed to perpetrate cyber-enabled fraud. Incorporation of this second portion of the bifurcated research provides important contextual intelligence into what factors, if any, may cause an individual to shift between victimization by, and victimizing others through, cyber-enabled fraud schemes.

Social Psychology and Cyber-Enabled Fraud Offender Psychology

As a result of the bifurcation in current literature, the second crucial element in cyber-enabled fraud research is the psychological factors that influence the offender to perpetrate a fraudulent scheme and victimize others. As documented in the corpus of literature collected, it is evident that social psychology also plays a role in one's predisposition to perpetrate a cyber-enabled fraud scheme (Mohammed et al., 2020),

despite that offenders appear to select victims at random (Norris et al., 2019). The findings of the review conducted by Norris et al. (2019), which reviewed 34 prior studies, support the need for a more comprehensive study related to the psychology of offenders as it relates to the decision to perpetrate cyber-enabled fraud schemes. Social engineering, which essentially involves tricking a victim to do something that they should not (Salahdine & Kaabouch, 2019), which has substantially grown in frequency and intensity in recent years (FBI, 2023), is an example of where offender psychology is an essential element that must be further investigated. This is due to the fact that social engineering plays a role in a wide array of crimes (e.g., theft, ransomware, phishing, etc.).

In fact, a study that was conducted by Steinmetz et al. (2021) found that there are 12 elements required to create a successful social engineering campaign. Researchers identified these elements by conducting interviews with 37 information security professionals. Ultimately, researchers identified that information security professionals believed that perpetrators of successful cyber-enabled fraud schemes exploited several psychological factors in the furtherance of the crimes.

Given that the scientific evidence supports the assertion that a selected stimulus (e.g., the perpetrator) has an influence over the way in which a potential victim perceives the product being offered to them (e.g., the fraudulent scheme being pitched) through an influence over the way in which one processes information, it is important to evaluate the role that the offender's social influence plays in scam compliance (Baker & Rojeck, 2020; Baryshevtsev & McGlynn, 2020, Esmaeili & Golpayegani, 2020; Wahab & Tao, 2019; Wang & Zhou, 2022; Ye et al., 2022). Additional psychological factors that were

identified in current academic literature included adequate incentivization (Attrill-Smith & Wesson, 2020; Orjiakor et al., 2022) and hubris (Van Driel, 2018; Yaksic, 2020).

Social Influence and Victim Compliance.

It is clear that offender psychology is an essential component of obtaining a comprehensive understanding of cyber-enabled fraud as a result of the binary approach taken by researchers. Studies investigating the psychological factors involved in perpetrating cyber-enabled fraud schemes provide an interesting perspective into the identified gap in current research that will be mitigated by the proposed study. Specifically, the way in which the victim perceived the offender was an essential component in how persuasive the bad actor was in soliciting victim participation in the scheme (Baker & Rojeck, 2020; Baryshevtsev & McGlynn, 2020, Esmaeili & Golpayegani, 2020; Wahab & Tao, 2019; Wang & Zhou, 2022; Ye et al., 2022).

The evidence indicates that social cognition plays an influential role in electronic commerce (Esmaeili & Golpayegani, 2020). This includes the finding that social conformance plays a role in one's decision to engage with one business over another. The extrapolation of this principle is appropriate given that cyber-enabled fraud schemes are fundamentally a business transaction between the fraudster and the victim. Thus, the notion that how one feels about another is an important component in one's decision as to whether or not to engage in business with that individual was a key finding uncovered by researchers that is also applicable to cyber-enabled fraud. The extrapolation of this principle and application to this area of research is also supported by additional scientific evidence in a variety of ways.

In a study exploring the role that language (e.g., signs and symbols) plays in the exploitation of potential victims in telecom and internet fraud, Ye et al. (2020) found that exploitation of various social and cultural perceptions of victims was crucial to obtaining compliance with the fraudulent scheme. The researchers also found that this understanding informed the persona creation of the fraudsters at the onset of the scheme.

Building upon this notion, one must consider the additional psychological factors that allow cyber-enabled fraud to occur (i.e., encourage victim compliance). In a study conducted by Baker & Rojeck (2020), researchers examined a specific cyber-enabled fraud scheme perpetrated via social media by Annabelle Gibson. Gibson used false claims to be a survivor of cancer as a means to fraudulently sell products to individuals. Gibson additionally made false representations as to the use of proceeds (e.g., profits would be donated to charity) to further entice victims to participate in the scheme. Through the conducted analysis, researchers uncovered that Gibson's scheme was successful as a result of her ability to manipulate her followers' perception of the depth of the emotional connection that was shared and the perception of her trustworthiness. It is unsurprising that social media is an effective persuasion tool (Ziyadin et al., 2019), especially in the context of financial decision-making, given that many investors, especially younger investors, typically rely on recommendations from social media influencers to make investment decisions (FINRA Investor Education Foundation, 2023). As a result of the driving force that one's need to connect has in the way in which one perceives the world around them (Fiske & Taylor, 2021), the evidence indicates that the exploitation of social media as a means to perpetrate cyber-enabled fraud schemes was

essentially inevitable due to success that bad actors have with this form of exploitation (Baker & Rojeck, 2020).

Interestingly, researchers also uncovered evidence supporting that the way in which messages are presented plays a role in victim compliance (Baryshevtsev & McGlynn, 2020). These findings further support the concept of social influence in victim compliance with cyber-enabled fraud as a result of the subject matter of the two studies conducted by the researchers. The first study, which involved 169 individuals from a large university in the southwestern United States, uncovered that social engineering emails appealing to the victim's desire to be liked and comply with authority were more successful than schemes that did not. The researchers strengthened the broader applicability of the original findings by conducting a second study involving 149 participants who were recruited via Amazon Mechanical Turk, which uncovered evidence supporting the initial results. These results further support the principle that a potential victim's perception of a perpetrator of a cyber-enabled fraud scheme is an essential component in the victim's compliance with the scheme. This provides additional support for a potential study investigating the role in which a perpetrator's self-esteem (i.e., a perpetrator's confidence in oneself) plays in the decision to victimize others via a cyber-enabled fraud scheme.

These concepts are supported by the findings uncovered in an earlier study, which was conducted via an online survey of 413 female participants from three Chinese universities, to identify a statistically significant relationship existed between social influence and purchase intent (Wahab & Tao, 2019). In fact, researchers found that celebrity status had a substantial impact on purchase intent. Interestingly, the evidence

supported that this included the para-social relationship that exists between social media influencers and followers. The implications of these findings include their applicability to cyber-enabled fraud susceptibility due to exploitation of a victim's need to be understood by bad actors in order to perpetrate the scheme. Given that social influence of a victim's perception of the bad actor may allow for the successful perpetration of a crime, it is important to explore one of the more destructive forms of cyber-enabled fraud schemes, pig butchering scams.

Pig butchering scams, which garner their name from the concept of a pig that is fattened up only to later be slaughtered (Wang & Zhou, 2022), generally result in substantial financial losses and severe psychological harm to victims. Through a qualitative investigation into the most persuasive form of exploitation, researchers found that complex emotional manipulation (e.g., fostering a false sense of intimacy through mirroring and flattery) of the victim was a common element in successful pig butcher schemes. This evidence provides further support for the assertion that the manipulation of the victim's perception of the bad actor is necessary to successfully execute a cyber-enabled fraud scheme. Interestingly, Wang & Zhou (2022) also identified support for the concept that individuals who were lonely were more susceptible to cyber-enabled fraud. Given that more frequent social media usage is indicative of higher levels of loneliness (Lin et al., 2022) and self-esteem is a mediating factor in loneliness (Rossi et al., 2020), these findings provide additional support for the need of a study evaluating the role of self-esteem in both the decision to perpetrate a cyber-enabled fraud scheme and one's susceptibility to exploitation by a bad actor. These findings also indicate that one must explore the additional psychological factors that drive one to perpetrate a cyber-enabled

fraud scheme, such as adequate incentivization (Attrill-Smith & Wesson, 2020; Orjiakor et al., 2022).

Adequate Incentivization.

Given that the three factors that drive cyber-enabled fraudsters were convenience (Bekkers & Leukfeldt, 2022; Buil-Gil & Zeng, 2022; Gottschalk, 2020; Nolasco Braaten & Vaughn, 2021), self-perception (Palmieri et al., 2021; Van Nguyen, 2022; Ye et al., 2019), and complex social structures (Leukfeldt & Holt, 2020), one must consider the common element across these three key themes – the incentives involved in perpetuating a cyber-enabled fraud scheme. The evidence indicates that this may include both social and financial incentives.

In fact, a qualitative study involving interviews of 12 Nigerian men actively perpetrating cyber-enabled fraud schemes found that bad actors were motivated by both financial incentives and group dynamics. While the limited sample size and lack of diversity in the sample make the broader applicability of these findings less reliable, this notion is supported by the broader findings outlined earlier in this chapter.

Additionally, one's drive to meet one's social needs is proven to be a factor in deciding whether or not to engage in cyber-enabled fraud (Attrill-Smith & Wesson, 2020), including one's need to satisfy one's own ego (Geis, 2011; Krancher et al., 2010; Pedneault et al., 2012; as cited in Vousinas, 2019). One could hypothesize that this is a driving factor in the decision to perpetrate cyber-enabled fraud schemes given that low self-control (Blickle et al., 2006) and an over-inflated sense of one's own authority (Aguilera & Vadera, 2008) were evident in male, white-collar offenders. One example of this pursuit involves the role that one's hubris plays in this decision.

Hubris.

Evidence of the social psychological factors influencing the decision to perpetrate cyber-enabled fraud also includes support for the assertion that hubris is a key determinant in one's risk preferences, including one's decision to engage in fraudulent activities (Van Driel, 2018). As a result of the ample scientific evidence that hubris is an important component of the decision to commit criminal acts (Yaksic, 2020), including fraud (Sharma & Aggarwal, 2022), it is unsurprising that individuals have a negative perception of individuals who are perceived to have hubris (Sundermeier & Kummer, 2022). These findings underscore the importance of understanding the psychological factors that influence the decision to perpetrate cyber-enabled fraud by also signaling the importance that perception management plays in the ultimate success of the cyber-enabled fraud scheme once it is perpetrated. Given that one could argue that hubris is essentially one's attitude towards oneself, which is synonymous with self-esteem (Greenhaus & Callanan, 2006), the evidence additionally suggests that self-esteem may be a substantial variable in the decision to perpetrate cyber-enabled fraud.

Biblical Foundations of the Study

There are three key theological principles that create the foundation of this study and inform all relevant constructs. These are one's callings to abstain from crime, remain wary of the dangers associated with greed, and treat others in a just way.

The calling to act in accordance with laws encompasses more than simply a focus on the laws of man (*New International Version Bible*, 1978/2011, Romans 13:1-4). One of the most prominent callings to refrain from perpetrating cyber-enabled fraud is the belief that one must respect the property of others (Exodus 20:15). One is also called to

appreciate the inevitable difficulties of life and retain one's strength by retaining one's resolve in one's pursuit of Him (John 16:33), which includes ceasing activities such as stealing and instead engaging with others in a generous way (Ephesians 4:28). While engaging in cyber-enabled fraud may provide one with short-term benefits, one is also called to appreciate that such unlawful behavior ultimately ends in adverse consequences (Proverbs 10:2).

The sentiment that engaging in cyber-enabled fraud ultimately results in negative repercussions is a testament to the second theological principle informing the proposed study – greed is dangerous (*New International Version Bible,* 1978/2011, Proverbs 1:19). This includes the warning against the pursuit of material goods as a means to obtain fulfillment (Luke 12:15). This is because greed can lead people to engage in unholy behaviors (1 Timothy 6:10), such as perpetrating cyber-enabled fraud schemes. Ultimately, the manifestation of these pursuits is never-ending given that greed is an insatiable beast (Ecclesiastes 5:10).

The final tenant of the theological support for the proposed study involves one's calling to interact with others in a just way (*New International Version Bible*, 1978/2011, Micah 6:8). Given that one is judged by Him on the merit of their actions rather than their socioeconomic status (Proverbs 28:6), the theological evidence clearly supports that the pursuit of justice is a worthwhile calling due to the fact that the provisioning of justice is a means to honor Him (Proverbs 21:15). This is because of one's responsibility to engage in activities which protect those who cannot protect themselves (Psalm 82:3), including the disadvantaged (Proverbs 22:7). In the context of business and financial transactions, this notion is reiterated in the principle that wealth earned through diligence and just

ways is more worthwhile than wealth accumulated fraud (Proverbs 13:11), which will severely impact oneself, family, and community (Proverbs 15:27).

Summary

As evidenced in the preceding sections of this chapter, there is a substantial gap in current literature related to the binary approach that researchers currently take to the topic of cyber-enabled fraud susceptibility. This is due to the evaluation of either a participant's susceptibility to exploitation or inclination to exploit others. No evidence could be identified of a study that investigated what psychological factors, if any, may cause an individual to shift between these two outcomes.

This study was additionally rooted in ample theological support related to three key principles derived from scripture. These include one's callings to behave lawfully, remain wary of greed, and engage with others in a just way.

Based on the gestalt of literature reviewed, the appropriate variables for the study were identified to be self-esteem, financial egocentrism, and fraud susceptibility. Self-esteem and financial egocentrism are appropriate variables for this analysis given the apparent applications of each of these variables as they relate to both one's susceptibility to fraud and one's propensity to commit fraud.

CHAPTER 3: RESEARCH METHOD

Overview

In order for this study to bridge the identified gap in current research, precise methodology was required to collect the appropriate scientific evidence that is needed. This necessitated a complex research design, an identification of an appropriate sample size of 246 participants through an a priori power analysis, detailed participant recruitment information, nuanced procedures to replicate the study, information concerning the appropriate measures and variables that were incorporated into the study, how the identified variables were operationalized, the way in which collected data are to be analyzed, and identified delimitations, assumptions, and limitations of the proposed study.

Research Questions and Hypotheses

Research Questions

RQ1: Does a relationship between financial egocentrism, as measured by a modified version of the trust game (Berg et al., 1995), and fraud susceptibility, as measured by the Brief version of the Susceptibility-to-Persuasion II Scale (StP-II-B)(Modic et al., 2018), exist in participants given their self-esteem level, as measured by the Rosenberg Self-Esteem Scale (Rosenberg, 1965)?

RQ2: How do financial egocentrism, fraud susceptibility, and self-esteem predict the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets in simulated situations?

RQ3: How do financial egocentrism, self-esteem, and the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets in a simulated situation relate to fraud susceptibility?

RQ4: How does the threat of punishment, as measured by the explicit threat of punishment, the explicit statement that there is no punishment, and no statement either way, predict the decision to perpetrate cyber-enabled fraud schemes involving crypto assets in simulated situations?

Hypotheses

Research Hypothesis 1: A statistically significant difference exists between financial egocentrism across the identified levels of self-esteem.

Null Hypothesis 1: A statistically significant difference does not exist between financial egocentrism and self-esteem.

Research Hypothesis 2: Higher self-esteem is associated with a lower level of fraud susceptibility and a higher level of financial egocentrism.

Null Hypothesis 2: Higher self-esteem is not associated with a lower level of fraud susceptibility and a higher level of financial egocentrism.

Hypothesis 3: The threat of punishment is an effective deterrent in the perpetration of cyber-enable fraud schemes involving crypto assets.

Null Hypothesis 3: The threat of punishment is not an effective deterrent in the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets.

Research Design

This quantitative study was designed to investigate the potential association between self-esteem, financial egocentrism, and fraud susceptibility as they relate to

cyber-enabled fraud schemes involving crypto assets. It was predicted that individuals with higher financial egocentrism will also possess higher levels of self-esteem. It was also predicted that higher levels of self-esteem will be associated with lower levels of fraud susceptibility and higher levels of financial egocentrism. The secondary analysis of this study experimentally tested if the threat of punishment was an effective deterrent of cyber-enabled fraud schemes involving crypto assets. The design of this study was appropriate to test the selected hypotheses. This study provided valuable scientific evidence to bridge the identified gap in current literature.

Participants

A priori Power Analysis

An initial alpha was selected as 0.05. This alpha level was selected as a result of the adequate balance that 0.05 provides between Type I and Type II errors when there is a limited selection of related studies previously conducted by researchers (Martin & Bridgmon, 2012, p. 139). The a priori power minimum effect was set to 0.8. Given that this is the ideal level to balance the risk of errors, this effect size was the appropriate estimate for use in the proposed study (Serdar et al., 2021).

The anticipated effect size was estimated to be 0.20 based on evidence collected in five previously conducted studies. The first of these was a study that was conducted by McCannon et al. (2016) investigating the Trust game, which was initially established by Berg et al. (1995). In this study, researchers established a large effect of overconfidence on investment decision-making ($\eta 2 = .154$) in a sample of 95 participants. In a study involving 50,715 participants that examined the impact of perceived financial literacy on actual financial literacy, researchers found a small effect size ($\eta 2 = .010$) (Sanchez &

Dunning, 2018). Researchers also examined the individual efficacy in identifying fraudulent schemes in a study with 100 participants in order to identify a small effect size ($\eta 2 = 0.034$) of confidence on one's accuracy in identifying emails related to cyber-enabled fraud (O'Connor et al., 2021). The weighted sample size average eta-squared of these three studies was 0.01316, which was converted to Cohen's f statistic and equaled 0.102085. A fourth study, which explored the relationship between emotional arousal and fraud susceptibility in 231 participants, was identified using a medium predicted effect size (f = .25) (Kircanski et al., 2018). The fifth study incorporated into the analysis investigated the relationship between beginner overconfidence in financial decision-making using a sample of 40 participants and a moderate estimated effect size (d = 0.5) (Sanchez & Dunning, 2018). This was converted to a medium predicted effect size (f = .25). These three f values were averaged together to identify the appropriate medium estimated effect size (f = 0.20).

All of these values were incorporated into the a priori power analysis using G*Power (Version 3.1.9.7; See Appendix A), which allowed for the necessary sample size of 246 participants to be calculated.

Participant Recruitment

Participants of the study were primarily recruited online. A convenience sample of participants was recruited via social media posts. A random sample of participants was also recruited via a global platform designed for academic researchers to access vetted participants. These forms of recruitment were appropriate given the requirement for a diverse sample to strengthen the broader applicability of any identified findings and the

global distribution of participants. Participants were offered payment for their participation in the study.

Given the use of deception in the study and various other factors, 334 participants, a larger sample than needed, were recruited to account for potential attrition. The inclusion criteria for participation in the study included positive attestation that the individual was age 18 or older and that the participant does not live in the European Union. This criteria was enforced through the criteria set on the global platform.

Study Procedures

The posting soliciting potential respondents included an outline of the time commitment for participation in the study and link to electronically participate (See Appendix B). Once participants clicked on the link, they were redirected to a web survey form wherein each individual was initially prompted to provide consent to participate in the study through a Study Information Sheet (APA, 2017; See Appendix C). After consenting to participate, participants completed the StP-II-B (Modic et al., 2018), the RSES (Rosenberg, 1969), and one demographic question (See Appendix D). Participant scores were electronically logged through the online survey platform that was leveraged to conduct the study. Based on the scores that each individual obtained during this portion of the study, each individual was assigned to a specific group within each variable.

After completing the survey portion of the study, participants were prompted with a pop-up notification providing instructions for completing the crypto asset investing game (See Appendix E). This notification included a description of the objective of the game, which was for participants to attempt to obtain the highest score that the individual

was comfortable achieving over 10 rounds. Each of these scenarios directly related to the decision to perpetrate a cyber-enabled fraud scheme against a fictitious potential victim. Prior to participating in the first scenario, participants were assigned to one of three different punishment scenarios and prompted with one of three statements concerning the use of punishment in the game (See Appendix F).

In response to each scenario prompt, the crypto asset investing game required participants to select a value between one and four, which represented how strongly the participant agreed or disagreed with keeping the investment in that specific scenario. Participant responses in the game were also electronically logged via the online survey platform.

Once each participant completed the last scenario of the game, participants were provided with a message describing the use of deception in the study (See Appendix G). This deceit involved the threat of punishment (i.e., no one was actually caught during the experiment). In adherence with APA guidelines concerning the use of deception, this notification provided participants with the option to request that any data associated with their participation with the study be withdrawn.

Instrumentation and Measurement

This study included three independent variables (self-esteem, fraud susceptibility, and threatened punishment). The solitary dependent variable of the study was financial egocentrism.

Self-esteem

Evidence indicates that self-esteem is an essential component in informing how successfully one navigates various stimuli (Orth & Robins, 2014), including one's

psychological functioning (Kernis, 2005) and self-efficacy (Stets & Burke, 2014). More broadly, research identified that self-esteem impacts one's life satisfaction (Moksnes & Espnes, 2013), including how optimistic and happy one identified themselves to be (Neff & Vonk, 2009). In the context of financial situations, the evidence indicates that self-esteem is linked to one's economic well-being (Twenge & Campbell, 2002).

Interestingly, high levels of self-esteem are linked to known precursors of financial fraud susceptibility and a predisposition to perpetrate a cyber-enabled fraud scheme, including inability to appropriately regulate emotions (Benson & Giacomin, 2020) and control impulses (Wilcox & Stephen, 2013). Unsurprisingly, research also linked high self-esteem to arrogance (Gardner & Pierce, 2011).

In this study, self-esteem was measured using the Rosenberg Self-Esteem Scale ("RSES"; Rosenberg, 1965). The RSES has possible scores between 10 and 40, with a higher score indicating higher self-esteem. Participants were assigned to one of three groups (high, medium, low) based on the score that each individual achieved on the RSES. Given that participants in the study only scored between 20 and 40 on the RSES, a score between 20 and 26 was categorized as low self-esteem. A RSES score between 27 and 33 was categorized as medium self-esteem, and a score between 34 and 40 was categorized as low self-esteem.

Fraud Susceptibility

The evidence indicates that fraud susceptibility is linked to a wide array of psychological traits, including openness (Akdemir & Lawless, 2020; Deliema et al., 2020; Murthy & Gopalkrishnan, 2022) and a greater inclination to trust others (Abdelhamid, 2020). Interestingly, adverse traits associated with fraud susceptibility

include less efficiency in regulation of one's thoughts (Kircanski et al., 2018), impulses (Jones et al., 2019; Palmieri et al., 2021), and expectations of one's abilities (Cheng et al., 2021; Sanchez & Dunning, 2018).

Given that one's susceptibility to fraud victimization is tantamount to one's susceptibility to persuasion, the Brief Susceptibility-to-Persuasion II Scale ("StP-II-B") was used to measure the cyber-enabled fraud susceptibility of each participant (Modic et al., 2018). Participants could achieve StP-II-B scores ranging between 31 and 217, with higher StP-II-B scores indicating higher fraud susceptibility.

Participants were classified in one of three categories based on the StP-II-B score that was achieved. Those whose scores were between 217 and 156 were classified as possessing high fraud susceptibility; those scoring between 155 and 93 as medium fraud susceptibility, and those who scored between 92 and 31 as low fraud susceptibility.

Financial Egocentrism

A person's proclivity to focus solely on themself and outcomes that benefit their own interests without consideration of the perspective of others is defined as egocentrism Piaget, 1951). Evidence indicates that egocentrism is linked to a wide range of negative psychological traits, including overconfidence (Kruger et al., 2005), narcissism (Wink, 1991), and emotional instability (Dambrun, 2017). Given prior evidence linking ego (Aguilera & Vadera, 2008; Geis, 2011; Krancher et al., 2010; Pedneault et al., 2012; as cited in Vousinas, 2019) and impulsivity (Blickle et al., 2006) to the perpetration of white-collar crime, the assertion that egocentrism may play a role in the propensity to pereptrate cyber-enabled fraud is supported by academic literature.

The study evaluated participant financial egocentrism through a modified version of the investment trust game originally established in a study by Berg et al. (1995) and re-

evaluated by McCannon et al. (2016). The modifications to the trust game allowed for the underlying principles of the game to be applied to cyber-enabled fraud involving crypto assets in a study that was electronically conducted. Given that surveys are established to be a reasonable way to control for confounding variables since all participants are asked the same questions (Check & Schutt, 2011, p. 160; Ponto, 2015) and electronically conducted studies are shown to be effective in replicating studies obtained through in-person experiments (Huber & Gajos, 2020), these modifications are appropriate and do not impact the reliability or validity of the concepts established in Berg et al. (1995) by allowing the study to overcome potential problems with data collection such as the college-sophomore problem (Jackson, 2015, p. 243).

The crypto asset investing game consisted of 10 scenarios. Each scenario required the participant to decide whether or not to retain the money that was provided to them under false pretenses by a fictious investor. The participant indicated how strongly they agreed or disagreed with retaining the money from the victim by selecting a value between one and four. Thus, the total potential financial egocentrism score of a participant in the study was between 10 and 40, with a higher score indicating a higher level of financial egocentrism in the participant.

Threatened Punishment

No evidence of a causal relationship between the threat of punishment and deterrence of cyber-enabled fraud schemes was identified. Evidence supporting or opposing the efficacy of threatened punishment as a deterrent to cyber-enabled fraud is

necessary given that white-collar offenders are generally treated less harshly by the media than other types of offenders (Levi, 2009).

Additionally, the evidence indicates that increased regulation typically follows significant financial events (Kurdas, 2009). Given the evolving regulatory landscape surrounding crypto assets, this is an important area of review that should be investigated to examine if a multi-faceted approach to deterrence is a more appropriate form of regulation in the emerging crypto asset market (Middleton, 2009; Rose, 2010).

The threat that one will face an adverse impact as a result of the actions of that participant in the study was evaluated by randomly assigning each participant to one of three groups (no explicit statement concerning punishment is made to participants, an explicit statement threatening punishment is made to participants, and an explicit statement that there is no potential for punishment for participants).

Operationalization of Variables

Self-Esteem – Self-esteem is a dependent, interval variable that was measured using the Rosenberg Self-Esteem Scale ("RSES"), which has possible scores between 10 and 40 with a higher score indicating higher self-esteem (Rosenberg, 1965). Based on their RSES score obtained in this study, participants were assigned to one of three groups: high (34-40), medium (33-27), low (26-20).

Fraud Susceptibility – Fraud susceptibility is a dependent, interval variable that was measured using the Brief version of the Susceptibility to Persuasion II scale (StP-II-B), which has possible scores ranging from 31 to 217 with a higher score indicating a higher

level of susceptibility. Participants were assigned to one of three groups: high (156-217), medium (93-155), low (31-92).

Financial Egocentrism – Financial egocentrism is a dependent, interval variable that was measured using a modified version of the trust game (Berg et al., 1995), which has possible scores ranging from 10 to 40 with a higher score indicating a higher level of financial egocentrism.

Threatened Punishment – Threatened punishment is an independent variable that consisted of three levels (No explicit statement concerning punishment, Explicit statement threatening punishment, Explicit statement that there will not be punishment).

Data Analysis

A 3 x 3 x 3 ANOVA was used to investigate if the between-subjects factors of self-esteem, fraud susceptibility, and the threat of punishment have a statistically significant main effect on financial egocentrism as it related to perpetrating a cyber-enabled fraud scheme involving crypto assets. Given that a statistically significant relationship was identified, Tukey HSD post hoc analysis for fraud susceptibility were conducted.

Since a significant interaction between self-esteem and threat was not identified, each self-esteem level was not examined using a one-way ANOVA. Post hoc analyses was also not conducted to explore if any difference exists between financial egocentrism and threat of punishment.

Delimitations, Assumptions, and Limitations

The key assumption of the study was that participants answered truthfully and behaved in a manner that is representative of how the individual would behave in a real-

world situation. Another assumption of the study was that the collected sample will be representative of the broader population.

A limitation of the study was the applicability of any identified findings to the real-world. In other words, the study examined financial egocentrism in a hypothetical situation and the efficacy of the threat of punishment in a low stakes environment.

Summary

The study answered four research questions through the methods described throughout this chapter. Additionally, an a priori power analysis was conducted to identify that 246 participants were required for the proposed study who were recruited through online platforms, which allowed for a diverse sample of participants that enhanced the applicability of any identified findings to the broader population.

The procedures of the study were outlined in detail in this chapter to allow for replication of the study. By describing the variables of the study, the way in which they were operationalized, and the methods for data analysis in significant detail, future researchers are better positioned to fully digest the findings of the study, which are discussed in detail in the next chapter.

CHAPTER 4: RESULTS

Overview

This quantitative study investigated the role of self-esteem, financial egocentrism, and susceptibility to cyber-enabled fraud schemes involving crypto assets. This was investigated through a series of self-assessments and simulated situations. This study also examined the efficacy of the threat of punishment as a deterrent to perpetrating cyber-enabled fraud schemes involving crypto assets in simulated situations.

A random sample was recruited via online platforms. The number of participants in the study was systematically reduced from 334 total respondents. Respondents were removed from the study for three key reasons. First, 48 respondents completed the study in less than three minutes, which indicated likely bot activity. Second, 26 respondents were removed from the study for failing to complete every item. Lastly, one respondent completed the study in preview mode and was removed from the study for "straight-lining". This left a total of 259 participants in the study, which still exceeded the a priori sample of 246.

Descriptive Results

Participants were asked a single demographic question in the study, which requested the participants to self-identify their gender from four available options. The sample included 139 males, 111 females, six individuals who identified as non-binary/third-gender, and three participants who preferred not to provide a response to this

question (See Table 1). Interestingly, there was no statistically significant relationship between financial egocentrism and gender (See Figure 1).

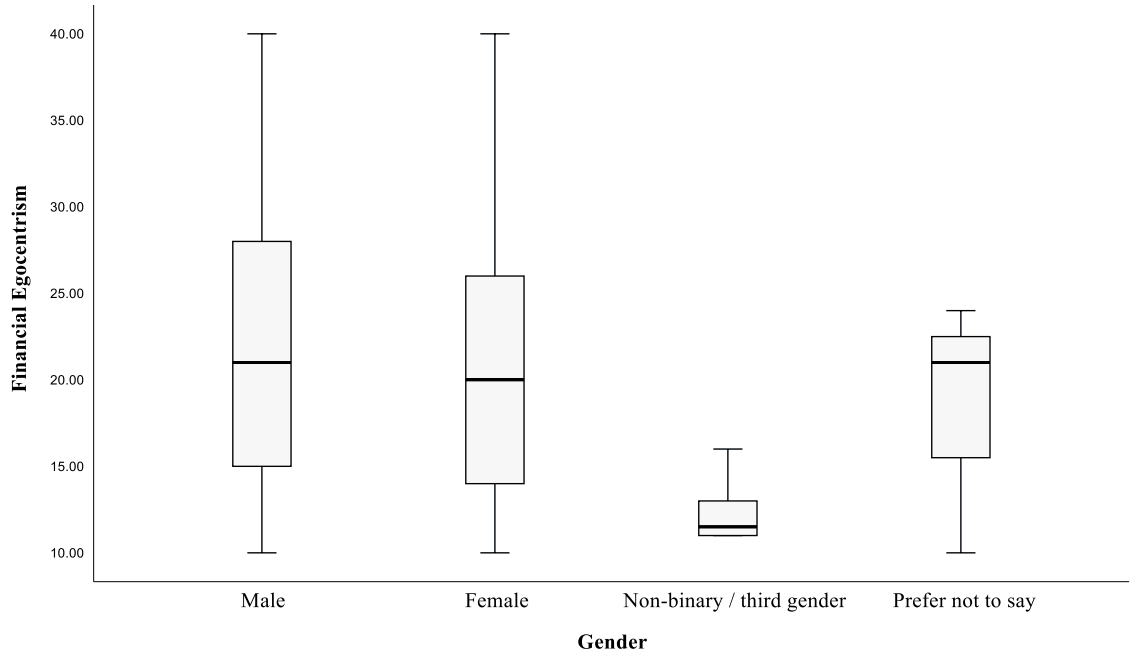
Table 1

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	139	53.7	53.7	53.7
	Female	111	42.9	42.9	96.5
	Non-binary / third gender	6	2.3	2.3	98.8
	Prefer not to say	3	1.2	1.2	100.0
	Total	259	100.0	100.0	

Figure 1

Financial Egocentrism by Gender



Note. The alpha level used was 0.05.

Each participant was randomly assigned to one of three threat scenarios. While the original disbursement of threat scenarios was even across respondents, more

participants were ultimately shown the explicit statement against punishment than the other two scenarios (See Figure 2). No statistically significant impact on financial egocentrism was identified in any of the three threat scenarios (See Figure 3).

Figure 2

Frequency of Threat Scenarios

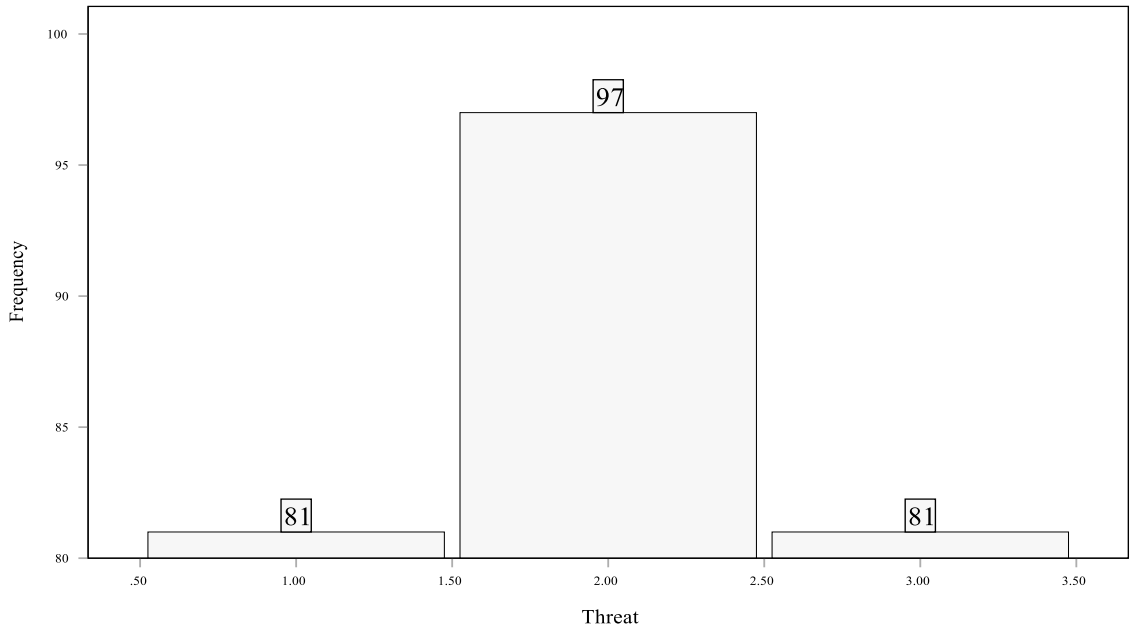
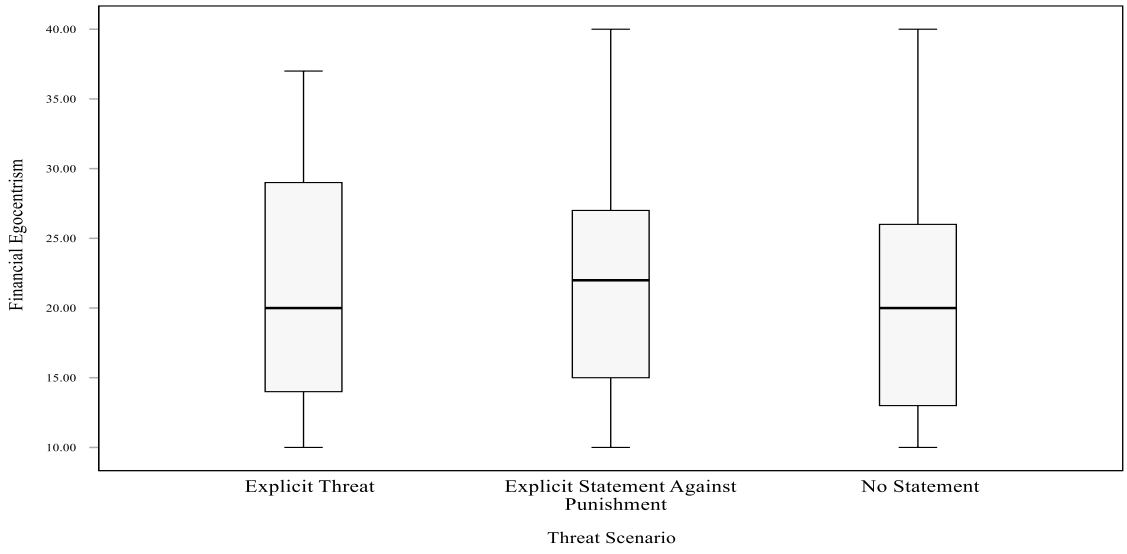


Figure 3

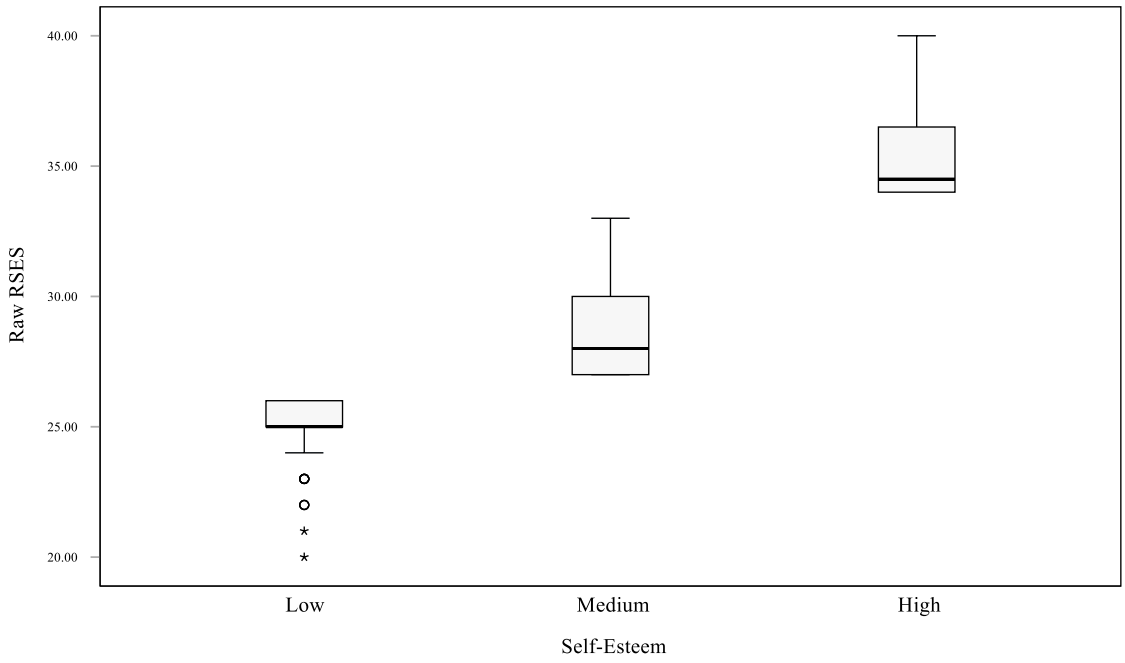
Financial Egocentrism Scores Across Threat Scenarios



Each participant was assigned to one of the three self-esteem groups based on the raw score that the participant achieved on the RSES. Participants who scored between 20 and 26 were assigned to the low self-esteem group. Participants who scored between 27 and 33 were assigned to the medium self-esteem group. Participants who scored between 24 and 40 were assigned to the high self-esteem group. Interestingly, no participants scored between 10 and 20 on the RSES, and the distributions of raw RSES scores between groups were relatively even (See Figure 4).

Figure 4

Raw RSES Score Distributions by Self-Esteem Group



Study Findings

A 3 x 3 x 3 ANOVA was used to investigate if self-esteem, fraud susceptibility, and the threat of punishment had a statistically significant effect on financial egocentrism, as it related to perpetrating cyber-enabled fraud schemes involving crypto assets (See Table 2). A statistically significant main effect of fraud susceptibility

$F(2,3.424) = 17.382$, $p < .001$ was identified (See Figure 5). Tukey HSD post hoc analyses for fraud susceptibility revealed that financial egocentrism increased with fraud susceptibility $p < .001$ (See Table 3).

Table 2

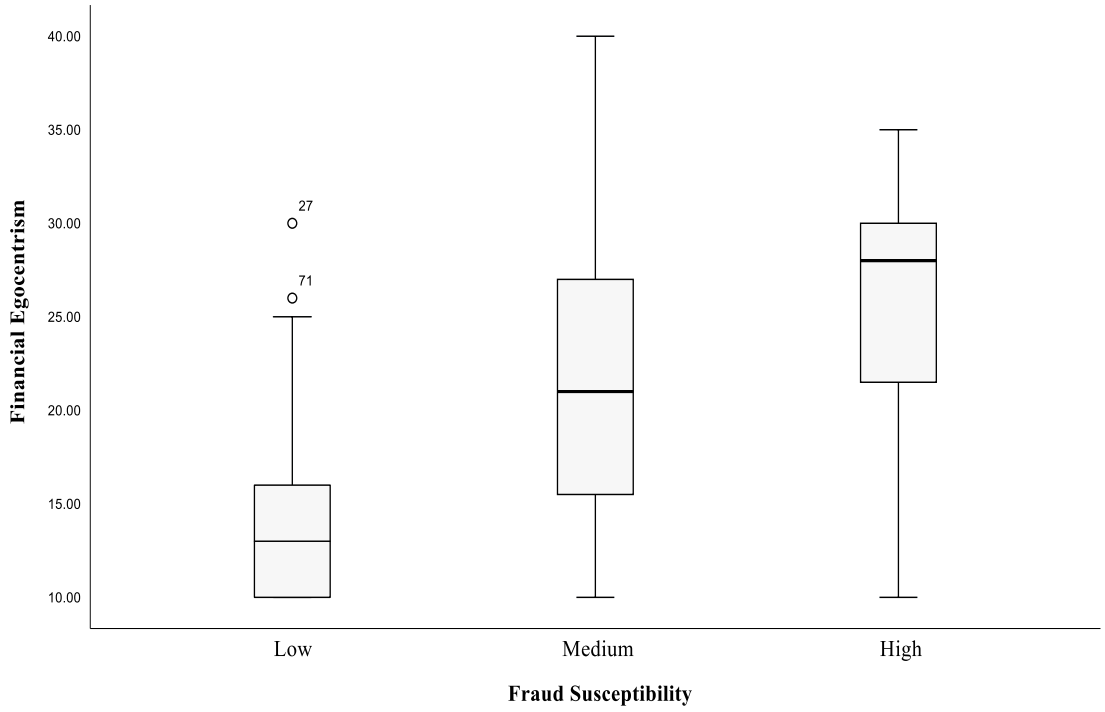
ANOVA Results

Source	Type III Sum of Squares	df	Mean Square	F	Sig.	Partial Eta Squared	Observed Power
Corrected Model	3676.042	22	167.093	3.424	<.001	.242	1.000
Intercept	33298.859	1	33298.859	682.393	<.001	.743	1.000
Threat	30.338	2	15.169	.311	.733	.003	.099
Self_Esteem	201.082	2	100.541	2.060	.130	.017	.422
Fraud_Susceptibility	1696.385	2	848.192	17.382	<.001	.128	1.000
Threat * Self_Esteem	85.193	4	21.298	.436	.782	.007	.152
Threat * Fraud_Susceptibility	318.225	4	79.556	1.630	.167	.027	.498
Self_Esteem * Fraud_Susceptibility	19.040	3	6.347	.130	.942	.002	.074
Threat * Self_Esteem * Fraud_Susceptibility	179.766	5	35.953	.737	.597	.015	.264
Error	11516.143	236	48.797				
Total	128280.000	259					
Corrected Total	15192.185	258					

Note. The alpha level used was 0.05.

Figure 5

Financial Egocentrism by Fraud Susceptibility



Note. The alpha level used was 0.05.

Table 3

Tukey Post Hoc Fraud Susceptibility by Financial Egocentrism

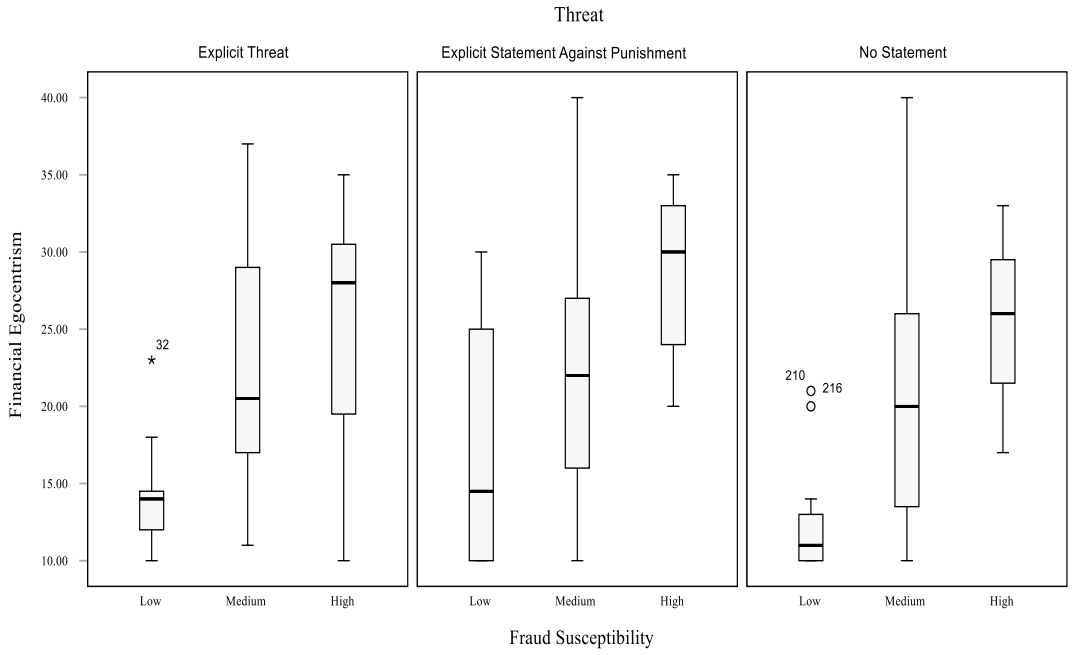
(I) Fraud Susceptibility	(J) Fraud Susceptibility	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
Low	Medium	-6.6133*	1.16490	<.001	-9.3608	-3.8658
	High	-11.4508*	1.57435	<.001	-15.1641	-7.7375
Medium	Low	6.6133*	1.16490	<.001	3.8658	9.3608
	High	-4.8375*	1.29105	<.001	-7.8826	-1.7924
High	Low	11.4508*	1.57435	<.001	7.7375	15.1641
	Medium	4.8375*	1.29105	<.001	1.7924	7.8826

Note. The mean difference is significant at the .05 level.

The secondary analysis conducted in the study revealed that threat of punishment did not have a statistically significant impact on financial egocentrism in simulated situations (See Figure 6).

Figure 6

Financial Egocentrism and Fraud Susceptibility by Threat



Summary

The study investigated the potential relationship and impact that self-esteem, fraud susceptibility, and the threat of punishment had on financial egocentrism as it related to the decision to perpetrate cyber-enabled fraud schemes involving crypto assets. The finding that a significant interaction between fraud susceptibility and financial egocentrism occurred supported one of the main hypotheses of the study. However, the other two research hypotheses of the study were rejected.

The key finding that higher financial egocentrism is related to higher fraud susceptibility is an important finding that was not previously supported by academic

evidence. Additionally, the finding that the threat of punishment, at least in the context of simulated situations, was not an effective deterrent of perpetrating cyber-enabled fraud schemes is another key finding of this study as this is an important consideration for public officials, criminal justice practitioners, and business executives. While the limitations of the study are important to consider, the study provided significant evidence in support of previously unproven relationships as will be discussed in the following chapter.

CHAPTER 5: DISCUSSION

Overview

The rapidly changing digital landscape provides substantial opportunities for exploitation by bad actors. A better understanding of the psychological factors related to cyber-enabled fraud schemes involving crypto assets is an essential first step. This study examined the nuanced relationship between self-esteem, fraud susceptibility, and financial egocentrism in this context in order to identify that a statistically significant relationship between financial egocentrism and fraud susceptibility exists.

Summary of Findings

The conducted study tested three key research hypotheses. First, a statistically significant difference exists between financial egocentrism across the identified levels of self-esteem, which was rejected by the findings of the study. Second, higher self-esteem is associated with a lower level of fraud susceptibility and a higher level of financial egocentrism, which was rejected by the findings of the study. Lastly, that the threat of punishment is an effective deterrent in the perpetration of cyber-enabled fraud schemes involving crypto assets, which was also rejected by the findings of the study. Importantly, a statistically significant relationship between financial egocentrism and fraud susceptibility was uncovered by the study, which is a finding that has not previously been supported by academic evidence.

Discussion of Findings

Identified Findings in an Academic Context

The key finding uncovered in the study is one that makes intuitive sense. Primarily, an individual who is more susceptible to cyber-enabled fraud is more likely to

perpetrate a cyber-enabled fraud scheme involving crypto assets. The reason behind this may be linked to that individual's desire to maximize their financial gain in different situations. Therefore, an individual who possesses higher levels of financial egocentrism may be more susceptible to fraud as a result of the fixation on that individual's own financial gain.

It should be noted that this is not the same as the incorrect notion that is spread through anecdotal evidence across fraud investigations and news stories. By extrapolating on the scientific evidence collected in this study, one could theorize that perhaps individuals are not more susceptible to fraud as a result of selfishness. Rather, the individuals are more susceptible to fraud as a result of self-centeredness, which may be the manifestation of an undue sense of invincibility based on hyper fixation on oneself.

This is an important distinction in this context given that fraud schemes require both a perpetrator and a victim. As uncovered in this study, the individuals who are more likely to be victimized are also the individuals who are more likely to victimize others, which is a notion that aligns with the victim-to-perpetrator cycle of abuse observed across many differing forms of abuse (Bharti et al., 2021; Nurse & Harding, 2023). The relationship between an individual's financial egocentrism and fraud susceptibility is a key finding because of this principle. The collected evidence supports that individual's self-centeredness is a key determinant of both their predisposition to be exploited by others and their propensity to exploit others for financial gain. As a result of the findings uncovered by this study, this previously unexplored area of research is an exciting opportunity for future studies.

Identified Findings in a Biblical Context

The three significant theological ideals on which this study is based are that one is called to abstain from crime (*New International Version Bible*, 1978/2011, Romans 13:1-4; Exodus 20:15; John 16:33; Ephesians 4:28; Proverbs 10:2), remain wary of the dangers of greed (Proverbs 1:19; Luke 12:15; 1 Timothy 6:10; Ecclesiastes 5:10), and treat others in a just way (Micah 6:8; Proverbs 28:6; Proverbs 21:15; Psalm 82:3; Proverbs 22:7; Proverbs 13:11; Proverbs 15:27). The findings uncovered by this study align with these three tenants in a significant way. This is the notion that one's fixation on one's self, without regard to laws or the impact of one's actions on others, will result in harm over the long-term, including the degeneration of one's soul.

Implications

The implications of the findings uncovered by this study are significant both in depth and breadth. Given that individuals who exhibit a higher degree of financial egocentrism also exhibit a higher propensity to be victimized by fraud schemes, the findings of this study exceed simply the academic community. For example, the findings of this study may increase the efficacy of anti-fraud educational programs by enhancing individual's understanding of themselves, which could potentially mitigate the risk that they are victimized by fraudsters. The evidence indicates that enhancing one's awareness of the impact of oneself on others may reduce both one's propensity to victimize others through cyber-enabled fraud schemes involving crypto assets and one's predisposition to be victimized by fraudulent schemes.

The finding that the threat of punishment is not an effective deterrent in the decision to perpetrate a cyber-enabled fraud scheme involving crypto assets is also an important principle with implications for policymakers, criminal justice practitioners, and

business executives. Given that the effectiveness of traditional punitive measures is not supported by the collected evidence, the strategy to the enforcement of cyber-enabled fraud schemes involving crypto assets should be reconsidered. One potential avenue for further exploration is a review of alternative approaches (e.g., education and early prevention efforts). The evidence suggests that a more robust approach to the enforcement of cybercrime laws is needed to mitigate the risks posed by this form of criminal activity.

Limitations

The generalizability of the identified findings to other forms of crime beyond cyber-enabled fraud schemes involving crypto assets is an important limitation of the study. Given the specific focus of the study to this form of crime, there is no evidence that the identified findings could be extrapolated and applied to other forms of crime. Additionally, the use of online platforms to recruit a random sample of participants allowed for the assumption of a diverse sample. However, the inclusion of a single demographic question may have created confounding variables that were not explored in this study.

Additionally, the low-stakes environment in which the study was conducted may also limit the broader applicability of the findings of the study. Individuals who received a threat of punishment (i.e., the loss of points in an online simulation) and perpetrated a cyber-enabled fraud scheme involving crypto assets in the study may not actually engage in cyber-enabled fraud schemes involving crypto assets in a real-world situation due to the more significant implications of the actions of that individual in the real-world, including both incarceration and actually engaging in a crime.

The lack of related studies is another key limitation of this study. Due to the lack of related studies, the findings of this study should not be overstated or overgeneralized. The approach of this study is a ground-breaking way to investigate cyber-enabled fraud schemes involving crypto assets. As a result of this innovative idea, the merits must be strenuously examined and retested by the scientific community to establish the usefulness of the scientific evidence that was uncovered.

Recommendations for Future Research

The scientific evidence uncovered in this unique study provides several opportunities for further research in this area. Primarily, the opportunity for comparative studies into the effectiveness of various educational methods and deterrence practices could provide further insight into the prevention of cyber-enabled fraud schemes involving crypto assets.

Additionally, studies examining the role of technological advancements on egocentrism could provide additional evidence in support of the findings uncovered in this study. This could support the theory that individuals are growing more egocentric as a result of modern society with scientific evidence, which may also explain the increasing prevalence of cyber-enabled fraud schemes.

A study that explores the relationship between financial egocentrism and age could also provide crucial evidence related to fraud susceptibility in older adults. This could provide evidence that provides additional insight into the current theory in fraud susceptibility research that normal cognitive decline is related to increased fraud susceptibility in older adults.

Summary

The study explored a variety of factors that were hypothesized to have a relationship to both fraud susceptibility and financial egocentrism, including if the threat of punishment was an effective deterrent to engaging in cyber-enabled fraud schemes involving crypto assets. The study revealed that higher levels of financial egocentrism were linked to increased susceptibility to fraud, which suggests individuals who exhibit higher levels of self-centeredness have both a higher predisposition to commit cyber-enabled fraud schemes and are more susceptible to fraudulent schemes.

This groundbreaking study provides unique scientific evidence into the research of cyber-enabled fraud schemes involving crypto assets. However, the study is not without its limitations that should be considered when interpreting the collected evidence. The findings uncovered in this study provide useful insights that should be leveraged in future studies in this burgeoning area of research. Moreover, the findings of this study provide a unique perspective into the psychological factors related to cyber-enabled fraud schemes involving crypto assets and the potential gaps in the preventative measures currently leveraged to mitigate criminal activity in this space.

REFERENCES

Abdelhamid, M. (2020). The role of health concerns in phishing susceptibility: Survey design study. *Journal of Medical Internet Research, 22*(5), Article e18394.

Aguilera, R. V., & Vadera, A. K. (2008). The dark side of authority: Antecedents, mechanisms, and outcomes of organizational corruption. *Journal of Business Ethics*, *77*(4), 431-449.

American Psychological Association. (2017). Ethical principles of psychologists and code of conduct (2002, amended effective June 1, 2010, and January 1, 2017).

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665-1687.

Arthur, J. N., & Delfabbro, P. (2017). Day traders in South Australia: Similarities and differences with traditional gamblers. *Journal of Gambling* Studies, 33(3), 855-866.

Asp, E., Manzel, K., Koestner, B., Cole, C. A., Denburg, N. L., & Tranel, D. (2012). A neuropsychological test of belief and doubt: damage to ventromedial prefrontal cortex increases credulity for misleading advertising. *Frontiers in Neuroscience*, *6*, Article 100.

Aquino, A., Alparone, F. R., Pagliaro, S., Haddock, G., Maio, G. R., Perrucci, M. G., & Ebisch, S. J. H. (2020). Sense or sensibility? the neuro-functional basis of the structural matching effect in persuasion. *Cognitive, Affective, & Behavioral Neuroscience*, *20*(3), 536-550.

Australian Securities and Investments Commission. (2021). Scam alert: ASIC sees a rise in crypto scams. https://asic.gov.au/about-asic/news-centre/news-items/scam-alert-asicsees-a-rise-in-crypto-scams/

Attrill-Smith, A., & Wesson, C. (2020). The psychology of cybercrime. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 653-678.

Baker, S. A., & Rojek, C. (2020). The Belle Gibson scandal: The rise of lifestyle gurus as micro-celebrities in low-trust societies. *Journal of Sociology*, *56*(3), 388-404.

Baryshevtsev, M., & McGlynn, J. (2020). Persuasive appeals predict credibility judgments of phishing messages. *Cyberpsychology, Behavior, and Social Networking*, *23*(5), 297-302.

Benson, A. J., & Giacomin, M. (2020). How self-esteem and narcissism differentially relate to high and (un) stable feelings of status and inclusion. *Journal of Personality*, *88*(6), 1177- 1195.

Berg, J., Dickhaut, J., & McCabe, K. (1995). Trust, reciprocity, and social history. *Games and Economic Behavior*, *10*(1), 122-142.

Blanco, F., Matute, H., & Vadillo, M. A. (2011). Making the uncontrollable seem controllable: The role of action in the illusion of control. *The Quarterly Journal of Experimental Psychology*, *64*(7), 1290-1304.

Blickle, G., Schlegel, A., Fassbender, P., & Klein, U. (2006). Some personality correlates of business white-collar crime. *Applied Psychology*, *55*(2), 220-233.

Buil-Gil, D., & Zeng, Y. (2022). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*, *29*(2), 460-475.

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2021). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimization: A realist review. *Experimental Gerontology,* Article 111678.

Button, M., & Cross, C. (2017). Technology and Fraud: The 'Fraudogenic'consequences of the Internet revolution. In *The Routledge handbook of technology, crime and justice* (pp. 78-95). Routledge.

Check, J., & Schutt, R. K. (2011). *Research methods in education.* Sage Publications.

Chen, F. X., Zhang, X., Laustsen, L., & Cheng, J. T. (2021). Harsh but expedient: Dominant leaders increase group cooperation via threat of punishment. *Psychological Science*, *32*(12), 2005-2022.

Cheng, J. T., Anderson, C., Tenney, E. R., Brion, S., Moore, D. A., & Logg, J. M. (2021). The social transmission of overconfidence. *Journal of Experimental Psychology: General*, *150*(1), 157–186.

Coinmarketcap. (2023). Market Cap [Data]. https://coinmarketcap.com/

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health*, *16,* Article 24.

Dambrun, M. (2017). Self-centeredness and selflessness: happiness correlates and mediating psychological processes. *PeerJ, 5*, Article e3306.

Dearden, T. E., & Scaptura, M. (2023). Can institutional anomie theory predict victimization? An experimental survey examining institutional anomie and affinity fraud. *Journal of Financial Crime*, *30*(4), 1006-1020.

DeLiema, M., Li, Y., & Mottola, G. R. (2021). Correlates of compliance: Examining consumer fraud risk factors by scam type. *Social Science Research Network*, Article 3793757.

Deliema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. *Journal of Consumer Research*, *46*(5), 904-914.

Eaton, T. V., & Korach, S. (2016). A criminological profile of white-collar crime. *Journal of Applied Business Research, 32*(1), 129-142.

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., ... & Oliveira, D. S. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B, 75*(3), 522-533.

Esmaeili, L., & Golpayegani, A. H. (2020). Conformance checking of the activity network with the social relationships structure in the context of social commerce. *Journal of Theoretical and Applied Electronic Commerce Research*, *15*(2), 93-121.

Faber, L. G., Maurits, N. M., & Lorist, M. M. (2012). Mental fatigue affects visual selective attention. *PloS One*, *7*(10), e48073.

Federal Bureau of Investigation. (2023) Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Financial Conduct Authority. (2019). Cryptoasset investment scams. https://www.fca.org.uk/scamsmart/cryptoasset-investment-scams

Financial Industry Regulatory Authority (FINRA) Investor Education Foundation. (2023). Gen Z and Investing: Social Media, Crypto, FOMO, and Family.

https://www.finrafoundation.org/sites/finrafoundation/files/Gen-Z-and-Investing.pdf

Fiske, S., & Taylor, S. E. (2021). *Social cognition: From brains to culture* (4th.). Thousand Oaks, CA: Sage Publications, Inc.

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, *94*, Article 101862.

Gardner, D. G., & Pierce, J. L. (2011). A question of false self-esteem: Organization-based self-esteem and narcissism in organizational contexts. *Journal of Managerial Psychology, 26*(8), 682-699.

Gottschalk, P. (2020) Modeling the Theoretical Structure of Deviant Convenience in White Collar Crime, *Deviant Behavior*, *42*(11), 1345-1365.

Greenhaus, J. H., & Callanan, G. A. (2006). Self-esteem. In *Encyclopedia of Career Development* (Vol. 1, pp. 723-727). SAGE Publications, Inc.

Handgraaf, M. J., Van Dijk, E., Vermunt, R. C., Wilke, H. A., & De Dreu, C. K. (2008). Less power or powerless? Egocentric empathy gaps and the irony of having little versus no power in social decision making. *Journal of Personality and Social Psychology*, *95*(5), 1136.

Hanoch, Y., & Wood, S. (2021). The scams among us: Who falls prey and why. *Current Directions in Psychological Science*, *30*(3), 260-266.

Houben, R., & Snyers, A. (2020). Crypto-assets: Key developments, regulatory concerns and responses. *Policy Department for Economic, Scientific and Quality of Life*

Policies, Directorate-General for Internal Policies, European Parliament, 648, 13.

Huber, B., & Gajos, K. Z. (2020). Conducting online virtual environment experiments with uncompensated, unsupervised samples. *Plos one, 15*(1), e0227629.

Jackson, S. L. (2015). *Research methods and statistics: A critical thinking approach (5th ed.)*. Boston, MA: Cengage Learning.

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PloS One*, *14*(1), Article e0209684.

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in Psychology*, *8*, Article 588.

Kamps, J., & Kleinberg, B. (2018). To the moon: Defining and detecting cryptocurrency pump-and-dumps. *Crime Science, 7*(1), 18.

Kahneman, D. (2011). *Thinking, Fast and Slow*. London: Macmillan.

Kernis, M. H. (2005). Measuring self-esteem in context: The importance of stability of self-esteem in psychological functioning. *Journal of Personality, 73*(6), 1569-1605.

Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola, G., ... & Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and Aging*, *33*(2), 325.

Koestner, B. P., Hedgcock, W., Halfmann, K., &Denburg, N. L. (2016). The role of the ventromedial prefrontal cortex in purchase intent among older adults. *Frontiers in Aging Neuroscience*, *8*, Article 189.

Kruger, J., Epley, N., Parker, J., & Ng, Z.-W. (2005). Egocentrism over e-mail: Can we communicate as well as we think? *Journal of Personality and Social Psychology*, *89*(6), 925–936.

Kurdas, C. (2009). Does regulation prevent fraud? The case of Manhattan hedge fund. *The Independent Review*, *13*(3), 325–343.

Levi, M. (2009). Suite revenge? The shaping of folk devils and moral panics about white-collar crimes. *The British Journal of Criminology*, *49*(1), 48–67.

Lichtenberg, P. A., Campbell, R., Hall, L., & Gross, E. Z. (2020). Context matters: Financial, psychological, and relationship insecurity around personal finance is associated with financial exploitation. *The Gerontologist, 60*(6), 1040-1049.

Lin, S., Liu, D., Niu, G., & Longobardi, C. (2022). Active social network sites use and loneliness: The mediating role of social support and self-esteem. *Current Psychology*, *41*(3), 1279-1286.

Martin, W.E. & Bridgmon, K.D. (2012). *Quantitative and Statistical Research Methods: From Hypothesis to Results*, Hoboken, NJ: Wiley Jossey-Bass.

Martin, B. A., Chrysochou, P., Strong, C., Wang, D., & Yao, J. (2022). Dark personalities and Bitcoin®: The influence of the Dark Tetrad on cryptocurrency attitude and buying Intention. *Personality and Individual Differences, 188*, Article 111453.

Marson, D. C., & Sabatino, C. P. (2012). Financial capacity in an aging society. *Generations: Journal of the American Society on Aging*, *36*(2), 6–11.

McCannon, B. C., Asaad, C. T., & Wilson, M. (2016). Financial competence, overconfidence, and trusting investments: Results from an experiment. *Journal of Economics and Finance, 40*(3), 590-606.

McDowell, J., & Woods, J. (2022). *An Introductory Explanation of Cryptocurrencies* [White paper]. InfraGard Blockchain Cross Sector Council.

McGregor, I., & Jordan, C. H. (2007). The mask of zeal: Low implicit self-esteem, threat, and defensive extremism. *Self and Identity*, *6*(3), 223-237.

Middleton, D. J. (2005). The legal and regulatory response to solicitors involved in serious fraud: Is regulatory action more effective than criminal prosecution? *The British Journal of Criminology*, *45*(6), 810–836.

Modic, D., Anderson, R., & Palomäki, J. (2018). We will make you like our research: The development of a susceptibility-to-persuasion scale. *PloS one*, *13*(3), Article e0194119.

Mohammed, A. M., Benson, V., & Saridakis, G. (2020). Understanding the relationship between cybercrime and human behavior through criminological theories and social networking sites. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 979-989). IGI Global.

Moksnes, U. K., & Espnes, G. A. (2013). Self-esteem and life satisfaction in adolescents— gender and age as potential moderators. *Quality of Life Research*, *22*(10), 2921-2928.

Mueller, E. A., Wood, S. A., Hanoch, Y., Huang, Y., & Reed, C. L. (2020). Older and wiser: age differences in susceptibility to investment fraud: the protective role of emotional intelligence. *Journal of Elder Abuse & Neglect*, *32*(2), 152-172.

Murthy, N., & Gopalkrishnan, S. (2022). Does openness increase vulnerability to digital frauds? Observing social media digital footprints to analyze risk and legal factors for banks. *International Journal of Law and Management*, *6*(4), 368-387.

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences, 169*, Article 109847.

Neff, K. D., & Vonk, R. (2009). Self-compassion versus global self-esteem: Two different ways of relating to oneself. *Journal of Personality*, *77*(1), 23-50.

New International Version Bible. (2011). Biblica. https://www.biblica.com/online-bible (Original work published 1978).

Nolasco Braaten, C., & Vaughn, M. S. (2021). Convenience theory of cryptocurrency crime: A content analysis of US federal court decisions. *Deviant Behavior, 42*(8), 958-978.

O'Connor, A. M., Judges, R. A., Lee, K., & Evans, A. D. (2021). Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience. *Journal of Elder Abuse & Neglect, 33*(3), 181-205.

Orjiakor, C. T., Ndiwe, C. G., Anwanabasi, P., & Onyekachi, B. N. (2022). How do internet fraudsters think? A qualitative examination of pro-criminal attitudes and cognitions among internet fraudsters in Nigeria. *The Journal of Forensic Psychiatry & Psychology*, 1-17.

Orth, U., & Robins, R. W. (2014). The Development of Self-Esteem. *Current Directions in Psychological Science*, *23*(5), 381–387.

Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior, 120*, 106745.

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, *128*, 17-26.

Piaget, J. (1951). *The child's conception of the world* (Vol. 213). Lanham, MD: Rowman & Littlefield.

Ponto J. (2015). Understanding and Evaluating Survey Research. *Journal of the advanced practitioner in oncology*, *6*(2), 168–171.

Raimundo Júnior, G. de S., Palazzi, R. B., de Souza Tavares, R., & Klotzle, M. C. (2022). Market stress and herding: A new approach to the cryptocurrency market. *Journal of Behavioral Finance*, *23*(1), 43–57.

Rose, A. M. (2010). The multienforcer approach to securities fraud deterrence: A critical analysis. *University of Pennsylvania Law Review*, *158*(7), 2173–2231.

Rosenberg, M. (1965). Rosenberg self-esteem scale (RSE). *Acceptance and Commitment Therapy Measures Package*, *61*(52), 18.

Sanchez, C., & Dunning, D. (2018). Overconfidence among beginners: Is a little learning a dangerous thing? *Journal of Personality and Social Psychology*, *114*(1), 10–28.

Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and Applied Social Psychology*, *36*(3), 272-279.

Serdar, C. C., Cihan, M., Yücel, D., & Serdar, M. A. (2021). Sample size, power and effect size revisited: simplified and practical approaches in pre-clinical, clinical and laboratory studies. *Biochemia Medica*, *31*(1), 27-53.

Sharma, N. J., & Aggarwal, D. (2022). YES Bank Fraud: Examining the softer underbelly of the fraud from a behavioral model. *Journal of Forensic Accounting Research*, *7*(1), 133-150.

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*, 342-361.

Speer, S. P. H., Smidts, A., & Boksem, M. A. S. (2022). Individual differences in (dis)honesty are represented in the brain's functional connectivity at rest. *NeuroImage, 246*, Article 118761.

Steinmetz, K. F. (2021). The Identification of a model victim for social engineering: A qualitative analysis. *Victims & Offenders*, *16*(4), 540-564.

Steinmetz, K. F., Pimentel, A., & Goe, W. R. (2021). Performing social engineering: A qualitative study of information security deceptions. *Computers in Human Behavior*, *124*, Article 106930.

Steinmetz, K. F., Schaefer, B. P., Brewer, C. G., & Kurtz, D. L. (2023). The Role of Computer Technologies in Structuring Evidence Gathering in Cybercrime Investigations: A Qualitative Analysis. *Criminal Justice Review*, *2023*, 1-18.

Stets, J. E., & Burke, P. J. (2014). Self-esteem and identities. *Sociological Perspectives*, *57*(4), 409-433.

Sudzina, F., Dobes, M., & Pavlicek, A. (2021). Towards the psychological profile of cryptocurrency early adopters: Overconfidence and self-control as predictors of cryptocurrency use. *Current Psychology, 40*(8).

Sur, A., DeLiema, M., & Brown, E. (2021). Contextual and social predictors of scam susceptibility and fraud victimization. *Social Science Research Network.* Article 4053903.

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science, 11*(1), 1-35.

Twenge, J. M., & Campbell, W. K. (2002). Self-esteem and socioeconomic status: A metaanalytic review. *Personality and Social Psychology Review, 6*(1), 59-71.

Van Driel, H. (2018). Financial fraud, scandals, and regulation: A conceptual framework and literature review. *Business History*, *61*(8), 1259-1299.

Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime, 25*(2), 226-247.

Vousinas, G. L. (2019). Advancing theory of fraud: the SCORE model. *Journal of Financial Crime, 26*(1), 372-381.

Wahab, H. K. A., & Tao, M. (2019). The Influence of Internet Celebrity on Purchase Decision and Materialism: The Mediating Role of Para-social Relationships and Identification. *European Journal of Business and Management*, *11*(15), 183-199.

Wang, C. (2022). Online Dating Scam Victims Psychological Impact Analysis. *Journal of Education, Humanities and Social Sciences*, *4*, 149-154.

Wang, F., & Zhou, X. (2022). Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan (杀猪盘) in China. *Victims & Offenders*, 1-28.

Wang, X., Ma, J., Liang, Y., Ma, L., & Liu, P. (2023). The association between experiences of being defrauded and depressive symptoms of middle-aged and elderly people: a cross-sectional study in China. *Public Health*, *216*, 51-57.

Wang, Y., Stuart, T., & Li, J. (2021). Fraud and innovation. *Administrative Science Quarterly*, *66*(2), 267-297.

Wei, R., Liu, X. S., & Liu, X. (2019). Examining the perceptual and behavioral effects of mobile internet fraud: A social network approach. *Telematics and Informatics*, *41*, 103-113.

Wen, J., Yang, H., Zhang, Q., & Shao, J. (2022). Understanding the mechanisms underlying the effects of loneliness on vulnerability to fraud among older adults. *Journal of Elder Abuse & Neglect*, *34*(1), 1-19.

White, J. T., & Wilkoff, S. (2023). The Effect of Celebrity Endorsements on Crypto: Evidence from Initial Coin Offerings (ICOs). *Social Science Research Network.* Article 4380845.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277-292.

Wilcox, K., & Stephen, A. T. (2013). Are close friends the enemy? Online social networks, selfesteem, and self-control. *Journal of Consumer Research*, *40*(1), 90-103.

Wink, P. (1991). Two faces of narcissism. *Journal of Personality and Social Psychology*, *61*(4), 590–597.

Xu, L., Wang, J., Xu, D., & Xu, L. (2022). Integrating individual factors to construct recognition models of consumer fraud victimization. *International Journal of Environmental Research and Public Health, 19*(1), Article 461.

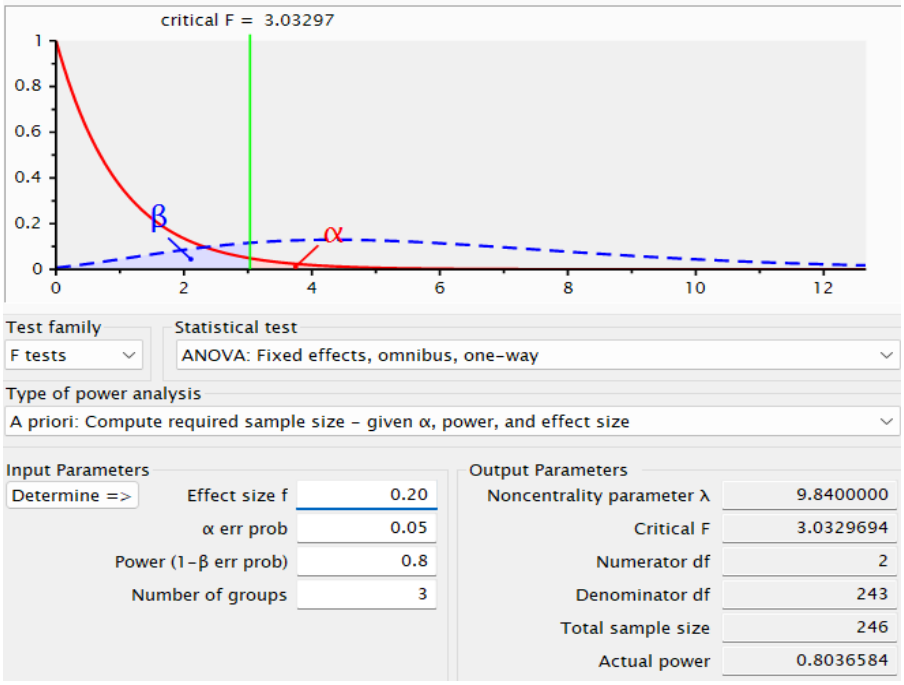
Yaksic, E. (2020). Evaluating the use of data-based offender profiling by researchers, practitioners and investigative journalists to address unresolved serial homicides. *Journal of Criminal Psychology, 10*(2), 123-144.

Ye, N., Cheng, L., & Zhao, Y. (2019). Identity construction of suspects in telecom and internet fraud discourse: from a sociosemiotic perspective. *Social Semiotics, 29*(3), 319-335.

Zebrowitz, L. A., Ward, N., Boshyan, J., Gutchess, A., Hadjikhani, N., Gillberg Neuropsychiatry Centre, Sahlgrenskaakademin, Göteborgsuniversitet, Gothenburg University, Gillbergcentrum, &Sahlgrenska Academy. (2018). Older adults' neural activation in the reward circuit is sensitive to face trustworthiness. *Cognitive, Affective, & Behavioral Neuroscience, 18*(1), 21-34.

Ziyadin, S., Doszhan, R., Borodin, A., Omarova, A., & Ilyas, A. (2019). The role of social media marketing in consumer behaviour. *Innovative Technologies in Environmental Science and Education, 135,* Article 04022.

APPENDIX A: G*POWER SCREENSHOT



APPENDIX B: TEXT OF PARTICIPANT RECRUITMENT POST

ATTENTION SOCIAL MEDIA CONTACTS: I am conducting research as part of the requirements for a Ph.D. at Liberty University. The purpose of my research is to investigate cyber-enabled fraud involving crypto assets. To participate, you must be 18 years or older and cannot be a resident of the European Union. Participants will be asked to complete a series of survey questions and an investing game, which should take about 15 minutes to complete. If you would like to participate and meet the study criteria, please click the link at the end of this post. A Study Information Sheet is provided as the first page of the survey. Participants who complete the study will be eligible to receive a $5 Visa Gift Card.

To take the survey, click here: [LINK].

APPENDIX C: STUDY INFORMATION SHEET

Title of the Project: Exploring the Relationship Between Self-Esteem, Financial Egocentrism, and Fraud Susceptibility in Cyber-Enabled Fraud Schemes Involving Crypto Assets.

Principal Investigator: James McDowell, Doctoral Candidate, Psychology Department, Liberty University

Invitation to be Part of a Research Study

You are invited to participate in a research study. You were selected as a possible participant because you are over the age of 18 and are not a resident of the European Union. Taking part in this research project is voluntary.

Please take time to read this entire form and ask questions before deciding whether to take part in this research.

What is the study about and why is it being done?

The purpose of the study is to explore the potential relationship between self-esteem, financial egocentrism, and fraud susceptibility in cyber-enabled fraud schemes involving crypto assets.

What will happen if you take part in this study?

If you agree to be in this study, I will ask you to do the following:

1. Complete an online survey providing demographic information, and information investigating your self-esteem, financial egocentrism, and fraud susceptibility. This will take about 10 minutes.
2. Complete an online game simulating 10 scenarios involving crypto asset investment schemes. This will take about 5 minutes.

How could you or others benefit from this study?

Participants in this study should not expect to receive any direct benefit from participation in this study. The benefits to society that may result from this study include enhancing the understanding of cyber-enabled fraud and the psychological factors that may influence one's predisposition to perpetrate cyber-enabled fraud and one's propensity to be victimized by bad actors perpetrating cyber-enabled fraud schemes.

What risks might you experience from being in this study?

The expected risks involved in this study are minimal, which means they are equal to the risks you would encounter in everyday life.

How will personal information be protected?

The records of this study will be kept private. Research records will be stored securely, and only the researcher and faculty sponsor will have access to the records. Participant responses will be anonymous. Data will be stored on a password locked computer. After three years, all electronic records will be deleted.

How will you be compensated for being part of the study?

Participants will be compensated for participating in this study.

At the conclusion of the survey participants not recruited via Amazon Mechanical Turk (MTurk) will be eligible to receive a $5 Visa Gift card. Email addresses will be requested for compensation purposes; however, they will be collected by email at the conclusion of the survey to maintain your anonymity.

Participants recruited via MTurk will be compensated through the MTurk platform upon completion of their participation. This will include payment of $5 per participant.

Is study participation voluntary?

Participation in this study is voluntary. Your decision whether to participate will not affect your current or future relations with Liberty University. If you decide to participate, you are free to not answer any question or withdraw at any time prior to submitting the survey without affecting those relationships.

What should you do if you decide to withdraw from the study?

If you choose to withdraw from the study, please exit the survey and close your internet browser. Your responses will not be recorded or included in the study.

Whom do you contact if you have questions or concerns about the study?

The researcher conducting this study is James McDowell. **You are encouraged** to contact him at [redacted]. You may also contact the researcher's faculty sponsor, Dr. Laura Beiler, Ph.D., at [redacted]

Whom do you contact if you have questions about your rights as a research participant?

If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher, **you are encouraged** to contact the IRB. Our physical address is Institutional Review Board, 1971 University Blvd., Green Hall Ste. 2845, Lynchburg, VA, 24515; our phone number is 434-592-5530, and our email address is irb@liberty.edu.

Disclaimer: The Institutional Review Board (IRB) is tasked with ensuring that human subjects research will be conducted in an ethical manner as defined and required by federal regulations. The topics covered and viewpoints expressed or alluded to by student and faculty researchers are those of the researchers and do not necessarily reflect the official policies or positions of Liberty University.

APPENDIX D: SURVEY

Disclosure: I am asking you to complete this survey as part of the requirements for my dissertation for a doctorate in psychology. Your answers will remain completely anonymous. No personal information about you will be linked to this survey. Please do not put your name or any other identifying information on the survey. You must be 18 years old or older in order to complete this survey.

Directions*:* There are two sections to this survey, which are followed by a cryptocurrency investing game. Please only provide one response per item and follow the detailed instructions provided in each of the sections.

Demographic Question

1. Gender:
    a. Answer options (select one): Male, Female, Binary/Third Gender, Prefer Not to Say

---

Section 1

Directions: There are ten statements on the following page (Rosenberg, 1965). Please only provide one response per statement by selecting the *number* that best represents your degree of agreement with each item.

	Strongly Disagree	Disagree	Agree	Strongly Agree
On the whole, I am satisfied with myself.	4	3	2	1
At times I think I am no good at all.	4	3	2	1
I feel that I have a number of good qualities.	4	3	2	1
I am able to do things as well as most other people.	4	3	2	1
I feel 1do not have much to be proud of.	4	3	2	1
I certainly feel useless at times.	4	3	2	1
I feel that I'm a person of worth.	4	3	2	1
I wish I could have more respect for myself.	4	3	2	1
All in all, I am inclined to think that I am a failure.	4	3	2	1
I take a positive attitude toward myself.	4	3	2	1

Section 2

Directions: Below are 31 statements. Please only provide one response per item by selecting the *number* that best represents the strength of your agreement with the statement (1 = strongly disagree, 7 = strongly agree) (Modic, 2018).

_____ 1. I only act to satisfy immediate concerns, figuring the future will take care of itself.

_____ 2. I think that sacrificing now is usually unnecessary since future outcomes can be dealt with at a later time.

_____ 3. I only act to satisfy immediate concerns, figuring that I will take care of future problems that may occur at a later date.

_____ 4. The appearance of consistency is an important part of the image I present to the world.

_____ 5. An important requirement for any friend of mine is personal consistency.

_____ 6. I make an effort to appear consistent to others.

_____ 7. I would like to travel to places that are strange and far away.

_____ 8. I wish I could have more respect for myself.

_____ 9. I would have enjoyed being one of the first explorers of an unknown land.

_____ 10. If it were possible to visit another planet or the moon for free, I would be among the first to sign up.

_____ 11. I say inappropriate things.

_____ 12. I do certain things that are bad for me if they are fun.

_____13. Sometimes I can't stop myself from doing something, even if I know it is wrong.

_____ 14. When buying products, I generally purchase those brands that I think others will approve of.

_____ 15. If other people can see me using a product, I often purchase the brand they expect me to buy.

_____ 16. I achieve a sense of belonging by purchasing the same products and brands that others purchase.

_____ 17. When a product I own becomes popular among the general population, I begin to use it less. *

_____18. I often try to avoid products or brands that I know are bought by the general population. *

_____ 19. The more commonplace a product or brand is among the general population, the less interested I am in buying it. *

_____ 20. Betting a day's income at the horse races.

_____ 21. Betting a day's income at a high-stake poker game.

_____ 22. Betting a day's income on the outcome of a sporting event.

_____23. Advertising is essential.

_____ 24. Advertising helps raise our standard of living.

_____ 25. Advertising results in better products for the public.

_____ 26. I would rather do something that requires little thought than something that is sure to challenge my thinking abilities.

_____ 27. I try to anticipate and avoid situations where there is a likely chance I will have to think in depth about something.

_____28. Learning new ways to think doesn't excite me very much.

_____ 29. I often combine possessions in such a way that I create a personal image that cannot be duplicated.

_____ 30. I often try to find a more interesting version of run-of-the-mill products because I enjoy being original.

_____ 31. Having an eye for products that are interesting and unusual assists me in establishing a distinctive image.

APPENDIX E: CRYPTO ASSET INVESTING GAME SCENARIOS

Directions: The goal of the crypto asset investing game is to end with the maximum amount of points that you are comfortable achieving (Berg et al., 1995). You will be given 10 scenarios. You will select whether or not you choose to obtain the points available during that scenario by committing the act described in the scenario. Please fully read each scenario.

Scenario	Pts.	Strongly Disagree	Disagree	Agree	Strongly Agree
While visiting my favorite social media platform, I received a notification from a random user who sent me $100 in a cryptocurrency believing that I was someone else who they were trying to invest their money with. I would take their investment.	200	1	2	3	4
A wealthy individual, in what appears to be expensive clothes, cuts in front of a line that I am in while I am waiting for coffee. When confronted about their	400	1	2	3	4

action, they tell me that they are late for an important meeting and can't wait in the line. Despite my visible annoyance, they begin talking to me while they wait for their drink (and I still wait to order). They mention that they are interested in investing in cryptocurrencies. I guarantee them a 1000% return on their investment in three months if they decide to invest in my cryptocurrency program. They offer to send me $10,000, which they can clearly afford to lose. I would take their investment.					
I need to raise money for a new company that I am starting. I began raising money with the intention of creating a profitable company. However, the downturn in the economy and other factors outside of my control quickly made that impossible. I decide to launch an initial coin offering ("ICO") to collect funds from people that clearly have more money than sense. I raise just enough money to keep a roof	600	1	2	3	4

over my family's head with my fake ICO. I would take their investment.					
An acquaintance of mine wins the lottery. They mention to me that they are interested in investing in cryptocurrencies, and don't know where to start. I offer to invest their money in my investment program to guarantee them a return of 10% in a few weeks. They offer to give me $100,000 based on these fake claims. I would take their investment.	800	1	2	3	4
Using a fake social media profile, I pretend to be a qualified investment professional. I direct message random individuals on different social media platforms. I find an individual who agrees to send me $500,000 based on their belief that I am someone else and can make them an excellent return on their investment. I would take their investment.	1000	1	2	3	4

While visiting a long-term care facility, I meet an elderly individual. As I begin talking to them, I learn that they have no living family or friends. They also mention that they are interested in sending me $1 million based on my claims that I can triple their money in three months through my cryptocurrency investment program. I would take their investment.	1000	1	2	3	4
I was recently laid off from my job and need to make money to pay rent. I launched a social media profile and use celebrity images to pretend that I am a famous person. I engage with unsuspecting investors to solicit cryptocurrency investments from them. I would take their investment.	800	1	2	3	4

I own a cryptocurrency company. Despite the fact that I know that accounts on my platform are not backed by a government, I market them as FDIC insured. This false advertisement raises several hundred thousand dollars from unsuspecting individuals. I would take their investment.	600	1	2	3	4
I make a post on social media joking about the “free money” that can be made by investing in cryptocurrency markets. I receive multiple messages from individuals offering to send me several hundred dollars. Before I can respond to tell the individuals that it was a joke, they send me their investments. I would take their investment.	400	1	2	3	4
I login to a popular messaging app to find several messages from individuals offering to pay me a ransom because they believe that I have compromising images of them. Before I respond, I login into my	200	1	2	3	4

cryptocurrency app to find that they have already sent me the money. I would take their investment.

APPENDIX F: PUNISHMENT STATEMENTS

Punishment Scenario	Statement to Participants
Explicit Threat of Punishment	*"To simulate the real-world, there is a chance that you may be caught if you choose to commit a deviant act during the following game. If caught, you will lose all accumulated points."*
Explicit Statement Against Punishment	*"There is no chance that you will be caught if you choose to commit a deviant act during the following game."*
No Statement	*" "*

Note. Participants were randomly assigned to one of the three punishment scenarios. The statement to participants appeared based on the scenario to which the participant was assigned.

APPENDIX G: STATEMENT CONCERNING THE USE OF DECEIT

Title of the Project: Exploring the Relationship Between Self-Esteem, Financial Egocentrism, and Fraud Susceptibility in Cyber-Enabled Fraud Schemes Involving Crypto Assets.

Principal Investigator: James McDowell, Doctoral Candidate, Psychology Department, Liberty University

Thank you for being part of a research study.

You recently participated in a research study. You were selected as a participant because you were over the age of 18 and not a resident of the European Union. Participation in this research project was voluntary.

Please take time to read this entire form and ask any questions you may have.

What was the study about and why was it being done?

The purpose of the study is to explore the potential relationship between self-esteem, financial egocentrism, and fraud susceptibility in cyber-enabled fraud schemes involving crypto assets.

Why am I receiving a debriefing statement?

The purpose of this debriefing statement is to inform you that the true nature of the study or an aspect of the study was not previously disclosed to you.

You were originally told false or misleading information that the point of the crypto asset investing game was to achieve as many points as you were comfortable collecting. In reality, accurate information is that the point value of the crypto asset investing game were arbitrary and this game was used as a way to evaluate your financial egocentrism.

Why was deception necessary?

Deception was necessary to ensure accurate responses were obtained in order to maximize the prospective scientific value of the experiment.

How will personal information be protected?

The records of this study will be kept private. Research records will be stored securely, and only the researcher and faculty sponsor will have access to the records. Participant responses will be anonymous. Data will be stored on a password-locked computer and may be used in future presentations. After three years, all electronic records will be deleted.

What should you do if you decide to withdraw from the study?

If you choose to withdraw from the study, please exit the survey and close your internet browser. Your responses will not be recorded or included in the study.

Whom do you contact if you have questions or concerns about the study?

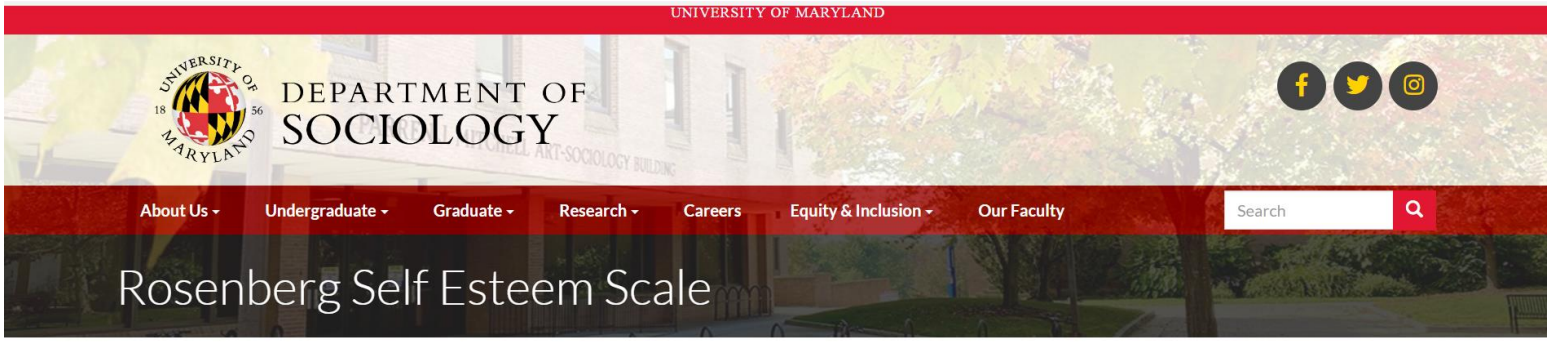
The researcher conducting this study is James McDowell. You may ask any questions you have now. If you have questions later, **you are encouraged** to contact him at [redacted]. You may also contact the researcher's faculty sponsor, Dr. Laura Beiler, Ph.D., at [redacted]

Whom do you contact if you have questions about your rights as a research participant?

If you have any questions or concerns regarding this study and would like to talk to someone other than the researcher, **you are encouraged** to contact the Institutional Review Board, 1971 University Blvd, Green Hall Ste. 2845, Lynchburg, VA 24515 or email at irb@liberty.edu.

Disclaimer: The Institutional Review Board (IRB) is tasked with ensuring that human subjects research will be conducted in an ethical manner as defined and required by federal regulations. The topics covered and viewpoints expressed or alluded to by student and faculty researchers are those of the researchers and do not necessarily reflect the official policies or positions of Liberty University.

APPENDIX H: USAGE OF ROSENBERG SELF-ESTEEM SCALE



The Rosenberg Self-Esteem Scale is perhaps the most widely-used self-esteem measure in social science research. Dr. Rosenberg was a Professor of Sociology at the University of Maryland from 1975 until his death in 1992. He received his Ph.D. from Columbia University in 1953, and held a variety of positions, including at Cornell University and the National Institute of Mental Health, prior to coming to Maryland. Dr. Rosenberg is the author or editor of numerous books and articles, and his work on the self-concept, particularly the dimension of self-esteem, is world-renowned.

The Rosenberg Self-Esteem Scale is now in the public domain, meaning you may use it without charge and without notifying the Sociology Department. This permission extends to making translations or adaptations as you see fit, consistent with traditional scholarly attribution practices. The department does not maintain any information on the scale beyond what is linked below, and cannot advise on its use.

Self Esteem: What Is it?

Rosenberg Scale FAQ

Using the Self Esteem Scale

APPENDIX I: USAGE OF SUSCEPTIBILITY TO PERSUASION II SCALE

MD

Modic, David <David.Modic@fri.uni-lj.si>

To: McDowell, James Morgan

Cc: Jussi Palomaki <hrzmies@gmail.com>

Mon 6/12/2023 2:27 AM

[EXTERNAL EMAIL: Do not click any links or open attachments unless you know the sender and trust the content.]

Dear James,

Please feel free to use StP-II in your research. I would be interested in reading your findings, so keep me updated if you wish and can manage it.

Kind regards,
-- David

On 11 Jun 2023, at 22:22, McDowell, James Morgan <jmcdowell38@liberty.edu> wrote:

APPENDIX J: USAGE OF THE TRUST GAME PRINCIPLE

Order Completed

Thank you for your order.

This Agreement between Liberty University -- James McDowell ("You") and Elsevier ("Elsevier") consists of your license details and the terms and conditions provided by Elsevier and Copyright Clearance Center.

Your confirmation email will contain your order number for future reference.

Printable Details

License Number	5584250822551
License date	Jul 08, 2023

Licensed Content

Licensed Content Publisher	Elsevier
Licensed Content Publication	Games and Economic Behavior
Licensed Content Title	Trust, Reciprocity, and Social History
Licensed Content Author	Joyce Berg,John Dickhaut,Kevin McCabe
Licensed Content Date	Jul 1, 1995
Licensed Content Volume	10
Licensed Content Issue	1
Licensed Content Pages	21

Order Details

Type of Use	reuse in a thesis/dissertation
Portion	excerpt
Number of excerpts	1
Format	electronic
Are you the author of this Elsevier article?	No
Will you be translating?	No

About Your Work

Title	EXPLORING THE RELATIONSHIP BETWEEN SELF-ESTEEM, EGOCENTRISIM, AND FRAUD SUSCEPTIBILITY IN CYBER-ENABLED FRAUD SCHEMES INVOLVING CRYPTO ASSETS
Institution name	Liberty University
Expected presentation date	Jul 2023

Additional Data

Portions	Student to use a modified version of the Trust Game in dissertation.

Requestor Location

Tax Details

APPENDIX K: IRB APPROVAL

LIBERTY UNIVERSITY.
INSTITUTIONAL REVIEW BOARD

September 29, 2023

James McDowell
Laura Beiler

Re: IRB Exemption - IRB-FY23-24-235 EXPLORING THE RELATIONSHIP BETWEEN SELF-ESTEEM, FINANCIAL EGOCENTRISIM, AND FRAUD SUSCEPTIBILITY IN CYBER-ENABLED FRAUD SCHEMES INVOLVING CRYPTO ASSETS

Dear James McDowell, Laura Beiler,

The Liberty University Institutional Review Board (IRB) has reviewed your application in accordance with the Office for Human Research Protections (OHRP) and Food and Drug Administration (FDA) regulations and finds your study to be exempt from further IRB review. This means you may begin your research with the data safeguarding methods mentioned in your approved application, and no further IRB oversight is required.

Your study falls under the following exemption category, which identifies specific situations in which human participants research is exempt from the policy set forth in 45 CFR 46:104(d):

Category 2.(i). Research that only includes interactions involving educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior (including visual or auditory recording) if at least one of the following criteria is met:
The information obtained is recorded by the investigator in such a manner that the identity of the human subjects cannot readily be ascertained, directly or through identifiers linked to the subjects;

For a PDF of your exemption letter, click on your study number in the My Studies card on your Cayuse dashboard. Next, click the Submissions bar beside the Study Details bar on the Study details page. Finally, click Initial under Submission Type and choose the Letters tab toward the bottom of the Submission Details page. Your information sheet and final versions of your study documents can also be found on the same page under the Attachments tab.

Please note that this exemption only applies to your current research application, and any modifications to your protocol must be reported to the Liberty University IRB for verification of continued exemption status. You may report these changes by completing a modification submission through your Cayuse IRB account.

If you have any questions about this exemption or need assistance in determining whether possible modifications to your protocol would change your exemption status, please email us at irb@liberty.edu.

Sincerely,
G. Michele Baker, PhD, CIP
Administrative Chair
Research Ethics Office