Georgia State University
ScholarWorks @ Georgia State University

AYSPS Dissertations | Andrew Young School of Policy Studies

Summer 8-1-2022

Exploring Online Fraudsters' Decision-Making Processes

Tessa Cole

Follow this and additional works at: https://scholarworks.gsu.edu/aysps_dissertations

Recommended Citation

Cole, Tessa, "Exploring Online Fraudsters' Decision-Making Processes." Dissertation, Georgia State University, 2022.
https://scholarworks.gsu.edu/aysps_dissertations/50

This Dissertation is brought to you for free and open access by the Andrew Young School of Policy Studies at ScholarWorks @ Georgia State University. It has been accepted for inclusion in AYSPS Dissertations by an authorized administrator of ScholarWorks @ Georgia State University. For more information, please contact scholarworks@gsu.edu.

ABSTRACT

EXPLORING ONLINE FRAUDSTERS' DECISION-MAKING PROCESSES

By

TESSA SIMONE COLE

AUGUST 2022

Committee Chair: Dr. Leah Daigle

Major Department: Criminal Justice and Criminology

A growing body of evidence suggests the situational context influences the social engineer (SE) characteristics and tactics offenders (i.e., fraudsters) deploy during the development of an online fraud event. Several attempts have been made to examine online the macro-social development of an online fraud event. Nevertheless, macro-level social examinations have been largely unsuccessful in combating online fraud because offenders and victims, including offender victims, are not computers; therefore, offenders' interactions, motives, and tactics are very difficult to surmise. To address online fraud, three independent studies were conducted to explore what is known about online fraudsters and investigate what is not accounted. Specifically, a scoping review of offenders SE characteristics and tactics is conducted. In addition, two empirical investigations examining linguistic cues used by offender and offender victims are conducted. for that present day literature or governmental reports do not address. Together, these studies examine the influence of the situational context on offenders' decision-making process, like their SE characteristics and tactics. The results and limitations associated with each study, along with recommendations for further research are discussed.

EXPLORING ONLINE FRAUDSTERS' DECISION-MAKING PROCESSES

BY

TESSA SIMONE COLE

A Dissertation Submitted in Partial Fulfillment
of the Requirements for the Degree
of
Doctor of Philosophy
in the
Andrew Young School of Policy Studies
of
Georgia State University

GEORGIA STATE UNIVERSITY
2022

Copyright by
Tessa Simone Cole
2022

ACCEPTANCE

This dissertation was prepared under the direction of the candidate's Dissertation Committee. It has been approved and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Criminal Justice and Criminology in the Andrew Young School of Policy Studies of Georgia State University.

Dissertation Chair:	Dr. Leah Daigle
Committee:	Dr. Volkan Topalli Dr. Joshua Hinkle Dr. Timothy Dickinson

Electronic Version Approved:

Sally Wallace, Dean
Andrew Young School of Policy Studies
Georgia State University
August, 2022

DEDICATION

This dissertation is dedicated to my late siblings, Skylar Piety, Zackery Piety, Roslyn Haste, and Patrick Piety. May we all be remembered for the positive impact we left on others.

Additionally, this dissertation is dedicated to black and brown girls, especially my daughter Mackenzie Cole. You do not need to prove your worthiness. You are already enough.

"Don't follow the path. Go where there is no path and start a trail."

-Ruby Bridges

ACKNOWLEDGMENTS

First, I would like to thank my chair, Dr. Leah Daigle, for her academic feedback and supervision during this arborous writing process. I also want to thank my committee members, Drs. Volkan Topalli, Timothy Dickinson, and Joshua Hinkle. A very special thank you goes out to Drs. Volkan Topalli and Timothy Dickinson for their unstinting source of patience, guidance, and personal support. Thank you for believing in me.

Second, I would like to thank Dr. Aunshul Rege. You had no obligation to meet with me weekly to develop me as a scholar and person, but you did. You have helped me refine my writing and developed my confidence as a scholar. The impact you have made in my life is not quantifiable. I hope I can one day impact students the way that you have. Also, Dr. S Gaston, thank you for encouraging me and believing I was smart enough to obtain this degree.

Third, my dear Georgia State peers, thank you for collaborating with me, answering questions my questions, and peer-reviewing my work. You all have made an enormous impact in my life, from my mentees, Ms. Jodi Miller, Ms. Sydney Flonnoy, and Mr. Cameron Hoffman, to my friends Mr. David Ayoni, Mrs. Jimmonique Rogers, Esq., Ms. Shelleen Akins, and Mrs. Shelby Hatcher-Gosnell, Mrs. Tasha Ramirez, Mr. Danye Medhin, Drs. Samaria Mohammad, Shanna Felix, and Katelyn Handcock. I cannot thank you enough for your patience, especially Ms. Jodi Miller, for going line by line with me on edits for various projects and Cameron for discussing statistics.

Fourth, I would like to thank my family and friends. In particular, Ms. Shahidah Habeeb-Ullah thank you for sacrificing and placing me for adoption. The Piety clan, thank you for understanding when I had to cart my computer around during family outings to complete work. To my parents, Dr. Kenneth Piety and Ms. Linda Gordon, thank you for encouraging me to

pursue my dreams. To my sister squad, thank you for rooting me on. Your funny memes and TikTok's kept me going. A special thank you to Mr. and Mrs. Eric Stone for letting me crash at your house and walking through my pregnancy during my dissertation, especially during the height of COVID.

Thank you to my husband, Mr. Dallas Cole, for understanding my early mornings and late-night edits, but most of all, the long conference calls with my peers where I was ensuring I could clearly and adequately explain my research. Your turn to be "hooded" is coming soon!

Third, I am very grateful for my friends and support system, Ms. Hayla Stone, Mrs. Kaylah Rogers, Mrs. Valerie Gallimore, Mrs. Jackie Iwuh, Mr. and Mrs. Seth Gilliam, Ms. Kati Wilson and Drs. Tessa Johnson, Kim, and Jeff Eckert. Ms. Hayla Stone and Mrs. Kaylah Rogers, thank you for loving on my baby and me when I was distracted with writing. Mrs. Valerie Gallimore, for letting me bounce ideas off of you and verbalize my thoughts. Mrs. Jackie Iwuh, you and your family, have been a so supportive and kind to me. Thank you for checking in on us and treating us like family. You have been an encouragement in my life. Seth and Amanda Gilliam, a special thanks to you for the humorous and late-night texts that brought me levity when I was bored writing. Kati, thank you for pushing me and believing in me. Dr. Tessa Johnson, thank you for being faithful for over 20 years and encouraging me to pursue my dreams. Drs. Kim and Jeff Eckert, thank you for your encouragement and optimism throughout my dissertation experience when I did not see an end.

Last but not least, I would like to thank my daughter Mackenzie Cole for giving up hugs, kisses, and playtime with me so I could finish this dissertation. You are kind, gracious, and witty. Thank you for being you, sweet child of mine.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1: Introduction

1.1 Introduction

Online fraud has dramatically increased over the last five years (Internet Crime Complaint Center, 2021). Specifically, nonpayment and non-delivery scams have increased by 34% (from 81,029 to 10,8869), while identity theft scams have increased by 157% (from 16,878 to 43,330) (Internet Crime Complaint Center, 2021). These increasing fraudulent online activities have contributed to the overall increase in online fraud losses from $1.5 to $4.2 billion in the United States (Internet Crime Complaint Center, 2021).

Despite the increasing prevalence of online fraud, researchers have only begun to examine fraudsters' individual-level decision-making processes (i.e., modus operandi) with limited literature addressing online fraud between criminals in general and against online fraudsters in particular (Franklin et al., 2007; Hutching & Holt, 2016; Kigerl, 2018; Kigerl, 2020; Maimon et al., 2019; Yip et al., 2013). For example, researchers have mainly relied on "crime scripts" to describe online offenders' engagement in criminality (Lavorgna, 2014; Zhu et al., 2020). Crime scripts are macro level[1] observations of offenders that attempt to generalize the processes of criminality in a step-by-step manner. For example, software programs are encoded with specific key words (i.e., hack, scam, attack, exploit, etc.) to detect risks and attempts of fraudulent activity. Therefore, if a fraudster uses a term such as "hack," then this detection software can potentially prevent the offender from a cyber-attack. Zhu et al. (2020) used crime scripts to describe offenders' characteristics and tactics engaged in on a macro level with computational tools (via hierarchical sequences). Although crime scripts have helped explore online fraudsters' engagement in crime, researchers fail to account for offenders' characteristics

[1] Observations of offenders' characteristics, behaviors, and interactions across the internet as a whole.

and tactics within the context of online fraud and with whom offenders directly interact (i.e., not accounting for the situation). Offenders and victims of online fraud are not computers, and thus their interactions, tactics, and motives vary, which emphasizes the importance of exploring offenders' decision-making processes (Lavorgna, 2014; Leclerc, 2013; Gilmore, 2014; Zhu et al., 2013). Offender behavior varies more than an automated computer system because there is a level of human and personal interaction. An offender can react according to a potential victims' linguistic cues to manipulate the situational context for the fraudster's benefit.

In an attempt to bridge this empirical gap, my research focuses on online fraudsters, specifically "rippers" (i.e., fraudsters who defraud other fraudsters), and their decision-making processes against offender victims to inform criminological theory, practice, and policy to help combat online fraud regardless of the victims' criminal status. To achieve this goal, I define and subsequently analyze online fraud incidents within the context of the cybercrime ecosystem, relying on a conceptualization of offenders' online fraud characteristics and tactics during the development of an online fraud attempt.

1.1.a Online Fraud

Fraud is the act of intentional deception that leads to personal and/or financial gain ("Fraud," 2019). Online fraud, as defined by the Federal Bureau of Investigation (FBI), is the use of "internet services or software with Internet access to intentionally defraud individuals, organizations or entities" (FBI, n.d.). Most research on online fraud describes fraudsters' characteristics and tactics. Specific to the characteristics of online fraudsters, research suggests that male computer users are more likely to commit online fraud compared to their female counterparts (Chan et al., 2014; Holt et al., 2020; Jegede et al., 2016; Tzani et al., 2020). In

addition, Holt and colleagues' findings suggest that male technological users (e.g., video games) are more likely to engage in online fraud tactics, like hacking than female technological users (Holt et al., 2020). Similarly, research indicates that fraudsters' online personas are associated with online fraud accounts (Leukfeldt et al., 2017; Huang et al., 2015). Huang and colleagues' (2015) research supports this assertion and indicates that users presenting as females on dating websites are more likely to be fraudsters than users presenting as males.

The sophistication of online fraudsters ranges from novice to experienced, with research suggesting that experienced fraudsters are older and less afraid of being caught by law enforcement agencies compared to novice fraudsters who are young and more afraid of being caught (Chan et al., 2013). Similarly, fraudsters' operations differ (Chan et al., 2013, Chang & Chang, 2013). Chan and colleagues (2013) point out that few fraudsters conduct high-dollar scams. Specifically, 5% of fraudsters are involved in online scams that account for over $50,000 (Hong Kong dollar, or HKD) (Chan et al., 2013). Therefore, it is not surprising that most fraudsters earn less than $1,000 (HKD) a month conducting their scams (Chan et al., 2013).

It can be challenging to conceptualize the online fraudsters' decision-making processes because of their behavioral changes and use of various tactics to conduct these scams (Aleem & Antwi-Boasiako, 2011; Atkins & Huang, 2013; Chang & Chang, 2014; Isacenkova et al., 2013; Jones & McCoy; 2014; Modic and Anderson, 2015; Park et al., 2014; Tzani et al., 2020; Van Der Zee et al., 2019). By way of illustration, Chang and Chang (2014) suggest that 80% of online fraudsters modify their fraudulent behaviors more than twice by using tactics that include but are not limited to advance fee fraud, phishing scams, auction fraud, employment scams, 419 scams,

and email scams[2] (Aleem & Antwi-Boasiako, 2011; Atkins & Huang, 2013; Isacenkova et al., 2013; Jones & McCoy; 2014; Maimon et al., 2019; Maimon et al., 2020).

Still, research suggests that criminals' communication (e.g., linguistics) is central to the completion of online fraud. Much of this research focuses on the use of particular linguistic cues such as authority cues (e.g., "trust me" or "have faith in me", urgency cues (e.g., "ASAP" or "urgency"), and delay cues (e.g., "wait" or "hold on"). Specifically, findings indicate that 100% of fraudsters used authority cues to persuade a target of their legitimacy in a sample of phishing emails. In comparison, 71% of fraudsters deployed urgency cues in phishing emails to persuade a target to click on their fraudulent link (Atkins & Huang, 2013). Similarly, Maimon and colleagues' (2019) research suggests the probability of a fraud occurring increases when the offender uses urgency cues.[3] Likewise, Pellon and Anesas' (2019) research suggests fraudsters frequently deploy linguistic cues of urgency when corresponding with their targets. Specifically, the presence of the word "urgent" was present in 1.26 of every 1,000 words of a written scam (Pellon & Anesa, 2019).

1.1.b Online Fraudsters

Criminals who operate online are "really no different than the traditional scam artist of the real world" but are more effective in conducting their criminal operations due to the extensive spatial dimensions of the internet (Handa & Dhawan, 2012). Previous researchers have explained online fraud with various criminological theories, including but not limited to lifestyle theory, routine activities theory, and social learning theory (Akers, 2009; Conrad, 2012; Cohen & Felson, 1979; Chiluwa & Anurudu, 2020; Choi, 2008; Pratt et al., 2010; Leukfeldt, 2014;

[2] See Appendix A. "High Profile Cyber Fraud Tactics Defined" for definitions of these listed scam tactics.
[3] In comparison to offenders who do not use urgency cues during an online fraud event.

Mesch & Dodel, 2018; Wang et al., 2015). However, criminologists have failed to account for and therefore examine all actors involved in the development of an online fraud event, like the website administrators monitoring illicit online marketplaces.

Online fraudsters' decision-making processes are critical to examine considering the losses to online fraud attacks. One decision offenders must make is whom to target, with offenders selecting victims that may also themselves be offenders. Indeed, a vast body of research has demonstrated a victim-offender overlap, with victims being offenders and vice versa (Erdmann & Reinecke, 2021; Reiss, 1981; Berg & Schreck, 2021). Research also suggests offenders are "repeatedly victimized" within the physical environment (see Erdmann & Reinecke, 2021, p. 9318). It is possible that offenders are also repeatedly victimized within the online environment because they re-create dangerous environments within the physical environment in the cybercrime ecosystem (i.e., illicit cybercrime marketplaces, see Yip et al., 2013) (Maimon & Louderback, 2019; Urbanik & Haggerty, 2018). The online environment exposes all actors, including offenders, to an elevated risk of victimization and technological advances (i.e., encryption) afford offenders risk mitigation from their crimes (Urbanik & Haggerty, 2018). As such, the decision-making process of offenders is critical to understand to potentially reduce online fraud and evaluations should not be limited to only those online interactions involving offenders and victims (who are not also offenders).

Fraudsters intentionally act and interact with a target to influence an individual's actions with specific socially engineered (SE) online fraud attacks, which can be observed via offenders' attack characteristics (i.e., linguistic persuasion cues and triggers) and tactics (i.e., nonpayment and non-delivery scams) that frequently result in the divulgence of sensitive information and financial loss (Rege, 2009; Hadnagy, 2010; Rege et al., 2019; Pellon & Anesa, 2019). SE is the

use of internet-based technologies to intentionally deceive or manipulate users into divulging personal, sensitive, or financial information (Hadnagy, 2010, Hadnagy, 2018; Hadnagy, 2019). Criminals' SE tactics often involve pre-texting (Carnegie Mellon University, 2020). Pre-texting is the act of building rapport with a target by developing an understanding of the contextual and situational environment in which an individual acts through preliminary communications with the potential victim (Carnegie Mellon University, 2020; Hadnagy, 2010, Hadnagy, 2018; Hadnagy, 2019). Several researchers have examined fraudsters' communications (via linguistic cues) used to build relationships with their victims in online communications. For example, Pellon and Anesa's (2019) research suggests fraudsters use specific linguistic cues of politeness (i.e., "please"), urgency (i.e., "hurry" and "now"), and delay (i.e., "wait") to elicit sincerity and trust with a target ultimately to defraud them.

Fraudsters' SE attacks are often so successful that they accumulate too much cash to withdraw (or "cash-out") themselves without the detection of law enforcement. Cybercrime marketplaces were created by offenders, like fraudsters, to remedy such issues (Kigerl, 2018). Fraudsters who use these marketplaces communicate about trades, purchases, and/or sales of the financial information or funds that they cannot cash out themselves (Kigerl, 2018). Within the context of online fraud environments, fraudsters' decision-making processes have only begun to be researched (Franklin et al., 2007; Hutching & Holt, 2015; Maimon et al., 2019; Yip et al., 2013), with limited analysis on fraudsters' activities within cybercrime marketplaces (Kigerl, 2018; Yip et al., 2013). Nevertheless, research suggests there are 21 "categories" of online fraudsters, with many of them alternating between one or more of these different "categories" or topics (Kigerl, 2018). This switching of categories suggests criminals' decision-making processes could be heavily dependent upon their interactions within the cybercrime ecosystem.

Criminologists have examined the association between offenders' interactions, including the "microgeographic" or the "immediate social and situational context" surrounding criminals, within the physical environment (Jacobs & Wright, 2006, p. 7, Konkel et al., 2021). The majority of research related to the social and situational context of criminality is primarily based on studies exploring offenders' in-person deals (Dickinson & Wright, 2015; Jacques, 2010; Jacobs & Wright, 2006; Topalli & O'Neal, 2003). For example, Dickinson and Wright (2015) explored the social and situational context of 33 drug dealers and their customers, discovering that the sellers would modify their behaviors to dissuade buyers from reporting the seller to law enforcement. Sellers may maintain their social relationship with a customer but stop selling drugs to them to avoid police detection (Dickinson & Wright, 2015). Similarly, Jacques (2010) suggests that offenders retaliate against other offenders without in-person interactions by stealing resources, like jewelry, drugs, and money, from the offender who wronged them. As a common retaliatory act, drug dealers will indirectly "recover losses" or steal from offenders who have grieved them (Jacobs & Wright, 2006). Criminals modify social behaviors (e.g., verbal defense mechanisms) depending on their surrounding contextual factors (i.e., code switch) (see Topalli et al., 2002; Topalli, 2005). Topalli and colleagues' (2002) research indicates that criminals manage social expectations by "code-switching," which depends on verbal defense mechanisms used to retaliate, depending on the contextual and situational environment (Topalli et al., 2002).

The aforementioned research supports the contention that offenders' motivations (i.e., situational environment) influence their criminal engagement style (Cornish & Clarke, 2003). With 307.2 million internet users in the U.S. alone, the internet is more widely used now than in the past decade, resulting in offenders who are not restricted to their residential communities (Dahlqvist et al., 2019; Statista, 2022) Therefore, the prevalence of offenders' social interactions

would be expected to increase because the internet has no geographical limitations and therefore allows for a much larger pool of targets (Handa & Dhawan, 2012). For example, the internet's capabilities allow offenders to access tools such as encryption, which enable them to hide their identities while helping them facilitate monetary gains (Erdmann & Reinecke, 2021; Jennings et al., 2011; Urbanik & Haggerty, 2018). Therefore, acknowledging the impact of the cybercrime ecosystem's environment, specifically the contextual and situational environment, is paramount to thoroughly understanding online fraudsters' decision-making processes.

Although criminological frameworks have examined online fraud, research has yet to thoroughly investigate the contextual and situational environment influence on fraudsters' SE characteristics and tactics as an online fraud attempt develops between actors. Specifically, there remains a gap in the literature examining the contextual and situational environment influence on fraudsters' decision-making processes with actors. However, the influence of communications on actors' actions and interactions and behaviors is well established within the communications field (Buller & Burgoon, 1996; Norris et al., 2019; Zhou, 2003; 2004). Norris et al.'s (2019) research indicates peripheral processing, such as an individual's evaluation of messages, is a useful "way to understand why people fall for scams" and thus the decision-making processes fraudsters deploy to defraud targets (p. 240).[4]

The following studies in this dissertation contribute to research by analyzing the contextual (i.e., illicit online marketplaces) and situational (e.g., offender motivations) environment influence on fraudsters' decision-making processes through the combination of both communication and criminological theoretical perspectives (Buller & Burgoon, 1996; Short, 1998). Specifically, I investigate key issues highlighted in this introduction by drawing on the

[4] Here, offenders' decision-making processes can be observed as a situational technique (Clark & Cornish, 2003).

criminal event perspective (CEP) postulated by Short (1998) as a framework, with the support of interpersonal deception theory (IDT) derived from Buller and Burgoon (1996). I achieve this by examining online criminals' decision-making processes (via characteristics and tactics observed during an online fraud attack) using previous research that applies CEP and IDT to explain the situational explanations of online fraudsters.

1.2 Theoretical Framework

1.2.a The Criminal Event Perspective (CEP)

As Short (1998) proposed, the CEP is a criminological perspective that contends criminality can be identified, explored, and explained during the microsocial development of an event. Specifically, the CEP focuses attention on criminal interactions between offenders and victims during the formation of crime (Meier et al., 2001). The CEP was built upon Goffman's (1955) social interaction perspective, which asserts that individuals will modify their actions and behaviors in reaction to their interactions within their environment. Similar to Goffman's (1955) social interaction perspective that explains the interactions between actors, Short's (1998) CEP has been used to explain the interactional processes of predatory crime to explain all types of crime (Cornish & Clarke, 2002; Fagan & Wilkinson, 1998; Deibert & Miethe, 2003).

Scholars have explored the situational factors surrounding criminals' physical environment using the CEP (Bierie et al., 2013). Specifically, the CEP has assisted in exploring individual criminal engagement factors based on demographics, such as age (e.g., juvenile delinquency), location (e.g., cohabitation), and marital status in their physical environment (Horney, Osgood, & Marshall, 1995, p. 667-669; Shaw & McKay, 1942). More recently, CEP has been used to explore opportunistic factors related to criminality and victimization (Kirwan &

Power, 2013; Jahankhani, et al., 2014; Ngo & Paternoster, 2011). Relevant to online fraud, CEP has been used to explain cyber property crimes, like fraud and identity theft (Bossler & Berenblum, 2019; Jahankhani, et al., 2014; Madarie, et al., 2019; Maimon, et al., 2019). Madarie et al. (2019) applied the CEP to analyze dark web forums, and their research suggests criminals learn from encrypted, or anonymous, positive interactions via website ratings. These positive interactions contribute to the overall understanding of why cybercriminals are willing to purchase entertainment services and financial institution account credentials from cyber hackers. Similar to Madarie and associates' (2019) findings, research completed by Maimon, Santos, and Park (2019) indicates that the cyber interaction between offenders and victims influences the commission of a cybercrime. According to these scholars, urgency cues at the beginning of a fraud attempt influenced the verbal and non-verbal urgency cues later in the digital interaction (Maimon, et al., 2019). While the CEP provides a framework to explain the microsocial development of a fraud incident between actors within their environment, it does not thoroughly explain the influence of criminals' communication with targets during the development of a crime. The addition of interpersonal deception theory by Buller and Burgoon (1996) is included in this analysis to fill this void.

1.2.b Interpersonal Deception Theory (IDT)

Researchers have used non-criminological theories to explain criminality, such as communication theories (see Maimon et al., 2019). Specifically, interpersonal deception theory (IDT), a communication theory, assists in explaining the social interactions between online fraudsters and targets in the cybercrime ecosystem. Buller and Burgoon (1996) propose in IDT that deception is similar to normative communication, as it involves strategic and non-strategic

behaviors (Buller & Burgoon, 1996). To define the difference between the two forms of behavior, strategic behavior involves humans' intentional and conscious awareness. In contrast, non-strategic behaviors involve unintentional and unconscious actions of humans. According to IDT, the sender's message affects the receiver and vice versa (White & Burgoon, 2001). Specifically, normative communication requires participation from both parties, with non-strategic (e.g., unconscious actions) behavior present throughout the interaction. Strategic behaviors are intentional actions (e.g., conscious actions) present in communications, such as the criminal's creation and dissemination of a deceitful message to manipulate the receiver (Buller & Burgoon, 1996).

Although IDT may appear to be a simplistic explanation for deceptive communication, it is not. There are 18 propositions assumed in Buller and Burgoon's (1996) IDT that thoroughly depict the deception between senders and receivers. Propositions 3 and 18 are two key propositions in IDT that can be applied to the examination of offenders' decision-making processes during the development of an online fraud event. Proposition 3 presumes deceitful individuals use more strategic activity to comprehend information, as well as using more non-strategic arousal cues and non-involvement cues than those who are honest. Proposition 18 presumes the success of a sender's (e.g., deceiver's) deception depends on the sender's cognition and behavior throughout communications with the target.

Evidence-based research indicates that fraudulent incidents (e.g., criminal events) are successful when criminals strategically and non-strategically deceive victims by adapting their behaviors based on the feedback that they receive to evade detection and increase credibility (Buller & Burgoon, 1996; Burgoon, Proudfoot, Schuetzler, & Wilson 2014). An example of this is observed in a study carried out by Burns and Moffitts (2014), in which linguistic cues (i.e.,

communication) are different between individuals who engaged in deceit and truth. To exemplify this difference, 911 homicide calls were transcribed and analyzed for callers who were deceitful during their interactions with 911 operators. The results suggested that those who engaged in lying negotiated with the operators more often through the use of assenting words (Burns & Moffitt, 2014). Although Burns and Moffitt's (2014) research examining 911 calls is not a criminological example, it provides theoretical support for the examination of offenders' communication on the microsocial level. As previously stated, deception is not a crime, but fraud always involves deceit. Therefore, Burns and Moffitt's (2014) findings are applicable when explaining how deceptive communication differs between truth-tellers (i.e., offender victims) and deceivers (i.e., fraudsters).

The theoretical framework detailed above accounts for the role of internet-based communications and how fraudsters exploit online communications for their benefit. Therefore, IDT is used in conjunction with the CEP to extend the existing research concerning fraudsters' decision-making processes during the development of an online fraud incident (Buller & Burgoon, 1996; Short, 1998).

1.3 Research Questions

As highlighted, there is little research on fraudsters' decision-making processes during the development of an online fraud event. To fill this void, my dissertation addresses the following research questions:

1.) To what extent do online fraudsters employ different approaches, tactics, and strategies based on their perception of targets' (or victims') situational environment?

a. What is known about offenders SE characteristics and tactics for targeting individuals within the situational environment online?
b. What are the SE characteristics and tactics offenders develop for successful online fraud events against other offenders?
c. How does the situational environment influence offenders SE characteristics and tactics during the development of an online fraud event against offending victims?

To address these questions, I conducted a scoping review of the situational factors supporting offenders' SE attacks (via characteristics and tactics) and investigated offenders' decision-making processes through fraudsters' interactions with other offenders in two independent studies.

1.3.a Study 1 (Chapter 2)

The purpose of chapter two is to identify what is known about the situational factors that support online fraudsters during the development of a successful online fraud event against their targets (or victims). I conducted a scoping review of fraudsters' SE characteristics and tactics against online targets to explore and identify what is known about fraudsters' decision-making processes, with a focus on the situational factors that support a successful online fraud event. To achieve this, I categorized fraudsters' attacks by characteristics (i.e., linguistic cues) and tactics. Specifically, the review covered the linguistic characteristics, like the observed syntax and grammar and the persuasion cues and triggers offenders use during computer-mediated technology to defraud targets. Fraudsters' tactics, such as the type of online fraud attack (i.e., online auction fraud) and the attack's sophistication were also documented.

The findings produced from this scoping review provided a blueprint for the following two studies in my dissertation.

1.3.b Study 2 (Chapter 3)

Research suggests a victim and offender overlap (see Reiss, 1981; Berg & Schreck, 2021) with offenders within the physical environment who are frequently "repeatedly victimized" (see Erdmann & Reinecke, 2021, p. 9318). Additionally, researchers have emphasized the importance of offenders' contextual environment, such as the influence of an offender's location on their interactions (Anderson & Meier, 2004, p. 420; Benson et al., 2009, p. 183). Despite the key role offenders play in crime that occurs in the physical environment, little research has explored the decision-making process of fraudsters who victimize other offenders (also known as rippers) within the context of fraud online (Kigerl, 2018). The uncertainty related to the microsocial level of offenders' interactions beg the question, "What situational factors support the development of a successful online fraud event against other offenders?" The current study examines fraudsters' interactions using Proposition 3 of IDT along with CEP to examine offenders' decision-making processes during the development of an online fraud event (Buller & Burgoon, 1996; Short, 1998). Proposition 3 asserts deceptive users employ longer response times or disengagement in communication to gather information from targets they intend to victimize (Short, 1998). Specifically, self-collected data from a mixed-methods study was used to explore the situational (i.e., motivations and techniques) environmental factors influencing offenders' decision-making processes (measured via urgency and/or delay cues deployed) during the development of an online fraud event (Anderson & Meier, 2004; Benson et al., 2009; Cornish &

Clarke, 2003; Hadnagy, 2010; Pellon & Anesa, 2019; Zhou et al. 2002; Zhou & Zhang, 2004; 2007).

1.3.c Study 3 (Chapter 4)

My third research question builds upon prior work suggesting that situational environmental factors influence deceptive users during computer-mediated communication by analyzing fraudsters on active carding marketplaces. Specific to criminology, criminals' communication and behaviors depend on with whom they interact (i.e., Topalli et al., 2002). Specific to computer-mediated interactions, research indicates deceptive users communicate with words that are on average a lower character count than honest users. In comparison, honest users communicate with words that are on average a higher character count than deceptive users (Zhou et al., 2002; Zhou & Zang, 2004; 2008). Therefore, building upon Proposition 18 of IDT that presumes the success of a sender's (e.g., deceiver's) deception depends on the sender's cognition and behavior throughout communications with the target, I suspect that fraudsters will strategically interact with their targets while attempting to avoid detection. They will do so by sending a lower prevalence of messages compared to those they are targeting (or victimizing) during the development of an online fraud event in an attempt of disclosing (in communications) less information about themselves to targets (i.e., situational technique see Clark & Cornish, 2003). I draw upon prior research (i.e., Zhou et al., 2002; Zhou & Zang, 2004; 2008), and I hypothesize that the prevalence of direct messages sent by deceitful offenders [fraudsters] to offender victims is overall lower than the prevalence of direct messages sent by offender victims to deceitful offenders [fraudsters]. In regards to the development of an online fraud event, I hypothesize that the prevalence of direct messages sent by deceitful offenders [fraudsters] to

offender victims is higher than direct messages sent by offender victims to deceitful offenders [fraudsters]. Alternatively, the prevalence of direct messages sent by deceitful offenders [fraudsters] to offender victims is lower than direct messages sent by offender victims to deceitful offenders [fraudsters]. The current study examines situational environmental factors that influence offenders' decision-making processes within the context of online fraud events through an examination of a self-collected data set from active illicit marketplaces.

Chapter 2: Fraudsters within the Cybercrime Ecosystem: A Scoping Review of Online Fraudsters' Decision-Making Processes

2.1. Introduction

The cybercrime ecosystem, recently defined as the illegal interactions between actors online, has expanded opportunities for crime and fundamentally altered the way many crimes are committed (Maimon and Louderback, 2018). Cyber-criminals have a wide selection of targets to defraud because the internet allows offenders greater access to targets than what would be available to them in the physical criminal environment. Identify theft is an example of a crime resulting from this expansion due to cybercrime growth. Cyber-criminals can defraud targets online by stealing and selling social security numbers and financial information without physically trespassing into the victim's residence (Leukfeldt et al., 2016; Maimon and Louderback, 2018).

Offenders commit identify theft and deploy various other online fraud attacks to cash their illicit funds while avoiding detection from law enforcement (Kigerl, 2018), which has led to the development of more online fraud forums that are based off of the need to buy others' identities for the sole purpose of withdrawing funds. For instance, criminals will use multiple stolen identities to "cash out"[5] on profits produced from their criminal interactions, which they may not otherwise be available to "cash out" on due to the large withdrawals that would attract attention from law enforcement (Kigerl, 2018). Identity fraud losses have increased by 118.54% from $100,429,691 to $219,484,699 from 2018 to 2020. Identity theft losses are important to highlight because identity theft is one of the frequent tactics fraudsters use to defraud targets,

[5] Cash-out is a slang word for deposit.

which can be observed in the 168.66% increase in reported victims within three years (Internet Crime Complaint Center, 2021).

Despite these losses and the increased number of victims, no research to date has specifically reviewed offenders' decision-making processes during the development of an online fraud event. The present scoping review fills this void in research as the first exploration into online fraudsters' decision-making processes by reviewing the characteristics and tactics used during attacks. Online fraudsters are theoretically conceptualized within the context of the cybercrime ecosystem in the first section of the review. The second section explores published online fraud reviews and highlights the current gaps in research. Lastly, the gaps in research are addressed through explanations of the situational factors that support offenders' social engineered (SE) attacks (via observed characteristics and tactics within deployed fraud attacks) from this scoping review with suggestions for future research.

2.1.a Previous Research Reviews

The current literature that examines online fraudsters' decision-making processes observed in their SE attacks (via characteristics and tactics within deployed fraud attacks) is limited and mainly relies upon descriptive data (Chang & Chang; 2014; Chan et al., 2013; Pellon & Anesa, 2019) with few experimental studies conducted (Maimon et al., 2019; Maimon et al., 2020). In an analysis of the linguistic characteristics observed in offenders' online fraud attacks, Akins and Huang (2013) found that 100% of offenders used linguistic cues of persuasion while only 71% of offenders used urgency cues to manipulate targets into clicking on a phishing link. The phishing emails examined by Akins and Huang (2013) are primarily based upon offenders' SE fraudulent emails from their targets' financial institution(s). Pellon and Anesa's (2019)

research suggests fraudsters used certain words (i.e., linguistics) to persuade targets with fake scenarios by offering them money (673 words signaled the promise of money) compared to other phony situations, like prizes (153 words signaled the promise of money) and awards (113 words signaled the promise of money). Alternatively, Chan et al. (2013) investigated offender tactics, with a focus on the sophistication of their tactics, used by offenders to defraud targets in online fraud attacks. Fraudsters range in sophistication from novice to experienced, and very few are substantially profitable (i.e., generating $50,000 or more) (Chan et al.2013). Additionally, Chang and Chang (2014) identified that 80% of fraudsters changed their behaviors at least two times during an online auction fraud attack. Offenders' modified their SE fraud attacks to deceive their targets by selling items on Yahoo!Taiwan auction websites (Chang & Chang, 2014).

Offenders' sophistication can be observed through their ability to adapt to the contextual environment (i.e., engaging in online auction fraud attacks compared to spoofed emails from a target's financial institution), including their ability to evade detection. Chang and Chang (2014) highlight this adaptation often occurs within the online criminal environment. Therefore, how the contextual and situational environment impacts offenders' decision-making processes is critical to understand.

2.1.b The Criminal Ecosystem

The situational environment, including the "microgeographic" or the "immediate social and situational context," influences offenders' decision-making processes (Jacobs & Wright, 2006, p. 7, Konkel et al., 2021). Recently, Konkel and colleagues (2021) investigated the situational location of sex offenders' offenses and found offenders committed more crimes within a strict microgeographic area. Similarly, offenders' decision-making processes have been

examined within the social and situational context of in-person drug dealing interactions (Dickinson & Wright, 2015; Jacques, 2010; Jacobs & Wright, 2006; Topalli & O'Neal, 2003). Jacques's (2010) research suggests that from a social aspect, offenders retaliate against other offenders by stealing resources (i.e., money and drugs) without in-person interactions. Offenders, for example, would retaliate by breaking in to steal another offender's money or drugs while the offender they were retaliating against was not physically present at the residence. The absence of in-person social retaliation, for example, often led to offender victims' loss of possessions within their situational environment (Jacques, 2010). Similarly, Dickinson and Wright's (2015) findings suggest offenders will maintain social relationships with customers but modify their situational environment and stop selling drugs to their customers to avoid police detection. For instance, if drug dealers perceived that a customer was "acting sketchy," the offender would stop selling drugs to that customer. When drug dealers stop selling illicit substances, the situational context changes with their customers.

Most research on online fraud is limited to a review of the contextual and situational environment influencing online fraud offenders, instead of covering offenders' characteristics and tactics themselves. Research indicates online fraudsters are no different than the offenders who operate in the physical world. Although online fraudsters and those who operate in the physical world are similar, the internet has no geographical limitations and therefore allows for a much larger pool of targets (Handa & Dhawan, 2012). Maimon and Louderback (2018) stress that online users' interactions with one another influence the cybercrime ecosystem. The five actors Maimon and Louderback (2018) identify are enablers, offenders, targets, victims, and guardians. Offenders deploy online fraud attacks on targets who become victims if they are successfully exploited. Enablers support offenders' criminal endeavors by providing the

offenders with the targets or elicit personally identifiable information such as stolen social security numbers. Agencies or system administrators are the guardians who are tasked with protecting targets and regulating the environment/ecosystem, which are oftentimes ill-equipped to handle the volume of fraudulent activity on their designated platform. Any of these actors operating within this ecosystem could become a fraud victim (Maimon & Louderback, 2018).

2.1.c Previous Reviews

The factors assessed in the online fraud literature predominately focus on the prevalence, victims, and the computational tools used to identify these types of crimes (Coluccia et al., 2020; Norrs et al., 2019; Reurink, 2016; Pratt et al., 2013). An example of this is Reurink's (2016) literature review conceptualizing the prevalence and consequences of online fraud. Reurink's (2016) explanations provide the foundation for types of online fraud attacks, like social engineering (SE) and technical subterfuge (TS) attacks. SE is the use of internet-based software or technology to persuade or manipulate users into divulging sensitive, personal, or financial information (Hadnagy, 2010, Hadnagy, 2018; Hadnagy, 2019). TS is more technical than SE and relies on offenders' technological ability to use computer systems to disrupt or corrupt navigational infrastructures to illegitimate websites for the victim's sensitive, personal or financial information. TS enables offenders to target a larger group of users than SE attacks because SE attacks require the offender to communicate with victims for the desired information. Reurink (2016) emphasizes offenders may embed SE within their TS fraud attacks to make them appear more legitimate (Reurink, 2016, p. 47-48).

The majority of online fraud reviews focus on victimized users (Norrs et al., 2019; Pratt et al., 2013; Pourhabibi et al., 2020). Pratt et al.'s (2013) meta-analytic review examined online

fraud victims' level of self-control through the dispositional traits of the victim (N=11 instances of fraud examined in review). The findings suggest an association between low self-control and online forms of victimization, like online fraud (Pratt et al., 2013). Similarly, Coluccia et al.'s (2020) scoping review documented three main factors observed from online fraud victims: (1) epidemiological aspects, (2) relationship dynamics, and (3) victims' and fraudsters' psychological characteristics. The review suggests between 1% to 3% of online users categorized themselves as victims of romance fraud with particular psychological factors like impulsivity and excessive dependency on others associated with victimization. Norrs et al. (2019) systematic review examined fraud victims' psychological processes and interactions with online fraud in a three-pronged approach: (1) the influence of users' personality characteristics (i.e., dispositional studies), (2) the messages deployed in online fraud attacks, and (3) users' experience, and expertise with online fraud attacks (i.e., experiential studies).[6] In particular, Norrs et al. (2019) questioned the validity of examining victims' personality characteristics to predict online susceptibility because there is "no clear pathway linking" a users' susceptibility and characteristics (p. 240). However, Norrs et al.'s (2019) findings suggest that reviewing offenders' and victims' direct interactions, specifically the peripheral processing that transpires during actors' interactions, "may provide the most useful way to understand why people fall for scams" (p. 240).

The computational tools used to identify these crimes vary, as indicated in Pourhabibi et al.'s (2020) evaluation. Pourhabibi et al.'s (2020) evaluation is a systematic review aimed at detecting fraudulent communications within networks through computational tools. The systematic review suggested the graph-based anomaly detection (GRAD) computational tool is

[6] N=44 papers

useful in detecting fraudulent interactions online with potential applications in cryptocurrency exchanges, like Fintech. Nevertheless, the researchers acknowledge the "intrinsic multiplex nature of human interactions" (i.e., liking or hearting other users' posts online) during the development of fraudulent interactions influencing online fraud events (Pourhabibi et al., 2020, p 12).

Collectively, the aforementioned reviews and Pourhabibi et al.'s (2020) research outline the critical role of online fraud offenders' interactions during the development of an online fraud event. However, researchers have neglected to review offenders' modus operandi, including their SE characteristics and tactics observed in their deployed attacks.

2.1.d Online Fraudsters

Perpetrators of online fraud can be reported to a wide variety of agencies. Still, no centralized system exists that records all reports of cybercrime instances, including information on the cyber-criminals who commit these crimes. The absence of this documentation makes it difficult to track the characteristics and tactics observed in offenders' attacks. Privatized agencies have an incentive to emphasize the purported necessity of their products, resulting in greater profits from higher rates of cyber threats (Verizon, 2020). An example of a private organization that sells products to protect customers from various forms of cybercrime protection (e.g., malware protection) is Verizon. Verizon (2020) reported that over 60% of their data breaches were financially motivated in 2019. The breachers underscored the potential profits from successful fraud operations and the lack of transparency in reporting, which could potentially include the increase of purchased products. An estimation of financial loss due to fraud is not included within their reporting, leaving a significant gap in data that is unavailable to analyze.

The FBI's Internet Crime Complain Center (IC3) currently provides the best reporting and presents the most effective countermeasures, but it fails to account for all actors involved in cybercrime incidents, especially offenders conducting cybercrime. Additionally, an unknown proportion of cybercrimes are unaccounted for because reporting incidents of fraud to IC3 is voluntary. Nevertheless, the IC3 reports online fraud losses have increased by 180% in the last five years from $1.5 to $4.2 billion (Internet Crime Complaint Center, 2021). These losses may be due to limited countermeasures in response to the wide variety and constantly evolving methods of cybercriminals (Aleem & Antwi-Boasiako, 2011; Mubarak et al., 2019; Park et al., 2014; Weber et al., 2020).

Despite the increase in online fraud, there is little systematic knowledge of effective fraud operation practices and methods for targeting victims. There remains disagreement about the most prevalent cyber fraud tactics and operational practices in academic communities, which have only begun to examine the criminals conducting these scams (Bowe & Jobome, 2001; Murad & Pinkas, 1999; Maimon et al., 2020; Wani & Jabin, 2016; Van Wilsem, 2011; Zyl & Joubert, 1994). Analysis of known operations and behaviors has been limited to a particular cybercrime niche, such as auction frauds and online marketplace listings (e.g., Craigslist) (Chan et al., 2014; Maimon et al., 2020). In addition, researchers have mainly focused on examining fraudsters' demographics and personal characteristics, such as their education level, age, personal motivation, and psychological factors within the cybercrime ecosystem (Chan et al., 2014; Lazarus, 2018; Rogers et al., 2006). The objective of this paper is to identify the current gaps of knowledge regarding cyber fraud by performing a scoping review of research on online fraudsters' decision-making processes (via characteristics and tactics observed in deployed

attacks) during the development of an online fraud event. In particular, the central question for this review is:

1.) What situational factors support the development of a successful online fraud event against targets?

Building upon previous research that suggests fraudsters strategically act with targets based on contextual and situational factors with specific socially engineered (SE) characteristics and tactics (see Rege, 2009; Hadnagy, 2010; Rege et al., 2019; Pellon & Anesa, 2019), I use Arkey and O'Malley's (2005) methodological framework for scoping reviews to explore and identify the characteristics and tactics observed in offenders' online fraud attacks.

2.2. Methods

Arkey and O'Malley's (2005) methodological framework for scoping reviews was adopted because it is one of the most commonly used methods for collecting relevant research. As a result, Arkey and O'Malley's (2005) methodological framework was used to ensure all research on online fraudsters is included in this review. The framework consists of a five-stage approach to ensure researchers thoroughly review relevant research (Daudt et al., 2013). The five stages are as follows: (1) identify research questions, (2) identify relevant studies, (3) study selection, (4) chart the data, and (5) collate, summarize, and report relevant results (Arkey & O'Malley, 2005).

(1) Identify research questions

The research question must be identified in the initial stages of a scoping review because it guides researchers in design strategies that ensure relevant areas of research are consulted (Arkey & O'Malley, 2005). The purpose of this scoping review is to identify online fraudsters'

decision-making processes (via characteristics or tactics observed in attacks). As indicated previously, the current scoping review focuses on the following question:

1.) What situational factors support the development of a successful online fraud event against targets?

(2) Identify Relevant Studies

I identified relevant literature pertinent to the research question using key search terms related to online fraud. Specifically, I used key terms closely related to online fraud and the offenders who conduct these crimes and organized them using Boolean logic to combine the required terms and narrow down search results. Therefore, I employed the following key terms using Boolean expressions to combine terms on all but two of the databases: "online" OR "internet" OR "electronic" OR "cyber" AND "fraud" OR "scam" AND "online*" OR "internet" OR "cyber" AND ("fraudster*" OR scammer*") AND "interpersonal decep*" OR "internet auc*" OR phishing* OR e-fraud* OR "social engineer*" OR "online Carding*" OR "online Credit Card Fraud*" OR "online Fraud Tactic*" OR "email fraud*. A similar search using Boolean expressions to combine terms was used to conduct searches on two distinct databases where the above search was not possible due to search function limitations. [7,8]

Arkey and O'Malley (2005) emphasize the importance of consulting various sources, such as reference lists, electronic databases and relevant conferences and organizations for a thorough review (p. 22). To do so, I conducted a broad search of nine databases were conducted:

[7] Institute of Electrical and Electronics Engineers (IEEE) Xplore only allowed seven wildcards to run at a time, and therefore, Boolean logic was modified. I used the following key terms with Boolean expressions to combine terms on (IEEE) Xplore: "Online" OR "internet" OR "cyber" AND "fraudster*" OR Scammer*" OR "Interpersonal decep*" AND "social engineer*" OR "Online Fraud Tactic*."

[8] Science Direct only allowed eight "Boolean connectors" to run at a time, and therefore, Boolean logic was modified. I used the following key terms with Boolean expressions to combine terms on Science Direct: "Online" OR "internet" OR "cyber" AND "fraudster" OR Scammer" OR "Interpersonal deception" AND "social engineering" OR "Online Fraud Tactics."

(1) Academic Search Complete, (2) Association for Computing Machinery (ACM)[9], (3) Criminal Justice (CJ) Abstracts, (4) American Psychological Association (APA) Psycinfo, (5) Institute of Electrical and Electronics Engineers (IEEE) Xplore[10], (6) Public Affairs Information Service (PAIS) Index, (7) ProQuest Central including ProQuest Dissertations and Theses (Galileo), (8) ScienceDirect, and (9) Web of Science. ProQuest Dissertations were included to yield any new, unpublished research on online fraudsters because there is limited research on offenders' decision-making processes. I also explored the grey literature, including governmental reports such as the FBI's IC3 annual cybercrime report to ensure a thorough review of the information relevant to the characteristics or tactics observed in online offenders' fraud attacks.

2.3. Data Collection and Analysis

(3) Study Selection

A total of 14,516 records were exported, with 4,155 studies failing to export.[11] Prior to analyzing the exported studies, I removed all the duplicates in Endnote following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) system (Clarivate, n.d.; PRISMA, n.d.). PRISMA (n.d.) is an evidence-based reporting system allowing scholars to evaluate research pertinent to their study. Endnote is a software package that manages references (Clarivate, n.d.). After removing the duplicates, I removed the 218 studies written in a different language. Then, I used an Endnote tool to locate the full text of my remaining studies. If I could not retrieve the full text of the remaining studies with Endnote, I manually searched for the text. Following my manual search, I conducted a preliminary search of the results by reviewing each

[9] ACM "omitted some entries very similar to the displayed" to present the most relevant results.

[11] ACM "omitted some entries very similar to the displayed" to present the most relevant results.

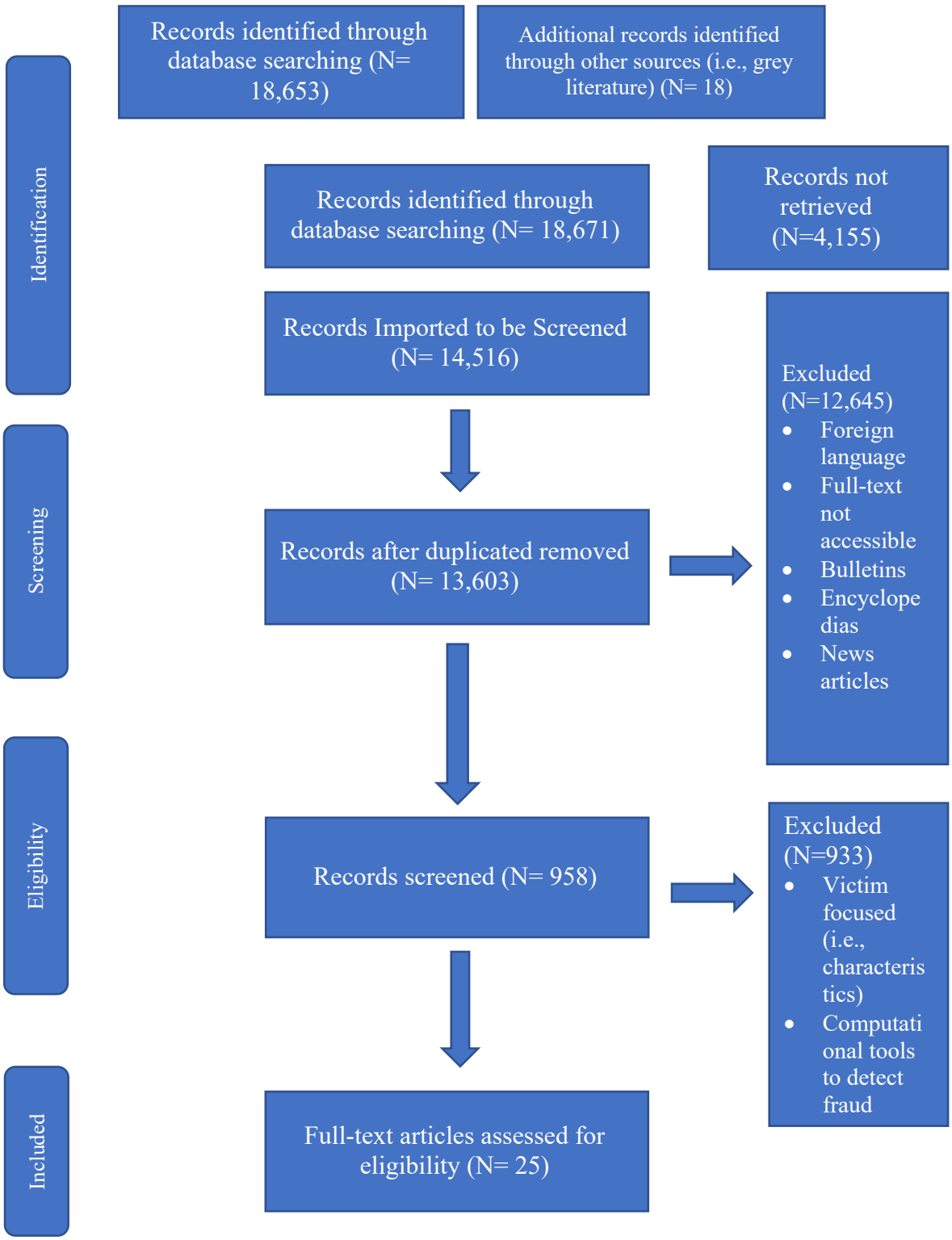
title and abstract in Endnote and removed studies not relevant to this scoping review (i.e., bulletins, encyclopedias, trade journals, news articles). Once the irrelevant studies were removed, 25 studies remained based on the eligibility for inclusion. Studies were eligible for inclusion if they met the following criteria:

(i) Population: This review is focused on perpetrators of online fraud. The population of online fraudsters will be identified based on two elements. First, studies that focus on computational tools used to detect online fraud and studies examining the effectiveness of computer detection systems against online fraudsters were excluded unless the research focused on using computational tools to quantify offenders' characteristics and tactics. Second, only studies examining perpetrators of online fraud were included.

(ii) Online Fraud: Online fraud is the act of intentional deception that leads to personal and/or financial gain on the internet ("Fraud," 2019). Therefore, studies about online fraudsters' decision-making processes, with a focus on online fraudsters' characteristics and tactics, were included.

(iii) Study design: The research included in my review was not restricted by study design and therefore could be qualitative, quantitative and/or mixed-methods.

Figure 1. PRISMA Flow Diagram for the Identification of Online Fraudsters' Characteristics and Tactics.

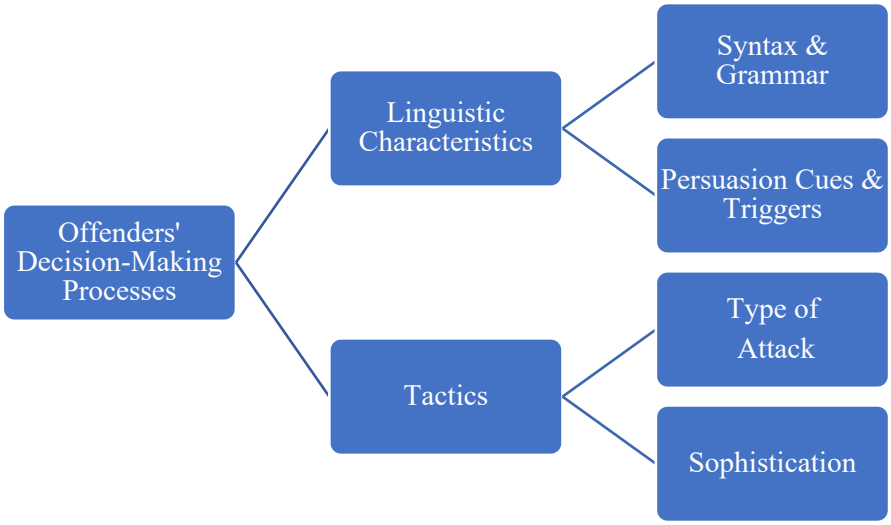


(4) Chart the Data

I collected and categorized key pieces of information from the selected articles and reports. Then, I organized the data by standard study information and online fraudsters' decision-making processes were categorized by attack characteristics and tactics in Table 1, "A Description of Fraudsters' Decision-making Processes by Characteristics and Tactics." I used the following categories for organization:(1) author (year of publication), (2) unit of analysis/sample size (N), (3) fraudsters' characteristics (i.e., linguistic[12] cues), (4) fraudsters' tactics for the type of scam attempted (e.g., phishing, advance fee), (5) financial information (e.g., money transfer application[13] or institution,[14] fake email notification, money mule[15], and check amount), (6) specific/additional information related to fraudsters' characteristics and/or tactics of interest, and (7) online forum where fraud reportedly occurred (i.e., online context).[16] An illustration of how fraudsters' decision-making processes were categorized can be found in Figure 2, "A Breakdown of Fraudsters' Deceptive Characteristics and Tactics."

[12] Variables associated with a fraudsters' linguistics cues will range from cues of urgency and politeness to word and message count sent by a fraudster to a target.
[13] An example of a money transfer application is PayPal.
[14] A bank is an example of a money transfer institution, like Regions bank.
[15] Money mulling is when an individual transfers financial funds associated with criminal activity on behalf of another individual(s). Frequently, a money mule is paid with a portion of the illicit funds.
[16] The online context could range from auction frauds (i.e., Craigslist advertisement, and eBay auction) to fake emails from a targets' financial institution(s).

Figure 2. “A Breakdown of Fraudsters’ Deceptive Characteristics and Tactics”



(5) Collate, Summarize and Report the Results

An initial 18,671 total results were extracted, but only 25 studies were included in the analysis after applying the exclusion criteria (see Figure 1). The studies vary in methodology and theoretical perspective with the two factors (offenders’ characteristics and tactics) identified within the data. The results are synthesized, summarized, and reported according to the defined research question within Table 1. The studies presented in Table 1 are documented with overall standard study information and categorized by the characteristics and tactics of offenders’ online fraud attacks. Key findings are highlighted as well.

Table 1. A Description of Fraudsters' Decision-making Processes by Characteristics and Tactics (N=25)

Author (Year of Publication)	Unit of Analysis/ Sample (N)	Fraudsters' Characteristics	Fraudsters' Tactics	Financial information	Specific Information Related to Fraudsters' Characteristics and/or Tactics	Online forum where fraud reportedly occurred (i.e., online context)
Aleem & Antwi-Boasiako (2011)	43 Emails		Phishing via spoofed PayPal emails	Fraudsters defraud between £220 ($251.68 USD) and £410 ($515.94 USD) plus £30 ($37.75 USD) delivery costs.	IP location of fraudsters: 50% of fraudsters from Nigeria 1 fraudster from the United States 1 fraudster from South Africa 1 fraudster from Romania Two IP addresses were hidden.	eBay Auction Fraud
Atkins & Huang (2013)	200 emails	Eight linguistic persuasion cues and triggers were examined within fraudsters' communication with targets: (1) authority, (2) urgency, (3) tradition, (4) fear/threat, (5) attraction/excitement, (6) pity, (7) politeness, and (8) formality.	Advance fee emails (100 emails) Phishing emails (100 emails)		Persuasions & Triggers used in advance fee emails: Authority: 84% Fear/threats: Formality: 24% Politeness: 78% Urgency: 70% Persuasions & Triggers used in Phishing emails: Authority: 100% Fear/threats: 41% Formality: 55% Politeness: 74% Urgency: 71%	Emails 100 "spoofed" financial institution emails (PayPal, eBay, HSBC bank, etc.) from MillerSmiles site) 100 total emails (85 e-mails coming from the researchers' inboxes and 15 from MillerSmiles site)
Chan, Chow, Kwan, Fong, Hui, & Tang (2014)	61 online auction offenders	Three types of behavioral characteristics: (1) Novice-Moderately-Active, (2) Intermediate-Inactive, and (3) Experienced-Active.		Fraudsters earnings: The total amount fraudulently earned was $1 million in HK 5% of offenders fraudulently earned $50,000 HK	The most associated with age and motivation for defrauding was Experienced-Active. Offenders' fraudulent activity varied: 48% of fraudsters were actively involved in less than 11 transactions per month.	Case reports from an online auction offender database

Tables 1 continued

				16% of offenders fraudulently earned more than $5,000 HK 52% of offenders fraudulently earned less than $1,000 HK per month	31% of fraudsters were actively involved in 11-30 transactions per month. 18% of the fraudsters were actively involved in more than 30 transactions per month.	
Chang & Chang (2014)	645 Fraudsters	The offenders ' interactions observed four types of behavioral characteristics: Aggressive, Classical, Luxury and Low-profiled.			The types of fraudsters evolve.	Yahoo!Taiwan Auction website
Costin, Isacenkova, Balduzzim, Francillon, & Balzarotti (2013)	67,244 unique cellular devices used in fraud instances	Characteristics of socially engineered scenarios linguistically presented in emails by offenders conducting fraud attacks.	Social engineer attacks (i.e., orphan, new partner, dying widow, dying merchant, fake lottery, 419 scam, next of kin, Zimbabwe, Yukos oils, and company representative scams)		90% of socially engineered scenarios linguistically presented in fraud attacks were attributed to: 62% were general scams 25% were lottery scams 8% were inheritance (next of kin) Offenders do not evenly disperse their fraud attacks across geographical areas Fraudsters reuse phone numbers more frequently than emails	Several sources associated with online fraud attacks (i.e., scam and spam messages, registration information of malicious domains (WHOIS) and Android malware).
Diekmann, Jann & Wyder (2004)	172 fraud instances	Characteristics of fraudsters' presentation involved in auction fraud.			Offenders with positive ratings (i.e., 4 or 5 stars) have a higher frequency of fraud attacks than first-time sellers with no ratings (24%).	Swiss Auction Fraud Events

Tables 1 continued

					No significant effects on the duration of the auction and the selling price.	
Garg & Nilizadh (2013)	30 Advertise ments		Social Engineer		There is an association between offenders and who they target (i.e., targets demographics). White males are positively associated with fraud attacks and are more likely to be targeted by offenders than their counterparts. High school graduates are positively associated with fraudulent attacks. Income (per capita) is positively associated with a fraudulent attack.	Craigslist Advertisements (focused on automobile scams of 30 American cities)
Huang, Stringhini, Yong (2015)	510,503 dating scam accounts		Social Engineer		Fraudsters social engineer their presentation on romance websites. 50% of fraudsters presenting themselves as “Swindlers” and “Dates for profit started conversations with their victims. 20% of “swindler” fraudsters were contacted by 90 potential victims	Romance scams (on DATINGSITE)
Jones & McCoy (2014)	1,315 (received) emails		Social Engineering Phishing	The average amount fraudsters attempted to defraud targets was $1,953.58 per check but $1,953.58 per	Offenders' social engineer checks used in fraud attacks: Only business addresses appeared on checks received, with more than 90% of checks associated with a legitimate business.	Craigslist Advertisements (total of 56 ads)

Tables 1 continued

				fraudulent PayPal payment. The total amount fraudsters attempted to have a target send a money mule/mover was $61,945.14.	Fraudsters deployed spoofed PayPal emails to defraud targets Over 50% of scam payments originated from five groups. Fraudsters attempted to avoid detection with money mules/movers in 43 transactions.	
Macinnes (2005)	129 dispdutes		Misrepresentation Fraud		The two payment types that were used for this model were cashier's checks and PayPal/credit cards. Most fraud instances on auction websites related to misrepresentation are quality disputes of used products: 76% of used products are disputed compared to new products.	eBay auction
Maimon, Santos & Park (2019)	623 email threads	Fraudsters ' communication with targets examines linguistic persuasion cues and triggers, specifically urgency cues. Additionally, the frequency of messages sent by fraudsters to victims with and without linguistic persuasion cues and triggers.	Social Engineering Phishing		Linguistic persuasion cues and triggers are positively associated with fraudsters' initial interactions with targets. The number of predicted messages with a fraudster is higher at 3.6 than non-fraudster at 2.3 emails when urgency cues are present. The frequency of fraudsters' messages with no urgency cues present are at 1.9.	Craigslist Advertisements

Tables 1 continued

Maimon, Howell, Moloney, & Park (2020)	623 Email Threads	Linguistic persuasion cues and triggers, specifically politeness and urgency cues, are examined within fraudsters' communication with targets.	Social Engineering Phishing		The timing an offender deploys linguistic persuasion cues and triggers are significant. Cues of politeness decrease the likelihood of fraud events while cues of urgency increase. Follow up emails contained linguistic persuasion cues: 71.1% of emails contained both politeness and urgency cues. 17% of the subsequent emails contained only politeness cues 5% of the subsequent emails only contained urgency cues. 6.64% of the subsequent emails did not contain politeness or urgency written cues.	Craigslist Advertisements
Mikhaylov & Frank (2016)	420 posts on carding forum		Fraudsters' money laundering on illicit marketplace online forums.		Offenders money launder their fraudulent earnings through: (1) Exchanging Currencies (i.e., Western Union, WebMoney, and Bitcoin) (2) Online Gambling (3) Money Mules	Two illicit hacking and carding forums (Russian speaking/based)
Mubarak, Yahya & Shaazi (2019)	3 Scammer Scenarios		Social Engineering Types of social engineered attacks observed in scenarios: Scenario 1: Phishing Scenario 2: Smishing		The three social engineered scenarios used by fraudsters were described: Offender pretending to be a law enforcement agency. SMS attack to access a target's banking information. Offender pretending to be a customs officer.	

Tables 1 continued

			(phishing via SMS) Scenario 3: Phishing			
Park, Jones, McCoy, Shi & Jakobsson (2014)	19,204 emails		Advance fee fraud (researchers also refer to it as "Nigerian scams"/ "419 scams")		90% of offenders deploy their fraudulent attack in response to an online classified advertisement via email within the first 24 hours. Fraudsters use the same email account to communicate with a target on average 3 times. Offenders' use various email providers: 65% of fraudsters used Gmail accounts. 10% of fraudsters used Microsoft (i.e., Hotmail and Live) accounts. 3.5% of fraudsters used Yahoo accounts.	Craigslist Advertisements
Park (2016)	204 emails		Advance fee fraud (researchers also refer to it as "Nigerian scams"/ "419 scams")	Offenders asked for payment using Western Union or MoneyGram.	72% of fraud attacks originate from 3 groups of fraudsters. 70% of fraudsters' shipping addresses originated from Nigeria. Offenders avoid detection by not reusing IP addresses. Offenders deployed emails in bursts ranging between 4.5 and 24.7 seconds, suggesting a level of computational automation.	Craigslist Advertisements

Tables 1 continued

Pellon & Anesa (2019)	507 emails	Linguistic persuasion cues and triggers	Advance fee fraud		Persuasions & Triggers used in fraud communications: The word "immediately" was observed in 1.26 of every 1,000 words used by fraudsters. The word "urgently" was observed 0.25 for every 1,000 words used by fraudsters. The trigger word "money" was observed 673 times. The trigger word "winning" was observed 200 times. The trigger word "prize" was observed 153 times. The trigger word "award" was observed 113 times.	Collection of emails sent to targets of online by offenders.
Rege (2009)	170 research articles documents examining the characteristics of online fraudsters	Linguistic persuasion cues and triggers	Social Engineering		Fraudsters' characteristics observed in social engineered attacks: Grooming of targets with linguistic persuasion cues and triggers Basic computer skills Routines Work in networks of offenders Use neutralization techniques to rationalize criminality.	Thematic saturation of romance scam and identify theft scams
Schaffer (2012)	30 emails	Linguistic persuasion cues and triggers	Nigerian fraud/419 scams		Offenders' social engineering fraud tactics. A few of the social engineered situations involved are misrepresented and are as follows: 30% of fraudsters misrepresented themselves as government officials 16.7% of fraudsters misrepresented themselves as bank officials	Collection of emails sent to targets of online by offenders.

Tables 1 continued

					Persuasions & Triggers used in emails: Confidence: 83.3 Urgency: 73.3% Grammar mistakes observed from offenders' communications via email: Punctuation errors (missing period): 93.3% Missing words: 86.7% Incorrect capitalization: 83.3% Misspelled words: 56.7%	
Tzani-Pepelasi, Nilsson, Lester, Pylarinou, & Ioannou (2020)	26 Fraudsters		Phishing	Offenders defrauded victims using various methods (i.e., gift cards and financial transfers): iTunes gift cards: 53.3% Bank Transfers: 10% MoneyGram: 3.3% Cash withdrawal: 6.7% Debt card information: 6.7%	46.7% of communications contained grammar mistakes. Offenders asked for personal information (i.e., targets' address and financial information) in 90% of fraudulent attacks.	HMRC/IRS Scammers

Tables 1 continued

Van Der Zee, Clayton, Anderson (2019)	44 email conversations with 21 unique fraudsters	Linguistic persuasion cues and triggers such as authority and consistency, and commitment.	Advance Fee Frauds (i.e., Nigerian fraud/419 scams)	Offenders tried to obtain money from targets using the following transfer options: Western Union (21%), MoneyGram (5%), Western Union/MoneyGram (5%), a general bank transfer (5%), or a mixture of methods (5%), and the remaining transfers were unknown.	98% of offenders' communications via email contained more than one spelling or grammar mistake. Persuasions & Triggers used in emails: Authority: 90.5% Commitment and consistency: 100%	Craigslist Advertisements (Rentals in United Kingdom)
Vasek & Moore (2018)	1780 unique cryptocurrency fraud instances		Ponzi Scheme		Offenders social engineer fraudulent attacks, including the duration of the attack. The average scam (fraud attack) lasted about a week. Scams, where offenders posted more lasted longer.	Cryptocurrency fraud (i.e., Bitcoin)
Weber, Schutz, Fertig & Muller (2020)	5 case studies	Linguistic persuasion cues and triggers were observed in 5 scenarios.	Social Engineering Types of social engineered attacks observed in scenarios: Scenario 1: Phishing Scenario 2: phishing	The amount offenders defrauded from victims in the 5 scenarios are as follows: Scenario 1: 3mill in tokens Scenario 2: 50 million Scenario 3: 1 million	Fraudsters used linguistic persuasion cues and triggers of authority and social proof in all 5 scenarios.	Cryptocurrency frauds

Tables 1 continued

			Scenario 3: pretexting and spear phishing Scenario 4: pretexting Scenario 5: bating	Scenario 4: 172.57 ETH Scenario 5: 0.755 ETH		
Xia, Wang, Geo, Su, Yu, Luo, Zhang, Xiao, & Xu (2021)	10,920 scam tokens		Rug pull attacks Backdoor attacks	50% of the tokens examined were fraudulent, worth about $365 million.	Offenders' tactics to defraud targets of scam tokens were described. Specifically, 6,288 fraudsters created 10, 920 scam tokens.	Cryptocurrency frauds

2.*3.a Fraudsters' Characteristics*

The majority of published studies exploring online fraud and the offenders who commit these crimes describe a link between fraudsters' linguistic characteristics, including but not limited to the syntax and grammar observed in communications during the progression of an online fraud event (Schaffer, 2012; Tzani-Pepelasi et al., 2020). Specifically, researchers have examined fraudsters' linguistic characteristics through offenders' syntax and grammatical errors and their deployed persuasion cues and triggers. As research emphasizes, fraudsters' syntax and grammatical errors range from misspellings to improper grammar, syntax, and diction. For instance, fraudsters' communications frequently contain capitalization problems, missing words, and/or misused verb tense (Blommaert & Omoniyi, 2006; Riga, 2003; Schaffer, 2012).[17]

Researchers have described fraudsters' persuasion cues and triggers as a target's motivation (or "nudge") to engage with an offender's fraudulent instance and/or attack (Atkins & Huang, 2013). A trigger is an incentive a target has for engaging with the offender via digital communications (Atkins & Huang, 2013). Fraudsters often deploy persuasion cues and triggers to establish legitimacy with the target. The combination of the fraudsters' persuasion cues and triggers is frequently observed in pre-texting, which is critical to an offender's successful fraud attack (Hadnagy, 2010, Hadnagy, 2018; Hadnagy, 2019).

2.3.a.a Syntax and Grammar. Offenders' mistakes vary in studies that examine fraudsters' syntax and grammar. Researchers identified some form of syntax and grammatical error in 33.3% to 93.3% of fraudsters' digital communications (Schaffer, 2012; Tzani-Pepelasi et al., 2020). For example, Schaffer's (2012) findings found that 30% of communications contained

[17] Schaffer's (2012) research was framed using scholars such as Blommaert and Omoniyi (2006) and Riga (2003) who examined scammers linguistic cues via mail.

run-on sentences, 46.7% contained sentence fragments, and 86.7% were missing words. Additionally, 53.3% of fraudsters had grammatical errors, including phrases within fraudulent communications like, “as I say to you before…” (Tzani-Pepelasi et al., 2020, p. 167). Identifying syntax and grammar mistakes within offenders’ linguistic characteristics suggests that the success of an online fraud attack may depend more on the fraudsters’ linguistic persuasion cues and triggers than their grammatical competency. Furthermore, offenders' written communications targeting victims, although challenging to analyze due to grammar errors (e.g., style and syntax) and jargon, do not have as much influence on the development of an online event as the persuasion tactics deployed during an online fraud event.

2.3.a.b Persuasion Cues and Triggers.. Although research indicates offenders use a variety of linguistic persuasion cues and triggers, researchers have mainly reported online fraudsters' use of authority, fear/threats, formality, politeness, and urgency (Atkins & Hunag, 2013; Maimon et al., 2019; Pellon & Anesa, 2019; Schaffer, 2012; Tzani-Pepelasi et al., 2020). For example, authority cues were more frequently used by fraudsters (i.e., 84% to 100% of online communications referenced by Atkins & Huang, 2013) than fear/threat persuasion cues that were only identified in 40% (Akins & Huang, 2013) to 90% of digital communications (Tzani-Pepelasi et al., 2020) with fraudsters’ targets. Formality persuasion cues and triggers were identified in 24% to 55% of digital fraud communications (Akins & Huang, 2013). Atkins and Huang (2013) identified statements such as “unauthorized recipients are requested to preserve this confidentiality” and “it may contain confidential or sensitive information” as formality persuasion cues and triggers. Similarly, fraudsters deployed politeness cues, like “Dear Valued Customer/Member,” “Best Regards,” and “Sincerely,” ranged from 14% to 78% of their online

communications (Atkins & Huang, 2013; Maimon et al., 2020). Researchers identified the presence of urgency cues, like "ASAP", "new message waiting," and "You have 24 hours to click on the link below and confirm…," in 6% (Maimon et al., 2020) to 71% of fraudulent communications online (Atkins & Hunag, 2013; Maimon et al., 2019; Pellon & Anesa, 2019; Schaffer, 2012; Tzani-Pepelasi et al., 2020).

As observed from the studies yielded in this reviewed so far, online fraudsters' characteristics are primarily based upon researchers' observation of the frequency of offenders' linguistic characteristics (Atkins and Huang, 2013; Maimon et al., 2019, Maimon et al., 2020, Schaffer, 2012). However, researchers have neglected to review offenders' modus operandi, including their SE characteristics and tactics observed within the context of their deployed attacks. Nevertheless, the literature examining fraudsters' characteristics has revealed the emergence of several themes, like the different types of linguistic cues and triggers deployed during the development of specific online fraud events and the timing of the deployment of these cues and triggers

The reported frequency of politeness cues deployed by fraudsters varies depending on the type and timing of the online fraud attack. Specifically, Schaffer's (2012) research only identified politeness cues in 23.3% of fraudsters' written communications during a Nigerian scam attack[18] in email (i.e., context) communications with targets. Alternatively, Maimon et al. (2020) research identified politeness cues in 60% of fraudsters' first messages to targets during nonpayment fraud attacks on classified advertisements on Craigslist (i.e., context). However, the prevalence of politeness cues deployed by fraudsters in nonpayment fraud attacks decreased by 46% as an online fraud attack developed. Specifically, only 14% of fraudsters' subsequent

[18] Also referred to as Nigeria 419 scams.

messages (i.e., any message sent by an offender to a target after the first message) sent to targets contained politeness cues (Maimon et al., 2020).

Given the observed differences with offenders' use of linguistic politesses cues within different online contextual environments (i.e., email compared to Craigslist advertisements), it is not surprising that research suggests the prevalence of offenders deployed urgency cues vary depending on the context and timing of the fraud attack. In support of this assertion, Atkins and Huang (2013) identified a higher frequency of urgency cues within phishing email scams (71%) compared to Maimon et al.'s (2020) research suggesting only 18% of initial fraudsters' written communications during a nonpayment fraud attack via Craigslist advertisements contained cues of urgency. However, Maimon et al. (2020) research suggests fraudsters' prevalence of urgency cues increases by 52% in subsequent written communications during a nonpayment fraud attack.[19] There is limited research exploring fraudsters' characteristics, let alone the connection between fraudsters' characteristics and tactics. Therefore, the following section explores fraudsters' tactics as a way to examine fraudsters' decision-making processes more thoroughly.

2.3.b Fraudsters' Tactics

A number of studies have explored, identified, and examined fraudsters' tactics that range in presentation (i.e., scam type) and sophistication. Specific to offenders' behavioral presentations, researchers have examined the type of attack offenders deploy. Specifically, research indicates that offenders deploy a variety of online fraud attacks, including but not limited to account takeover, advance fee, advertisement fraud (via Craigslist advertisement), auction fraud (via eBay), Nigeria 419 scams,[20] phishing (via spoofing) and nonpayment fraud

[19] Urgency cues are present in approximately 70% of subsequent emails (Maimon et al., 2020).
[20] Nigeria 419 scams are when an offender pretends to be someone Nigeria like a Nigerian prince.

(via eBay and Craigslist) (Atkins & Huang, 2013; Maimon, et al., 2019; 2020; Park et al, 2014; Schaffer, 2012).

2.3.b.a Types of Attack. The most common types of attacks examined by researchers within this review were advertisement and auction frauds within the contextual environment of eBay and Craigslist. Nevertheless, research suggests offenders modify their behavior depending on the situation presented within the contextual environment. Offenders, for example, may use misrepresentation tactics to spoof a financial institution (i.e., PayPal) to conduct phishing attacks within the context of Craigslist classified advertisements (Park et al., 2014; Park, 2016). At the same time, fraudsters, within the context of Craigslist classified advertisements, may defraud targets using nonpayment attacks (Maimon et al., 2019; Maimon et al., 2020). Based on these situational differences examined by researchers within similar contextual environments (i.e., Craigslist classified advertisements), it is not surprising that the yielded literature suggests offenders change their behaviors more than two times (see Chang & Chang, 2014 and Kigerl, 2020) through deceptive linguistics cues that elicited misrepresentation (via government misrepresentation and spoofing). Specifically, Schaffer (2012) research found 30% of offenders pretended to be government officials, whereas Aleem and Antwi-Boasiako (2011) identified 21% of fraudsters' emails were spoofed[21] to collect a target's financial information.

Researchers also describe the monetary amounts fraudsters successfully defraud, and offenders' tactics used to avoid detection to cash out their illicit earnings. The yielded literature suggests approximately half of offenders (52%, Chan et al., 2014) earned between $1,000 to $1,346.63 per month compared to 16% who defrauded victims of more than $5,000 per month

[21] Spoofing can be attributed to a wide array of scams but often involves targets' giving the offender technological permissions associated with their device.

(Jones & McCoy, 2014).[22] Park et al. (2014) research supports the claim that a small portion of offender networks, specifically ten fraudster groups, were responsible for over 13,000 scam attempts (Park et al., 2014) and limited their participation in fraudulent transactions per month to less than 11 transactions per month (Chan et al., 2014). These findings emphasize how offenders are able to avoid detection while purportedly victimizing a large number of victims for financial gain, but their monetary gains and methods may depend on their level of sophistication (Chan et al., 2014; Jones and McCoy, 2014).

2.3.b.b Sophistication. A number of studies highlight indicators of a fraudster's tactical sophistication depending on the situational environment, including their cash-out methods (Mikhaylov and Frank, 2016). For instance, Chan et al. (2014) findings indicate offenders defrauding targets of high-priced items will be more experienced than novices who do not engage in fraud as frequently. Additionally, Chang and Chang's (2014) research suggests that sophistication does "evolve over time and that various fraudulent behaviors are exhibited by fraudsters reported in different years" (p. 96). As an added layer of protection from detection, the use of cryptocurrency could be described as a level of tactical sophistication among offenders affording them encrypted funds (Mikhaylov and Frank, 2016). Although any actor could purchase, invest, and trade cryptocurrency, an ordinary actor may not be knowledgeable in obtaining or defrauding targets with this type of currency (Khandelwal, 2019; Weber et al., 2020). In addition to fraudsters' frequent use of cryptocurrency to "cash out" on their "steals," research suggests fraudsters use digital forms of payment like electronic gift cards. Specifically, Tzani-Pepelasi et al. (2020) research found that 53% of offenders used iTunes gift cards to cash

[22] $1,000 Hong Kong Dollars is approximately $127.39 USD today.

out on monetary gains. These limited examples highlight the lengths who which offenders are willing to go while obtaining stolen goods and also emphasize their various tactical sophistication in getting their stolen monetary gains.

2.4 Discussion and Conclusion

Up to now, far too little attention has been given to conceptualizing and examining the offenders who are key influencers affecting the growing prevalence of financial loss to online fraud (Internet Crime Complaint Center, 2021). This review identified the contextual (i.e., online classified advertisement via eBay and Craigslist) and situational (i.e., offenders' SE characteristics and tactics observed within their deployed attacks) factors supporting the development of a successful online fraud event against targets via offenders' decision-making processes to fill this gap in research. The current scoping review explored the characteristics and tactics of fraudsters' interactions (via communications and digital interactions) reported in 25 studies.

The study contributes to our understanding of cybercriminals' (i.e., offenders) decision-making processes thorough their linguistic characteristics and tactics observed through their deployed SE fraud attacks. This is the first study to review and identify the frequency and prevalence of particular linguistic characteristics used by fraudsters. It also reviewed the timing of the deployed linguistic cues and the type of fraud attacks offenders choose to deploy, such as Nigerian 419 scams, non-delivery fraud, and advance fraud (Atkins & Huang, 2013; Maimon et al., 2019; 2020; Park et al., 2014; Schaffer, 2012). Additionally, this review provides evidence with respect to the type of attack offenders deploy, including their tactical level of sophistication and the technological advancements providing anonymity that are provided for them (Chang &

Chang, 2014; Chan et al., 2014). Offenders' use of cryptocurrency to cash out their stolen monetary funds, for example, is more technologically sophisticated (Khandelwal, 2019; Weber et al., 2020) than defrauding targets of iTunes gift cards, as observed among offenders in Tzani-Pepelasi et al. (2020) research.

The yielded literature raises important theoretical issues that have a bearing on the research conducted within the physical environment examining the role of offenders' decision-making processes. As previously stated, the "immediate social and situational context" influences offenders' decision-making processes that include offenders' in-person interactions with other actors such as offenders and guardians (i.e., law enforcement) as supported by numerous researchers (Dickinson & Wright, 2015; Topalli & O'Neal, 2003). As it relates to the online environment, fraudsters will deploy SE fraud attacks to fit the situational context. An example of this is how offenders misrepresented themselves (via spoofed emails) as financial institutions (i.e., PayPal) to defraud targets through online classified advertisements featured on eBay and Craigslist (Aleem & Antwi-Boasiako, 2011; Maimon et al., 2019; Maimon et al., 2020). At the same time, fraudsters' have misrepresented themselves as governmental entities via email in Nigeria 419 scams (Schaffer, 2012).

The present review has shed light on the influence of offenders' situational environment, such as the various linguistic persuasion cues and triggers embedded during the development of an online fraud event depending on the situational context (i.e., online classified advertisements on eBay and Craigslist compared to Nigerian scams via email communications) (Atkins & Huang, 2013; Maimon et al., 2019; 2020; Park et al., 2014; Schaffer, 2012). An example of this is how Schaffer only identified cues of politeness in 23.3% of fraudsters' written communications during Nigerian scam attacks, while Maimon et al.'s (2020) research found that

60% of initial written communications from fraudsters to targets contained politeness cues during nonpayment scams on Craigslist (Maimon et al., 2020). The difference of use with particular linguistics, like politeness, within each situational context online (i.e., Craigslist advertisements) emphasizes the importance of fraudsters' SE attacks (via characteristics).

As illustrated above, the increasing losses and prevalence to online fraud events (via identity theft scam) increase offenders' successful defrauding of targets. Therefore, it is important to examine fraudsters' decision-making processes so their characteristics (e.g., , linguistic cues) and tactics (e.g.,, non- delivery fraud) can be used to help formal respondents (e.g.,, law enforcement) attain the identifications tools needed for the successful prevention and intervention of fraud. Fraudsters aim to use these specific linguistics cues to appeal to a variety of demographics and cultures; doing so allows them to gain access to a vulnerable population of individuals' personal information. Specifically, fraudsters have successfully nudged, manipulated, and threatened targets using a combination of tactics (e.g., phishing scams) to defraud targets without them being aware of the scam (e.g., by using deception). However, the yielded studies did not examine the influence of the situational context on fraudsters who deploy SE attacks online. For example, the yielded studies did not account for the influence of where fraudsters participate within illicit online forums (e.g., Telegram carding channels); this would have allowed for a more in-depth observation of fraudsters characteristics and tactics between offenders.

Study limitations make any overall conclusions about online fraudsters extremely difficult. The small body of literature examining the SE characteristics and tactics of online fraudsters' attacks produces difficulties in generalizing their decision-making processes, particularly with the focus on macro-level fraud events (Atkins & Huang, 2013; Park et al.,

2014). Secondly, technological capabilities grant offenders anonymity that could heavily skew the prevalence of characteristics and tactics observed within the yielded results (Atkins & Huang, 2013; Maimon et al., 2019; 2020; Park et al., 2014).

If scholars hope to identify overarching themes throughout online fraud communities, a better understanding of online fraudsters must be developed to thoroughly and effectively examine the nuances of online fraud. For example, the offender victim overlap is widely acknowledged, but there currently is limited research into the online fraudsters' SE characteristics and tactics against other offenders. In fact, much of the research examining the offender victim overlap online is focused on the macro-social level (Kigerl, 2018; Kigerl, 2020). The current study focuses on the micro-social level of fraudster interactions. This type of examination is important to the field because fraud activity is still increasing even with current macro-level prevention methods (those used across the internet). Therefore, focusing on micro-level methods can potentially resolve this issue to prevent and intervene upon the offenders who conduct this fraud activity. Focusing on macro-level social interactions has been unsuccessful in preventing online fraud activity. Micro-social interactions, including offenders' direct communications within the deployed attack (e.g., non-delivery scam), with the target(s) will address specific tactics unaccounted for during macro-level interactions.

The yielded literature and findings of this scoping review should guide research and justification for the necessity of future studies, while remaining focused on the important theoretical issues regarding exploitation of a target's negligence for security. Specifically, scholars should examine the situational context that influences offenders' decision-making processes to explore the cybercrime ecosystem in which fraudsters have thrived by defrauding both offending and non-offending targets to combat online fraud.

Chapter 3: The Pot Calling the Kettle Black: A Mixed Methods Analysis of Rippers' Decision-Making Processes on Telegram

3.1. Introduction

Cybercriminals have generated over 13.3 billion dollars in total losses in the past five years, by engaging in various types of online fraud attacks, like online credit card fraud, to defraud targets (Internet Crime Complaint Center, 2021). Credit card fraud losses have increased by 169.4048%, from $48,187,993 to $129,820,792, and offenders have successfully defrauded 10.81% more victims from 2016 to 2021 (Internet Crime Complaint Center, 2017; Internet Crime Complaint Center, 2021). Online frauds like credit card fraud are lucrative. Still, criminals often cannot deposit the cash acquired from their fraudulent schemes themselves without drawing the attention of law enforcement. Cybercrime marketplaces were partly created to remedy this issue. Fraudsters use these marketplaces to communicate the trades, purchases, and/or sells of the financial information or funds that they cannot cash out themselves (Kigerl, 2018).

Recent evidence suggests fraudsters use cybercrime marketplaces to communicate about the trades, purchases, and/or sale of financial information or funds they have acquired and to defraud or "rip" each other (Kigerl, 2018). Rippers, a slang term commonly used for fraudsters who defraud each other, have been explored by researchers. Most research exploring rippers is qualitative and does not account for how rippers' decision-making processes influence their communication with targets during an online fraud event (Garg, Afroz, Overdorf, & Greenstadt, 2015; Gaspareniene & Remeikiene, 2015; Holt, 2013; Holt & Lampke, 2010; Soudijn & Zegers, 2012; Yip, Shadbolt, & Webber, 2013; Yip, Webber, & Shadbolt, 2013). Additionally, the quantitative research is limited to categorizing fraudsters' attacks by offenders' behavior, like the

number of times an offender changed their SE tactics during their interactions with targets (Benjamin, et al, 2014; Chang & Chang, 2014; Motoyama, et al, 2011). Specifically, Chang and Chang (2014) observed that 80% of fraudsters modified their SE fraud attacks at least two times during online auction frauds.

Research suggests the contextual (i.e., online platform[23]) and situational environment influences fraudsters' intentional interactions with targets (Anderson & Meier, 2004; Cornish & Clarke, 2003, p 52; Hadnagy, 2010; Jacobs & Wright, 2006, p. 7, Konkel et al., 2021; Maimon & Louderback, 2019). The situational context, like the external factors that influence and motivate an offender's behavior during the development of an online fraud event, can be observed through the linguistic cues used by other offenders to defraud others (Atkins & Huang, 2013; Cornish & Clarke, 2003, p 52; Pellon & Anesa, 2019). Specifically, research suggests fraudsters deploy a high frequency of linguistic cues of delay (i.e., "wait" and "hold") and urgency (i.e., "hurry" and "ASAP") to trick (i.e., deceive) targets into falling victim to an online fraud attack with emerging research suggesting the frequency of fraudsters use of these cues depend on the timing of the fraud event (Atkins & Huang, 2013; Maimon et al., 2020; Pellon & Anesa, 2019; Zhou et al. 2002). For instance, Maimon et al. (2020) research found that 18% of fraudsters' first messages to their targets contained urgency cues. As the online fraud event developed, 70% of fraudsters' subsequent emails contained urgency cues. The 52% increase of urgency cues used by fraudsters in written communications to defraud targets after their initial emails suggests linguistic cues play a critical role in the development of online fraud attacks.

Additionally, research indicates the situational context, such as an offender's employment position and the location of where a juvenile delinquent lives, influences offenders' interactions

[23] Digital platforms like eBay and Craigslist advertisements or Nigerian scams via email.

(Anderson & Meier, 2004, p. 420; Benson et al., 2009, p. 183). White-collar criminals, for example, decide to defraud others based on information they obtain from interactions with their targets (i.e., customers) through direct conversations or access they have to sensitive and financial information (Benson et al., 2009, p. 183). Specific to online communications, research suggests that the situational context influences deceptive users' interactions with truthful users. Zhou et al (2002) research, for example, suggests that deceptive users communicate in words that are on average shorter in length compared to honest users (Zhou & Zang, 2004; 2008).

The use of deceptive communication can present unfavorable outcomes (e.g., victimization) for fraudsters [offenders] who often interact with other offenders. In this instance, the offender also becomes a victim, presenting a victim offender overlap. Over the past four decades, research has indicated an offender and victim overlap (see Reiss, 1981; Berg & Schreck, 2021) with offenders who are often "repeatedly victimized" within the physical environment (see Erdmann & Reinecke, 2021, p. 9318). Emerging research suggests offenders reproduce the dangers of the physical environment within the online environment using technological advancements such as encryption to avoid detection (Smoak & Liu, 2006; Urbanik & Haggerty, 2018). Because offenders and victims may not be distinct, one area of interest is the tactics used against victim offenders in comparison to victims who are not offenders. Nevertheless, much uncertainty still exists about the relationship between fraudsters[24] [offenders] and the offender victims they target, which begs the question, "What situational factors support the development of a successful online fraud event against other offenders?"

[24] Another name for a fraudster who defrauds another fraudster [offender] is a ripper. Ripper comes from the slang word "ripped off" and thus has a negative connotation. Therefore, fraudsters may be referred to as rippers because this study focuses on offenders who victimize other offenders.

To explore the relationship between fraudsters [offenders] and offender victims online, the current study investigates the influence of rippers' decision-making processes through computer-mediated communication with their targets on Telegram channels using a mixed-methods analysis. Telegram channels are online forums where illicit activity has been reported like the selling and purchasing of stolen bank accounts and credit card information. There are various forums in addition to the illicit online fraud forums on Telegram, like channels where news or pop culture is discussed among computer users. Nevertheless, offenders actively use Telegram to communicate about their illicit transactions, including if they were ripped off during criminal activities. Consequently, some Telegram channels are online forums where fraudsters [rippers] are reported of defrauding victims of illegal purchases like stolen bank accounts.[25]

Furthermore, these Telegram channel forums provide researchers with a considerable amount of information on fraudsters' microsocial interactions with their targets. This information can be used to build upon what is known about offenders' interactions via previous research using crime scripts (Leclerc, 2013; Gilmore, 2014; Zhu et al., 2013). Crime scripts are researchers' attempts to describe and outline offenders' criminal engagement in step-by-step processes (Lavorgna, 2014). Crime scripts have assisted researchers in examining online fraudsters but fail to thoroughly account for the influence of human interactions during the development of online fraud attacks (Leclerc, 2013; Gilmore, 2014; Zhu et al., 2013). Considering human beings (i.e., offenders) use the situational context within the online environment to SE their fraudulent attacks, it is critical to account for offenders' and offender

[25] The dataset used in this study comes from correspondence between fraudsters who defraud (or rip) other fraudsters on illicit online fraud forums. Specifically, I used the digital written communications (i.e., qualitative) between fraudsters and offender victims to construct linguistic cue variables.

victims' interactions on a microsocial level, which requires more detail than what current crime scripts provide as it relates to online fraud.

In investigating rippers' decision-making, the criminal event perspective ("CEP") postulated by Short (1998) is applied as a framework with the support of interpersonal deception theory ("IDT") derived from Buller and Burgoon (1996). This theoretical framework is utilized to conceptualize fraudsters' decision-making processes through linguistic cues used in communications with offender victims. Specifically, Proposition 3 of IDT asserts deceptive users compared to honest users use more strategic activity, non-strategic arousal cues, and non-involvement (i.e., longer response times or disengagement in communication) to gather information from targets they intend to victimize. Additionally, I suspect the microsocial contextual and situational factors observed in CEP will support the development of a successful online fraud event against other offenders who are the targets of ripping victimization on Telegram channels. Therefore, I hypothesize deceptive offenders' [rippers] tactically[26] deploy linguistic cues against other offenders [victims] on Telegram channels and that these linguistic cues differ pre-offense versus post-offense[27] (with concomitant reverse patterns for offender victims) depending on the linguistic cues offender victims present to offenders [rippers].

3.2 Literature Review

3.2.a Online Fraud

The intentional act of deception resulting in personal and/or financial gain is fraud ("Fraud," 2019). Similarly, online fraud is the use of software with internet access or internet

[26] "Tactically" here refers to fraudsters' conscious and intentional actions to defraud targets. Specific to this study, offenders tactically (or intentionally) deploy specific linguistic cues.
[27] These linguistic cues serve as a binary variable, like yes (1) or no (0) before or after the fraud attack.

services to intentionally defraud others (FBI, n.d.). An offender or criminal who engages in online fraud is a fraudster. Fraudsters' intentional actions and interactions with targets to influence behaviors has been referred to as socially engineered (SE) tactics, often resulting in sensitive information and financial loss for the target, like credit card fraud (Rege, 2009; Hadnagy, 2010; Rege et al., 2019; Pellon & Anesa, 2019). Credit card fraud is the unauthorized use of credit cards. Carding is a slang term for the illegal activities involved in hiding unlawful credit card fraud transactions (Kigerl, 2018).

Online fraudsters' SE tactics involve the use of technological software or internet services to deceive targets into divulging sensitive or financial information while avoiding detection (Hadnagy, 2010, Hadnagy, 2018; Hadnagy, 2019). Fraudsters often embed pre-texting, the use of communication to build rapport with a target through an understanding of the target's contextual and situational environment, into SE attacks to appear legitimate to the target (Carnegie Mellon University, 2020).

Online fraudsters deploy various scams to conduct their fraudulent schemes. These scams include but are not limited to advance fee fraud (Gabosky, 2015), non-delivery scams (Almendra & Enachescu, 2012), and impersonation (Akins & Huang, 2013; Koch, 2017), with research suggesting that fraudsters' decision-making processes (e.g., characteristics and tactics) vary depending on the situational context (i.e., auction fraud scams compared to investment fraud scams) (Kigerl, 2018). Specifically, research indicates fraudsters' characteristics and tactics may differ in presentation to avoid detection (Aleem & Antwi-Boasiako, 2011; Atkins & Huang, 2013; Chang & Chang, 2014; Isacenkova et al., 2013; Jones & McCoy; 2014; Modic & Anderson, 2015; Park et al., 2014; Tzani et al., 2020; Van Der Zee et al., 2019).

A key factor/aspect of online fraudsters' decision-making processes is communication. This is exemplified in work undertaken by Maimon et al. (2020), whose research indicates that fraudsters' use of politeness and/or urgency cues will increase as communication continues with potential targets (Maimon et al., 2019). Similarly, Akins and Huang (2013) explored fraudsters' use of linguistic cues in 200 fraudulent emails and discovered variation among persuasion cues and triggers and the deployed scam tactic. For example, authority cues were present in 100% of the phishing emails but only present in 84% of advance-fee emails (Akins and Huang, 2013). In both phishing and advance-fee emails, urgency cues were equally present (e.g., 71% and 70% in the phishing and advance-fee emails, respectively). Additionally, Pellon and Anesa (2019) found the word "urgent" was present in 1.26 every 1,000 words of a written scam. These studies exemplify the variations of fraudsters' communication and deployed scam tactics.

Researchers have explored criminals' interactions specific to online marketplaces (Yip et al., 2013; Kigerl, 2018). For instance, Yip et al.'s (2013) carding marketplace analysis indicates users who are verified as legitimate fraudsters (or vendors[28]) communicate at a higher frequency within the forums compared to users who have not been verified as legitimate fraudsters (or vendors). To further emphasize the influence of communication among criminals within the cybercrime ecosystem, Dupont et al. (2017) examined the role of trust (e.g., authority) among hackers. They found that 90.7% of hackers identified (via written communication within the online hacking forum) the user who invited them to the website forum when the hacker accepted the invitation and first introduced themselves to others already on the forum (Dupont et al..2017). Taken together, this research highlights the critical role that fraudsters'

[28] A vendor is an individual or group of individuals who sell stolen products (i.e., bank accounts, social security numbers) and/or services to conduct online fraud (i.e., hacking instructions or "methods").

communications have during the development of an online fraud event, especially among other offenders.

Previous research has increased our understanding of fraudsters' decision-making processes (Atkins & Huang, 2015, Ferreria & Lenzini, 2015; Kigerl, 2018; Maimon et al., 2019; Maimon et al. 2020). So far, however, there has been little discussion about rippers' decision-making processes during the development of an online fraud event. What we know about online fraudsters' decision-making processes is limited by interactions between fraudsters and victims (Ferreria & Lenzini, 2015, Atkins & Huang, 2015) or is based mainly on observations of macrolevel interactions between offenders and nonoffending victims, not on illicit online fraud forums (i.e., cybercrime marketplaces) (Maimon et al., 2019; Maimon et al. 2020). Research has only begun to explore the phenomena of rippers on cybercrime marketplaces like their cashing out methods using non-offenders' personal, sensitive and financial information to obtain their illicit funds (Kigerl, 2018). To address this empirical gap, I explore rippers' decision-making processes within cybercrime marketplaces. My research is focused on the interactive communications between offenders and victims using the criminal event perspective (CEP) to frame communications with the support of interpersonal deception theory (IDT) to analyze the fraudsters' characteristics through linguistic cues (Atkins & Huang, 2015; Buller & Burgoon, 1996; Maimon et al., 2019; Short, 1998).

3.3 Theoretical Framework

3.3.a The Criminal Event Perspective (CEP)

Researchers have analyzed individuals' social interactions for decades (see Goffman, 1955). One of the most well-known criminological social interactions examinations is Short's

(1998) Criminal Event Perspective (CEP), a perspective that identifies, explores, and explains criminality during the microsocial development of a criminal event among offenders and victims. Similarly, criminologists have explored the contextual and situational context in criminals' physical environment (see Bierie et al., 2013), like offenders' demographics (e.g., age and location) and interactions (Anderson & Meier, 2004, p. 420; Benson et al., 2009, p. 183; Cornish & Clarke, 2003, p 52; Dickinson & Wright, 2015; Horney, Osgood, & Marshall, 1995, p. 667-669; Shaw & McKay, 1942; Topalli et al., 2002).

The situational context influences criminality (Anderson & Meier, 2004; Benson et al., 2009; Cornish & Clarke, 2003, p 52). For instance, the situational context, such as the desire for money, may influence an offenders' use of motivational cues[29] in criminal engagement (Anderson & Meier, 2004; Benson et al., 2009; Cornish & Clarke, 2003, p 52). Benson et al. (2009) research indicates the situational context, like an individual's place of employment, can influence their decision to engage in crime, specifically who they target to defraud. Specifically, white-collar criminals were motivated to defraud their clients of money and were capable of doing so because of their proximity to their financial funds (p. 182). Similarly, Cornish and Clarke's (2003) research indicates offenders' motivations, like monetary rewards, are positively associated with criminal engagement. Cornish and Clarke (2003) attest offenders will be motivated to engage in crime when they have an opportunity, and the ability to avoid detection using situational techniques to control their interactions (e.g., precipitator controls) (Cornish & Clarke, 2003, p. 52).

Anderson and Meier (2004) suggest that location (e.g., location of educational institutions) influences delinquency. Students, for example, attending educational institutions

[29] A motivational cue for offenders may be a desire for money.

located in urban areas were more likely to engage in delinquency than students attending educational institutions located in non-urban areas (Anderson & Meier, 2004). Research suggests the "microgeographic" or direct contextual and situational environment in which offenders are situated influences their interactions, specifically who they victimize (Konkel et al., 2021). Consequently, Anderson and Meier (2004) attribute students' delinquency to their location because students in urban areas typically are unsupervised after school. Students are unsupervised because they come from single-parent homes with a parent who generally is still working after school hours (Anderson & Meier, 2004).

The situational context also influences offenders who are engaged in illicit drug transactions. Research suggests drug dealers modify their behaviors depending on who they interact with (Dickinson & Wright, 2015; Topalli et al., 2002). By way of illustration, Dickinson and Wright's (2015) research suggests drug dealers will stop selling drugs to certain buyers to evade law enforcement detection. In a similar case, Topalli and colleagues' (2002) research suggests offenders "code switch" depending on the contextual and situational environment.

More recently, CEP has been used to explain deception involved in online crimes, like identity theft and fraud (Bossler & Berenblum, 2019; Maimon, Santos, & Park, 2019). For example, Maimon, Santos, and Park's (2019) research suggests offenders' verbal and non-verbal interactions (i.e., linguistic cues) influence offenders' use of urgency cues during the development of an online fraud incident. Maimon, Santos, and Park (2019) contend that written responses between fraudsters and targets (i.e., victims) are non-verbal social cues. Specifically, a target's first response back to a fraudster's probe email also acts as a non-verbal social cue confirming the suitability of the target for a SE fraud attack online. Therefore, the individual interactions discussed within the CEP helps frame the deceptive communications that transpire

within a fraudulent event. Because of this individualistic approach, microsocial theoretical perspectives can be used to explain the development of fraud.

3.3.b Interpersonal Deception Theory (IDT)

Interpersonal Deception Theory (IDT) is a communication theory used to explain the microsocial interactions between online fraudsters and targets within the cybercrime ecosystem (see Maimon et al., 2019). IDT, derived by Buller and Burgoon (1996), argues all communication, including deceptive communication, involves strategic and non-strategic behaviors. Buller and Burgoon (1996) thoroughly depict deceptive processes between senders and receivers in 18 Propositions. Proposition 3 is a key proposition in IDT that presumes deceitful individuals use more strategic activity (i.e., intentional actions) to comprehend information and non-strategic arousal cues and non-involvement than those who are honest.

Evidence-based research supports the propositions presumed in IDT and indicates criminals adapt their behaviors based on the feedback received from others to increase credibility and evade detection (Buller & Burgoon, 1996; Burgoon, Proudfoot, Schuetzler, & Wilson, 2014). An example of IDT from the communications literature that is applicable to criminology is the difference in language used between deceptive and honest callers and 911 operators (Burns & Moffitt, 2014; O.C.G.A. § 16-10-20 (2010). Specifically, Burns and Moffitt's (2014) research suggests deceptive callers communicate with a higher frequency of positive affirming words (i.e., “promise” and “vow”) to 911 operators than honest callers.

Deception is not a crime. However, offenders often employ deceptive tactics in communication when committing crimes, as demonstrated in Burns and Moffitt's (2014) research. Specifically, it is illegal to intentionally deceive 911 operators (see O.C.G.A. § 16-10-

20 (2010). Similarly, by definition, fraud always involves deceit (Fraud, 2019). Although IDT is a communication theory, the combination of IDT with the CEP as a framework helps extend the research concerning fraudsters' decision-making processes during the development of an online fraud incident. Specifically, elements of IDT (i.e., Proposition 3), like a deceiver's intentional interactions, help guide research on fraudsters, considering their interactions with targets are embedded in deceit (Buller & Burgoon, 1996).

3.4 Current Study

Using IDT and CEP as a guide, the following testable hypotheses were produced from my review of the existing literature. The hypotheses were constructed to examine offenders' [rippers'] decision-making processes on Telegram. Hence, drawing upon prior research, it is hypothesized that deceitful and delinquent individuals' motivations during an online fraud are associated with their contextual and situational environment. Furthermore, Proposition 3 of IDT asserts that, in contrast to individuals who engage in truthful communication, individuals who engage in deceitful communication use more strategic activity (i.e., specific information, idea(s), or concept(s)) to comprehend information presented to them and use more non-strategic arousal cues (i.e., longer responses times) and non-involvement by delaying or disengaging in communication (Anderson & Meier, 2004; Cornish & Clarke, 2003, p 52; Zhou et al. 2002). Therefore, I hypothesize offenders' [rippers'] tactical presentations of deception transform over time (Buller & Burgoon, 1996). Specifically, I hypothesize that offenders' deceptive tactics on Telegram channels will respond to offender victims' cues; thus, they will differ pre-offense versus post-offense (with concomitant reverse patterns for offender victims) based on previous

research that suggests the prevalence of fraudsters specific linguistic vary as an online fraud event develops (Maimon et al., 2019; Maimon, et al., 2020).

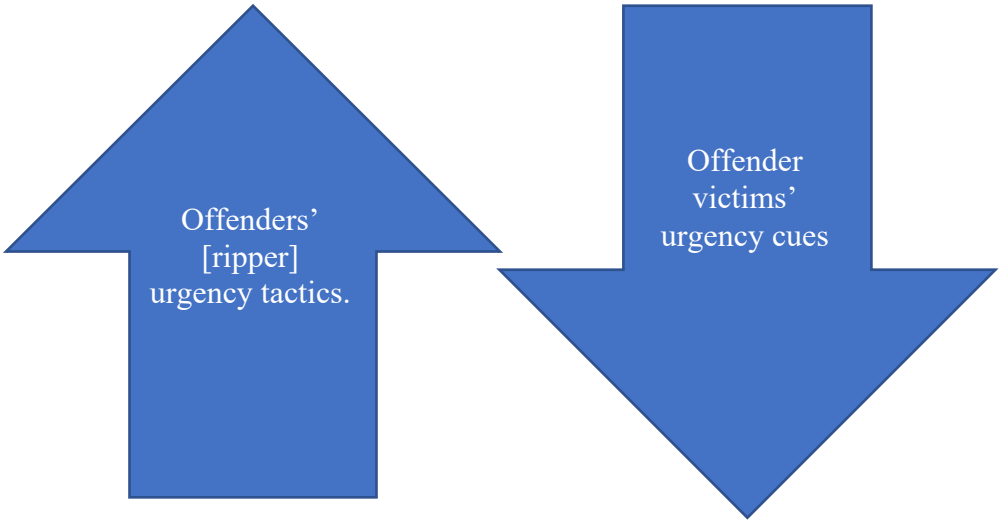
I account for the situational context of offenders' interactions with offender victims, specifically offenders' decision-making processes (via deployed linguistic cues of delay and urgency) with offender victims, during the development of an online fraud event with various pathways detailed in Figure 3.

As observed in Figure 3, it is hypothesized that (A) the prevalence of offenders' [rippers] urgency tactical cues will be higher than offender victims' urgency cues before a fraud event. The presentation of these linguistic cues sent by offenders [rippers] and offender victims transforms after a fraud event. Specifically, (B) the prevalence of offenders' [rippers] urgency tactical cues will be lower than the prevalence of offender victims' urgency cues after a fraud event.

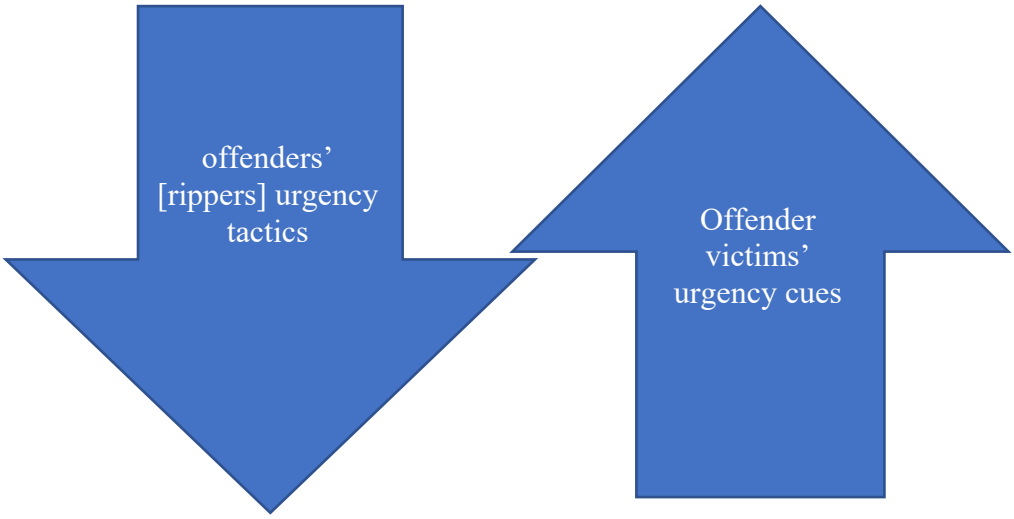
Similar to the hypothesized transformation of urgency cues, it is hypothesized the prevalence of delay cues will be transformed. Specifically, (C) the prevalence of offenders' [rippers] delay tactical cues will be lower than offender victims' delay cues before a fraud event. Alternatively, (D) the prevalence of offender' [rippers] delay tactical cues will be higher, compared to the prevalence of offender victims' delay cues after a fraud event.

Figure 3. Offenders' [Rippers] Deceptive Tactics and Offender Victims' [Fraudsters] Urgency Cues Outlined.

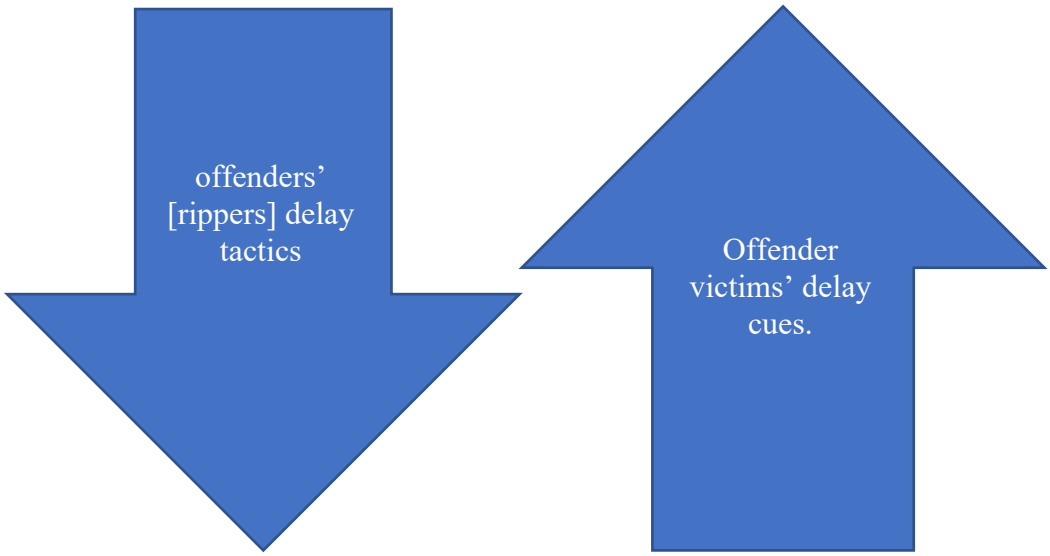
A. Urgency Cues Before the Fraud Event



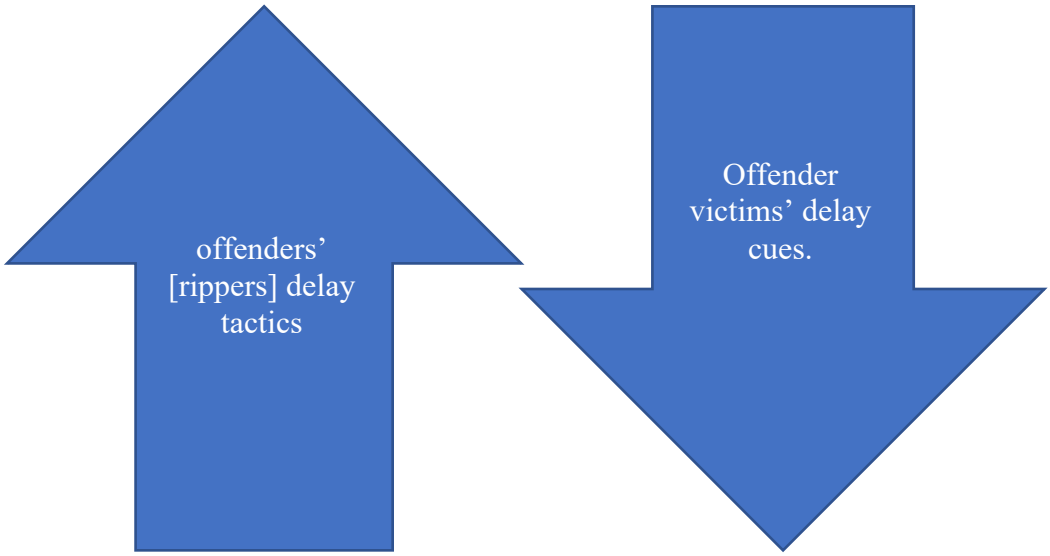
B. Urgency Cues After the Fraud Event



C. Delay Cues Before the Fraud Event



D. Delay Cues After the Fraud Event



The following study accounts for offenders' decision-making processes, such as the situational and contextual interactions between offender and offender victim, during the development of an online fraud event. Research emphasizes how fraudsters attempt to avoid detection in their interactions (via linguistic cues), especially with products or services in high demand among targets (i.e., customers, Stanelyte et al., 2022) (Hadnagy, 2010, Hadnagy, 2018; Hadnagy, 2019). Yet, researchers have not accounted for how offenders [fraudsters] interact with offender victims via linguistics cues deployed before and after a fraud event to offender victims, which may be tactically used to support their online schemes. Therefore, I hypothesize contextual and situational factors will support the development of a successful online fraud event against other offenders who are the targets of ripping victimization on Telegram channels.

A. Specific to linguistic cues, I hypothesize offenders' [rippers] urgency tactics, such as urgency linguistic cues (i.e., "ASAP"), will be more prevalent before the completion of an online fraud event compared to offender victims' [fraudsters] cues of urgency (e.g., "now"). Alternatively, urgency cues will be more used more frequently by offender victims' [fraudsters] than offenders' [rippers] after the completion of an online fraud event.
B. I hypothesize offenders [rippers] delay tactics (i.e., "wait") will not be as prevalent compared to offender victims' delay cues before the completion of an online fraud event. Alternatively, offender victims' [fraudsters] delay cues (i.e., "hold") will not be as prevalent after the completion of an online fraud event compared to offenders' [rippers] delay tactics.
C. I hypothesize that the prevalence of offenders' tactical urgency cues before the fraud event and delay cues after the fraud event will be higher for stolen personal, sensitive

and financial information of non-offending victims compared to unknown products and/or services stolen.

D. I hypothesize that reports of monetary losses will be higher when the offender deploys tactical urgency cues before the fraud event and delay cues after the fraud event.

E. I hypothesize that the mean for offender victims' messages is higher when offenders' urgency cues before a fraud and offender delay cues after a fraud event.

3.4.a Methodology

Deibert and Miethe's (2003) approach was used to examine the sequence of events in an online fraud event. Specifically, Deibert and Miethe's (2003) approach guided me in the collection of textual data (e.g., temporal sequencing of action) among users on the Telegram channels where fraudulent behaviors were reported (N=225). Georgia State University's Institutional Review Board (IRB) approved the study.

3.4.b Procedure

I systemically selected fifty-five Telegram channels where fraud information is reported to have been distributed.[30] The channels were selected using the following search terms associated with online fraud on Telegram: 1) Carding, 2) Fraud, 3) Rip, and 4) Scam. I listed my search terms in alphabetical order, searched each term once, and joined the top, relevant yielded result. I explored each selected channel and joined the most recent advertised online fraud

[30] The decision was made to identify only 55 Telegram channels due to the amount of data Telegram illicit marketplaces provide, which I had the responsibility to monitor. It took me approximately 50 hours a week to monitor 55 channels.

channel listed in the prior twenty-four hours.[31] I repeated this pattern, starting with the word carding, which appeared at the top of the alphabetized list until I had fifty-five channels. Of the 55 channels, only 52 channels could be analyzed because of language barriers[32] and technological issues.[33] However, these 52 channels were among the busiest that I identified in terms of traffic and are likely to represent the typical offenders involved in online fraud. Detecting their presence on channels is already limited because of the deception used by online fraudsters.

The current study explores how offenders' decision-making processes contribute to a successful scam online among fraudsters. I separated the channels into two categories for analysis. I placed all the channels where fraud services and products were actively being sold into one category and termed them "ripping channels." The second category of Telegram channels contained 13 channels and was termed "exposure channels." Exposure channels had minimal to no active sales of stolen or illicit content and were dedicated to exposing offenders who had "ripped off" or defrauded other Telegram users. Offenders and victims commonly referred to these channels as "Ripper Walls."

I focus my analysis in this study on "exposure channels" or "Ripper Walls" because these channels provided more data (i.e., message screenshots between offenders and offender victims) specific to the digital interactions between fraudsters and offender victims (via communications) during the development of online fraud events compared to active illicit online fraud forums. Each channel was monitored daily, and I exported all the data from these channels every Friday for 12 weeks. The export acquired, downloaded, and output past conversations and uploads from

[31] Several of the channels did not have additional channels advertised in the prior 24 hours.
[32] An example of a language barrier I was faced with is how one of the channels was in Chinese and I cannot speak or read Chinese.
[33] Several of the channels would not download completely each week.

the channels, including but not limited to pictures, videos, and files. Therefore, my data collection included written texts and photographs uploaded by users on these channels.

3.4.C. Sample

At the start of this research study, 242 conversations were initially observed but there was not enough information to identify that a fraudulent event occurred and so those conversations were removed from this study. The unit of analysis in this study is *conversations* (N=225) because I am exploring the contextual and situational environment of offenders' decision-making processes during the development of an online fraud event. Each offender and offender victim was assigned a unique identifier in the examined conversations. Each instance of fraud reported on the "Ripping Walls" was manually documented and analyzed. Then, I inputted the documented conversations into Nvivo and conducted a qualitative analysis to identify instances of ripping. Nvivo (n.d.) is a data software analysis tool used to organize unstructured and qualitative data like interviews and conversations.

I used Maruna's (2010) manifest content analysis approach to analyze the data. Manifest content analysis is a research technique that guides researchers in gathering evidence of the direct dialogue (via qualitative data) exchanged between individuals.[34] Specifically, Maruna's (2010) manifest content analysis approach guiding me in operationalizing offenders and offender victims' written texts and cues for reported fraud instances (via screenshotted conversations) on "Ripping Walls" (Field, 2013). For example, I used Maruna's techniques for content coding because it is an effective approach for mixed-method studies. I adopted Maruna's content coding technique to code the observed qualitative data. Content coding helped me review lengthy

[34] This interaction can occur between the subject (i.e., offender) and the interviewer (i.e., researcher and/or victim, etc.).

messages between offender and offender victims and sort them into simpler categories allowing for easy management and in-depth analyses of my qualitative findings (Maruna, 2010). Specifically, I observed and identified themes (e.g., urgency and delay tactical cues)[35] while reviewing the collected conversations for assessment of stolen product and/or service and monetary losses.

Previous studies have successfully used a manifest content analysis to examine the sequence of events (i.e., crime scripts) involved in online fraud using computational tools to detect offenders' behaviors (Zhu et al., 2013). Specifically, Zhu et al.'s (2013) hierarchical sequence of an online fraud event used a manifest content analysis to analyze fraudsters' written texts and cues. Therefore, I used a manifest content analysis to explore offenders' various decision-making processes researchers typically do not address. Specifically, each conversation was coded for the following variables (1) offender, (2) report by offender victim or victim advocate,[36] (3) offenders' deployed urgency tactics before a fraud event, (4) offenders' deployed urgency tactics after a fraud event, (5) offenders' deployed delay tactics before a fraud event, (6) offenders' deployed delay tactics after a fraud event, (7) offender victims' presentations of delay cues before a fraud event, (8) offender victims' presentations of delay cues after a fraud event, (9) offender victims' presentations of urgency cues before a fraud event, (10) offender victims' presentations of urgency cues after a fraud event (11) total frequency of offenders' messages, (12)total frequency of offender victims' messages, (13) reported financial amount lost (in USD), and (14) fraud product and/or service stolen.

[35] See Appendix A. Urgency and Delay Linguistic Cues Categized by themes.
[36] Victim advocate is a user who was not defrauded by the ripper but reports the fraud victimization on behalf of the offender victim. I observed victim advocate's reporting rippers or ripping instances when offender victims no longer had access to their accounts and/or the Telegram channel where the fraud occurred.

Research indicates that fraudsters deploy urgency and delay cues during the development of an online fraud event (Atkins & Huang, 2015; Pellon & Anesa, 2019). I structured my qualitative data in the following method but was cognizant of salient linguistic cues.[37] Urgency and delay tactical cues, for example, are not mutually exclusive because linguistic cues are dependent on the contextual and situational interactions during communications (i.e., "socially shared "gists") (Luangrath et al., 2107; Sidi et al., 2021).[38] Consequently, I could not separate the number of times a cue was sent before and after a fraud event to account for the number of times a cue was used. Therefore, building upon prior research, I used the unstructured conversations to inform and construct the following analyzed measures: (1) offender urgency tactics, (2) offender delay tactics, (3) offender victim urgency cues, and (4) offender victim delay cues.[39, 40, 41]

An example of urgency tactics used by offenders from the data is how offenders would rush offender victims into disclosing sensitive or financial information with words like "ASAP" or sentences like "Now send me screenshot" and "Lmk ASAP cuz I gotta go." Additionally, offenders deployed delay tactics to offender victims with words like "wait" and sentences like "I

[37] See Appendix A. Urgency and Delay Linguistic Cues Categized for the specific linguistic cues that were not "linguistical "gists"" that helped me identify offender and offender victims' urgency and delay cues. A (linguistic) "gists" is substance or the main point of speech ("Gist", 2022). An example of this is how someone might say "what's up" and the "gist" of what they are saying "how are you" rather than "what is actually up in direction."
[38] I was limited in analysis because of linguistical "gists" (Luangrath et al., 2107; Sidi et al., 2021). See Appendix A: Evidence from data, for how expressive and/or paralinguistic cues are often viewed as linguistical "gists" that can limit a researcher in analysis.
[39] Atkins and Huang's (2013) analysis of fraudsters linguistic cues was built upon Capaldi (1971), Huang and Brockman (2011), and Ross (2009) prior research of linguistic cues of persuasion.
[40] The frequency of offender urgency tactics, (2) offender delay tactics, (3) offender victim urgency cues, and (4) offender victim delay cues before and after the fraud event could not be measured. This is because some messages from offenders and offender victims were consecutive and the preceding message was needed to elicit urgency or delay (Luangrath et al., 2107; Sidi et al., 2021). Therefore, the measures offender urgency tactics, (2) offender delay tactics, (3) offender victim urgency cues, and (4) offender victim delay cues are binary.
[41] These linguistic cues (i.e., urgency and delay tactics and presentational cues) vary depending on the discipline (i.e., sociological field compared to the psychological field compared to the criminological field) because expressions differ and change depending on the perceptions of victims and the tactics offenders deploy (Atkins & Huang, 2013; Capaldi, 1971; Huang & Brockman, 2011; Ross, 2009)

was sleep bro" and "Sorry for the delay I was really busy helping someone else too." Similarly, I accounted for and clustered offender victims' presentational cues into two distinct categories: urgency and delay. An example of urgency cues presented by offender victims from the data is how offender victims correspond with offenders with words like "now" and "ready" and sentences like "You going on both ripper walls if u dont send For instance, the offender victim stated during conversation with an offender, "I see exactly what your doing…its you had two weeks to add the address… wasting my time…send now". Alternatively, offender victims present delay cues in correspondence with offenders through words like "wait" or sentences like "I will send 4". For example, an offender [ripper] stated during a conversation with a victim offender "… now im a ripper… give me a min I'm busy rn… it was my boys bday niggas was offa perc Nd drank ofc I'm not gon b as active.." to delay a target.

3.4.c.a Dependent Measures. Research suggests the initial presentation of written text and situational cues (i.e., motivational cues and precipitator controls) determine the non-verbal and verbal cues presented throughout a deceptive online event (Cornish & Clarke, 2003, p. 52; Zhou et al., 2003). Therefore, the situational variables, *offenders' use of urgency tactics* and *delay tactics,* were created and measured on a nominal scale (*urgency tactics before fraud event= 0; urgency tactics after fraud event= 1; delay tactics before fraud event= 0; delay tactics after fraud event= 1).*

3.4.c.b Key Independent Measures. Although it is impossible to control for the contextual and situational environment surrounding offenders perfectly, Wortley (1997, p. 45) stressed the importance of examining these elements to comprehensively analyze offenders'

characteristics and tactics during the development of an online fraud event (Cornish & Clarke, 2003). For that reason, I created variables to account for the influence of the situational context during the development of an online fraud event: (1) offender victim use of urgency cues, (2) offender victim use of delay cues, (3) offenders' frequency of messages, (4) offender victims' frequency of messages and (5) financial amount lost in United States dollars (USD), and (6) stolen product and/or service.

The variables, *offender victim use of urgency cues,* and *offender victim use of delay cues*, were created to account for the situational contextual of offender victims' presentation during the development of an online fraud event and were measured on a nominal scale (no offender victims' presentation of urgency cues present = 0; offender victims' presentation of urgency cues present =1; offender victims' presentation of delay cues present= 0; offender victims' presentation of delay cues present= 1). The variable, *financial amount lost in United States dollars (USD*), was created to account for the reported monetary losses during an online fraud event and measured on a continuous scale. Financial amount may be related to urgency because rippers are eager to get victims money quickly; however, when victims become suspicious about the creditability of the fraudster [ripper], the fraudsters may use delay cues (i.e., "wait", "hold") for monetary gain. The variable, *stolen product and/or service,* was measured on a categorical scale (not stated= 0; non-offending victims' stolen personal, sensitive, and financial information = 1; documents (i.e., online theft methods; crypto)).

3.4.d Analytic Strategy

As previously stated, I conducted a mixed-methods analysis with the data. Specifically, I used the qualitative data to construct the quantitative variables. The quantitative variables

granted me the ability to assess the association between the two main dependent variables of interests, offenders' urgency and delay tactical cues, and the key contextual and situational environmental variables in a series of bivariate analyses (Farrington and Loeber, 2000). Specifically, the series of bivariate analyses allowed me to assess the association between offenders' tactical cues and situational context variables. The nature of the linguistical "gists" observed within the analyzed conversations limited how I could quantify my key dependent variables (i.e., binary) (Hotelling, 1935).

3.5 Results

The 225 observed fraud conversations are described in Table 2. As presented in Table 2, offenders employed urgency tactical cues in 10% of messages to offender victims before the completion of an online fraud event. Alternatively, only 1% of the messages from offenders to offender victims after the online fraud event contained urgency tactical cues. Only one offender deployed delay tactical cues before the completion of an online fraud event to offender victims (0.44%). On the other hand, offenders employed delay tactical cues to offender victims in 41% of messages after completion of a fraud event.

Offender victims presented urgency cues in 1% of the messages sent before the fraud event. In comparison, offender victims presented urgency cues in 22% of the messages sent after the completion of the fraud event to offenders. Offender victims presented delay cues in 8% of messages before and only one offender victim presented delay cues after the completion of the fraud event to offenders.

Specific to the contextual variables, the average amount of losses reported was $807.35. The average number of messages sent by offenders to offender victims and offender victims to

offenders during the development of an online fraud event was 18.18 (SD=28.60) and 24.87 (SD= 33.98), respectively. Most of the stolen products and/or services were not stated (M=40), although 35% of the stolen products and/or services were documents (i.e., online theft methods; crypto) and 24% of the stolen products and/or services were non-offending victims' stolen personal, sensitive and financial information.

Table 2. Descriptive Statistics (N= 225 Fraudent Interactions/Conversations)

Variables			**Minimum-Maximum**
Dependent Variables			
Offenders' [Ripper] Tactics			
Urgency Tactics	**%**	**N**	
Before Fraud	9.78	22	0-1
After Fraud	.89	2	0-1
Delay Tactics			
Before Fraud	.44	1	0-1
After Fraud	41.33	93	0-1
Independent Variables			
Motivations			
Offender Victims' Presentation Cues			
Urgency Cues	**%**	**N**	
Before fraud	1.33	3	0-1
After fraud	22.22	50	0-1
Delay Cues			
Before Fraud	8.00	18	0-1
After Fraud	.44	1	0-1
	M	**SD**	
Financial Information			
Financial Amount Lost (in USD)	$807.35	$3,374.72	$.08- $430,000.00
Motivations			
Message Frequency (i.e., position/location)			
Offenders' Frequency of Total Messages	18.18	28.60	1-249
Offender Victims' Frequency of Total Messages	24.87	33.98	1-328
Stolen Product and/or Service	.96	.87	0-2
Not Stated	.40	.49	0-1
Non-offending victims stolen personal, sensitive and financial information	.24	.43	0-1
Documents (Paperwork (i.e., Methods, PPP)	.35	.48	0-1

Table 3 presents a series of chi-square analyses between the two main dependent variables of interest (i.e., offenders' urgency and delay tactical cues) and the independent

variables reflecting offender victims' presentational cues of delay and urgency. The preliminary findings suggest a relationship between written urgency cues used by offenders and offender victims before an online fraud event. Specifically, 9.78% of written communications from fraudsters before a fraud event contain urgency cues, while only 1.33% of written communications from offender victims before a fraud event contain urgency cues ($p < 0.0$).

Alternatively, the bivariate analysis of offenders and offender victims' urgency cues after a fraud event, offenders and offender victims' delay cues before a fraud event, and offenders and offender victims' delay cues after a fraud event, revealed no statistically significant relationships. Nevertheless, it is important to note that 41.33% of offenders written communications after a fraud event contained delay cues and only two conversations contained urgency cues, which highlights offenders intentional decision-making processes to deploy specific linguistic cues during the development of an online fraud event.

Table 3. Bivariate Analysis between Offenders' and Offender Victims' Linguistic Cues before and after a fraud event.

Groups	**Fraudsters % (N)**	**Offender Victims % (N)**	**χ^2 (Fishers Exact)**
Urgency Cue Before Fraud	9.78 (22)	1.33 (3)	11.15*
No Urgency Cue Before Fraud	90.22 (203)	98.67 (222)	
Urgency Cue After Fraud	.89(2)	22.22(50)	.90[a]
No Urgency Cue After Fraud	99.11(223)	77.78(175)	
Delay Cue Before Fraud	0.44(1)	8.00(18)	.09[a]
No Delay Cue Before Fraud	99.56(224)	92.00(207)	
Delay Cue After Fraud	41.33(93)	.44(1)	.71[a]
No Delay Cue After Fraud	58.67(132)	99.56(224)	

*p<.001 [a] The number of cases in these cells was below five; thus, Fisher's Exact test was used as the measure of association.

Additionally, a series of chi-square analyses were conducted to examine the relationship between offenders' linguistic tactical cues before and after an online fraud event and stolen

product and/or service and financial amount lost (in USD). Turning to Table 4, we observe no statistically significant relationship between offenders' linguistic tactical cues before and after an online fraud event and the type of stolen product and/or service. Although there is no statistically significant relationship between these variables, it is of importance to highlight offenders use of delay cues after the completion of a fraud event because it appears a similar percentage of conversations involve fraudsters deploy delay cues regardless of the products and/or services defrauded from their victim (38%, not stated; 44%, non-offending victims stolen personal; 43%, documents)

Table 4. Bivariate Analysis between Offenders' Linguistic Tactical Cues and Stolen Product and/or Service.

Groups	**Not Stated** % (N)	**Non-offending victims stolen personal, sensitive and financial information** % (N)	**Documents (Paperwork (i.e., Methods, PPP)** % (N)	**χ^2 (Fishers Exact)**
Offender Urgency Before Fraud Event	12.09 (11)	9.09 (5)	07.59 (6)	1.01
Offender Urgency After Fraud Event	1.10 (1)	1.82(1)	.00 (0)	.52[a]
Offender Delay Before Fraud Event	.00(0)	.00 (0)	1.27(1)	.40[a]
Offender Delay After Fraud Event	38.46 (35)	43.64(24)	43.04 (34)	0.52

[a]The number of cases in these cells was below five; thus, Fisher's Exact test was used as the measure of association.

Table 5 presents the series of independent samples t-tests comparing the financial amount (in USD) lost when offenders use and do not use linguistic tactical cues before and after an online fraud event. The analysis suggests that the use of urgency cues before the fraud event by an offender is related to the amount of money lost. Specifically, the mean amount of losses when offenders use delay cues after a fraud is $1,376.90 compared to $311.78 when delay cues are not

used by the offender. The t-test for the difference in mean amount lost when offenders use and do not use urgency cues was not significant. Nevertheless, the mean values suggest that the mean amount lost is higher when offenders use urgency cues. T-tests were unable to be performed for the mean values lost and offender urgency cues after a fraud and offender delay cues before because there was only one case in each. However, it does appear that the mean values are higher when offenders do not use urgency cues after a fraud or delay cues before.[19]

Table 5. Bivariate Analysis between Offenders' Linguistic Cues and Financial Amount Lost (in USD).

Variables	**Yes=1**	**Amount Lost in USD**		
Offender Linguistic Cues	**(Present)**	**M**	**SD**	**t-statistic**
Offender Urgency Cues Before Fraud	Yes	$1,724.83	$4,561.84	-1.15
	No	$692.67	$3,200.98	
Offender Urgency Cues Before Fraud	Yes	$2.01	--	--[b]
	No	$812.99	$3,385.90	
Offender Delay Cues Before Fraud	Yes	$91.76	--	--[b]
	No	$812.36	$3,386.04	-3.85
Offender Delay Cues After Fraud	Yes	$1,376.90	$4,840.26	-4.36**
	No	$311.78	$740.47	

** $p < 0.01$; [b] There was only one case in each of these yes groups; thus, the mean value could not be calculated nor a t test performed.

Table 6 and Table 7 illustrate a series of t-test analyses examining the frequency of messages of offender victims and offenders' use of tactical linguistical cues and the frequency of messages of offenders and offender victims' linguistical cues during the development of an online fraud event. Table 5 provides the results obtained from a series of independent sample t-tests comparing offenders' linguistic cues and the total frequency of messages sent from offender victims to offenders. Offender victims send a higher number of messages to offenders [rippers] when offenders use tactically deploy urgency cues before a fraud event ($M= 46.27$, $p \leq 0.001$).

Offender victims send a greater number of messages to offenders [rippers] when offenders tactically deploy delay cues after a fraud event (M= 36.19, $p \leq 0.0$) as compared to when offenders do not use delay cues after a fraud event. Alternatively, there was no statistically significant difference in the mean level of offender victim message frequency when offenders' use urgency cues after a fraud event and when they do not.[42]

Table 6. Independent Group T-test Comparing the Total Message Frequency of Offender Victims' and the Presence of Offenders' Linguistic Cues.

Variables	**Yes=1 (Present)**	**Offenders Victims' Message Frequency**		
Offender Linguistic Cues		**M**	**SD**	**t-statistic**
Offender Urgency Cues Before Fraud	Yes	46.27	57.44	3.17*
	No	22.55	29.71	
Offender Urgency Cues After Fraud	Yes	10	2.82	.62
	No	25.00	34.10	
Offender Delay Cues Before Fraud	Yes	45	--[b]	--[b]
	No	24.78	34.02	-3.85
Offender Delay Cues After Fraud	Yes	36.19	45.30	4.36*
	No	16.89	19.43	

*$p < 0.001$ [b] There was only one case in each of these yes groups; thus, the mean value could not be calculated nor a t test performed.

Table 6 provides the results obtained from a series of independent group t-tests comparing the total message frequency of offenders and offenders' presentation of tactical linguistic cues before and after a fraud event. The findings indicate that offenders' send a greater number of messages to offender victims when offenders victims present urgency cues after a fraud event compared to when they do not use these cues (M= 23.92, $p \leq 0.05$). Offenders send a greater number of messages to offender victims when offenders victims present delay cues

[42] See footnote 19.

before a fraud event as compared to when they do not (M= 42.33, $p \leq 0.0$). Alternatively, no other statistically significant relationship was observed between the offender's total message frequency and offender victims' urgency cues before a fraud event or offender victims' delay cues tactics after a fraud event.

Table 7. Independent Group T-test Comparing the Total Message Frequency of Offenders' and the Presence of Offender Victims' Linguistic Tactical Cues.

Variables	**Yes=1 (Present)**	**Offenders' Message Frequency**		
Offender Victims Linguistic Cues		**M**	**SD**	**t-statistic**
Offender Victim's Urgency Cues Before Fraud	Yes	16.67	8.08	.09
	No	18.20	28.78	
Offender Victims' Urgency Cues After Fraud	Yes	23.92	26.90	1.61*
	No	16.54	28.93	
Offender Victims' Delay Cues Before Fraud	Yes	42.33	54.47	3.85**
	No	16.08	24.27	
Offender Victim's Delay Cues After Fraud	Yes	149	--[b]	--[b]
	No	17.60	27.29	

*$p \leq 0.05$; ** $p < 0.001$; [b] There was only one case in each of these yes groups; thus, the mean value could not be calculated, nor a t test performed.

3.6 Discussion and Conclusion

The principal objective of this study was to investigate offenders' decision-making processes, specifically fraudsters' tactical linguistic cues, during the development of an online fraud event when defrauding other offenders (Buller & Burgoon; 1996; Short, 1998). The current analysis is important because little attention has been given to fraudsters' decision-making processes (i.e., modus operandi) when targeting other offenders. Based upon previous research, we would expect the situational context to influence offenders' online interactions (Kigerl, 2018;

Kigerl, 2020). The CEP along with IDT was used to frame offenders and offender victims' interactions to analyze fraudsters characteristics (via linguistic cues) because prior research indicates the situational context influences fraudsters interactions (Atkins & Huang, 2015; Buller & Burgoon, 1996; Maimon et al., 2019; Short, 1998). The analyses produced several key findings related to fraudsters' situational contextual environment (Buller & Burgoon, 1996; Short, 1998).

It is apparent from the series of chi-square analyses and independent group t-tests that offenders' tactical cues depend on the situational context. Specifically, offenders' use of tactical urgency cues before the fraud are associated with offender victims' presentational cues of urgency. The findings indicate that additional variables associated with the situational context, such as the frequency of messages sent during an online fraud event by offenders and offender victims, along with the monetary amount stolen, could influence offenders during the development of an online fraud event.

First, offenders use of tactical cues of urgency were present in 10% of messages before the completion of an online fraud event, which aligns with recent research (Maimon et al., 2019). Although not statistically significant, offenders' tactical cues of delay after completion of an online fraud event were prevalent (41%) in contrast to previous research (Pellon & Anesa, 2019) in which words of delay are used to signal urgency cues to defraud a target quicker (e.g., "do not wait or you will lose this offer").[43] The difference may be attributed to the type of fraud committed by the offender. For example, Pellon and Anesa' (2019) research explored offenders'

[43] Pellon and Anesa's (2019) research suggests that words used by fraudsters associated with delay like "wait" were also used to nudge (or rush) a target into a specific action (see Appendix A for a thorough breakdown of fraudsters' use of linguistic cues, including an explanation of linguistic "gists").

delay cues deployed in advance free frauds versus nonpayment fraud as examined in Maimon et al.'s (2019) research, while this research examined offender on offender interactions.

These findings highlight the influence of the situational context on offenders' interactions with targets (Short, 1998). The observations from the series of chi-square analyses highlight the statistically significant relationship of offenders' tactical urgency cues and offender victim use of urgency cues before the completion of an online fraud event. Offenders' use of tactical urgency cues after the completion of an online fraud event and offender victims' use of these cues are not statistically significant. Additionally, the findings regarding offenders' use of tactical delay before and after the completion of an online fraud event and offender victims' use of these cues are not statistically significant. Though insignificant, the higher frequencies highlight offenders use of cues against other offenders (i.e, offender victims).

Taken together, offenders [rippers] perhaps deployed different tactical linguistic cues of delay, or as Proposition 3 of IDT suggests, non-strategic arousal cues and non-involvement, upon the completion of an online fraud to cast a wider net of offenders to victimize. For instance, offenders [rippers] may avoid detection and "buy time" before being identified by another offender as a "ripper" within their illicit marketplaces through the use of delay cues (Buller & Burgoon, 1996; Kigerl, 2018; Kigerl, 2020). Furthermore, the highlighted interactions are interesting considering previous research highlights the prevalence of offenders' linguistic delay cues during fraudulent interactions online against non-offending victims (see Pellon &Anesa, 2020), which consequently emphasizes the importance of examining offenders during their interactions and not solely based on overall "crime scripts" related to specific crimes (Lavorgna, 2014; Leclerc, 2013; Gilmore, 2014; Zhu et al., 2013).

Secondly, the evidence presented confirms the influence of the situational context, like the influence of offenders' tactical use of delay cues on monetary rewards (Akins & Huang, 2013; Maimon et al., 2019; Zhou & Zhang, 2004; 2007). For example, when offenders used delay cues after a fraud event the mean average of losses was $1,376.90 compared to when offenders did not use delay cues after a fraud event ($311.78, $p < 0.01$).

What stands out between Tables 5 and 6 is the difference between offenders and offender victims' utilization of cues and message frequency. For example. Table 5 shows a lower number of offender victims' messages when offenders use urgency cues before fraud, whereas Table 6 shows there is no statistically significant difference in message frequency when offender victims' use urgency cues before fraud and when they do not. Previous research (see Zhou & Zhang, 2004; 2007) suggests the frequency of messages differs between deceptive computer users compared to honest users. Zhou and Zhang's (2004; 2007) research suggests the average length of messages sent by deceptive users compared to honest users will be lower, and the results presented in this study support the relationship between deceptive users' interactions. Specifically, deceptive offenders' linguistic cues nudge offender victims to send a lower frequency of messages.

Additionally, the mean difference of offender urgency cues before the fraud and offender victims' prevalence of messages supports prior research that suggests the situational context like non-verbal cues (i.e., responding back to a message that says respond to verify via clicking on a hyper click) influence offenders' interactions (Akins & Huang, 2013; Pellon & Anesa, 2019; Maimon et al., 2019). In the current study, the mean for when offenders use delay and tactical cues of urgency and when they do not are reported. Reports of delay and urgency cues for offender victims to offenders and offenders' frequency of messages were also provided (see

Table 6). Specific to the statistically significant mean difference between offenders and offender victims message frequency and delay cues, offenders may non-verbally support their tactical delay cues by responding to offender victims' messages with a lower average of messages during the development of an online fraud event. The mean number of offender victims' messages to offenders and offenders' tactical delay cues may be higher to non-verbally nudge (via "blowing up") an offender's digital device to get them to respond. These interactions between offenders and offender victims highlight the influence of non-verbal cues (in support of Proposition 3) during the development of an online fraud event that are often not accounted for within the situational context of criminality (Buller & Burgoon, 1996). Regardless of the type of cue deployed by fraudsters, the current study highlights the types of linguistic cues used by offenders to defraud targets. This finding is important because it highlights the extent of manipulation tactics used by offenders to obtain the desired stolen products. In addition, some of offenders' tactical cues are associated with higher monetary losses. This finding illustrates the need for more effective prevention strategies due to the extent of money lost from victims regardless of their involvement in crime.

Future research will benefit from this study by conducting more in-depth analyses with larger sample sizes to inform policy and practice. For example, the FBI's Internet Crime Complaint Center (IC3) reported increasing rates of credit card losses. IC3 data are limited because they come from self-reported victims. IC3 fails to acknowledge that there are offender victims who mostly do not report their victimization; this, can be inferred by the situational context in which offender victims abide by the code of the street (Dickinson & Wright, 2015; Topalli et al., 2002). The code of the streets, or in this situational context the code of the keyboard, between offenders and offender victims, conceptually states, "you don't tell or type

about me, I don't type of tell on you." Consequently, these findings highlight the dark hidden figure of crime (e.g., offenders victimizing other offenders). Therefore, it is quite likely that the prevalence of online fraud is not accurately represented.

The current research on this topic informs educational institutions and agencies on the extent of victimization associated with fraudulent events online. Researchers, practitioners, and agencies can use these findings to improve their knowledge of offenders' decision-making processes, specifically the characteristics and tactics used to defraud targets, and victim typologies. Specific linguist cues, such as "ASAP," and "hurry," used *before* a fraud event with "hold," and "wait," *after* a fraud event by offenders to their "victims" signals fraudulent interactions between offenders (i.e., offender victims). Thus, these findings highlight the fact that online fraud cannot be solely combated with computational tools because human beings, especially offenders, uniquely vary in their deployed SE characteristics and tactics. Educational, privatized and governmental institutions can provide guidance to individuals through cybersecurity seminars, commercials, and community journals to bring awareness to the SE characteristics, such as offenders use of urgency and delay cues, deployed during an online fraud event.

Although the current study its strengths, it also has limitations. Specifically, the study used a small sample. Future research should include a greater number of conversations so that multivariate analyses can be conducted. Additionally, the relationship between offenders' tactical cues and offender victims' presentational cues might be stronger if the frequency of cues could be counted before and after the fraud event. However, the nature of the data with linguistic "gist" did not allow me to assess or measure for that. Additionally, offenders frequently would delete their conversations with offender victims, commonly referred to by the fraudster community as

"cleared/ing chats," to hide their interactions. Cleared chats makes it difficult to examine offenders' interactions and therefore impairs researchers' ability to account for those cases. Future researchers should account for the difficulties in generating large samples when conducting their research. Further, the nature of the internet (i.e., anonymity via encryption), especially among offenders who use encryption tools to hide their identity, creates difficulties in tracking actors involved during the development of an online fraud event (Erdmann & Reinecke, 2021; Jennings et al., 2011; Urbanik & Haggerty, 2018).

It is clear from the findings that the situational context influences offenders' decision-making processes, but the association depends on the actors' interactions. This research provides steps towards understanding the influence of the situational context on offenders' decision-making processes through their communications with targets and victims online. Although it can be challenging to examine offenders' decision-making processes because of the online environment (i.e., encryption tools), this study demonstrates the benefit of examining the situational context to identify fraudsters and their tactics to conduct fraud. Consequently, the current study contributes to understanding offenders' decision-making processes, provides evidence for the criminological field, and guides researchers in future online fraud research.

Chapter 4: Do Offenders [Fraudsters] "Collaborate and Listen?": A Quantitative Analysis of Fraudsters' Decision-Making Processes on Active Cybercrime Marketplaces

4.1. Introduction

Online fraudsters have exploited the capabilities of the internet to defraud targets of $18.7 billion in the last five years (Internet Crime Complaint Center, 2022). Identity theft is one of the various cybercrime attacks offenders have used to generate monetary gains from unsuspecting targets online. Identity theft fraud losses have increased by 316.47% (from $66,815,298 to $278,267,918) from 2017 to 2021 (Internet Crime Complaint Center, 2018; 2022). The increased losses to identity theft demonstrate the monetary successes fraudsters have experienced operating online.

Offenders play a fundamental role in the development and completion of an online fraud event. Still, there is limited research exploring offenders [fraudsters'] individual-level decision-making processes (i.e., modus operandi) against other offenders (a.k.a. offender-victims) (Franklin et al., 2007; Hutching and Holt, 2015; Kigerl, 2018 & Kigerl, 2020; Maimon et al., 2019; Yip et al., 2013). Critical to fraudsters' individual-level decision-making processes are their communication with targets (e.g., victims and victim-offenders). For instance, research indicates that online fraudsters intentionally interact (via written communications) with targets using socially engineered (SE) characteristics and tactics to obtain sensitive and financial information for monetary gain (Rege, 2009; Hadnagy, 2010, 2018, 2019).

In addition to the vital role fraudsters' SE characteristics and tactics play in an online fraud event, empirical evidence indicates that the direct situational context influences offenders' individual-level decision-making processes through their interactions (in the physical environment) with other offenders (see Jacobs & Wright, 2006, p. 7; Topalli et al., 2002). For

example, Topalli et al. (2002) observed interactions between offenders, specifically drug dealers, and found drug dealers would retaliate against those who ripped them off.

However, there is limited research exploring the influence of the situational context on offenders' decision-making processes. What is known about the situational context as it relates to digital interactions among actors primarily focuses on deceptive users, not criminal users. For instance, Zhou and Zhang's research indicates deceptive users communicate with words that are, on average, shorter in character count compared to honest users who communicate on average with words longer in character count (2004; 2007). Research also suggests that deceivers communicated with fewer words than truth-tellers who used more words to communicate (Toma & Handcock, 2010; 2012; Ho et al., 2016). Specifically, Toma and Handcock's (2010; 2012) research indicates that deceptive user profiles on dating websites featured fewer words than those associated with honest users whose profiles featured more words.

Furthermore, researchers have used "crime scripts"[44] to explore offenders' macro-social interactions (Lavorgna, 2014; Gilmour, 2014). For instance, Gilmour (2014) research outlines five stages of actions offenders use to money launder (e.g., business set up, purchase commodity, allocation of funds from purchased illicit products, sell commodity and transactional processes to elicit funds). Yet, these five stages do not account for offenders' micro-level social interactions with targets, including both victims and victim offenders. Examining offenders' micro-level social interactions is important because it captures human interactions that the macro-level does not and allows for the detection of victimization more effectively by accounting for offender victims.

[44] "Crime scripts" are step-by-step processes detailing an individual's criminal engagement (Lavorgna, 2014).

Specific to offenders' victimization of offenders, offenders' decision-making processes among offender victims are important to examine. This is important because the situational context of the online environment with emergent technological advances, such as anonymity, helps facilitate offenders' monetary gains, and mitigates risks among offenders (e.g., preserving anonymity lessens risks of detection). Considering the impact and influence digital communications have on all users with offenders who use digital communication to pursue a wide selection of targets, the findings from this study go beyond helping victimized offenders (e.g., both offender victims and non-offender victims) (Kigeral, 2018; 2020; Maimon & Louderback, 2019).

It is still not well known how and if fraudsters' decision-making processes differ when interacting with other offenders online during the development of an online fraud event. This ambiguity raises the question, "How does the situational environment influence offenders during the development of an online fraud event against offending victims?" The current study investigates offenders' decision-making processes through their SE characteristics and tactics during the development of an online fraud event with specific attention to the influence of the situational context on offenders. To achieve this and build upon prior research, I will provide a conceptual definition of fraudsters. Then, online offenders' characteristics and tactics will be explored and theoretically explained with the criminal event perspective (CEP) postulated by Short (1998) as a framework. Supportively, interpersonal deception theory (IDT) with Proposition 18 of IDT, that presumes the success of a sender's (e.g., deceiver's) deception depends on the sender's cognition and behavior throughout communications with the target (Buller and Burgoon, 1996), will be used to examine online offenders' decision-making processes. These theoretical perspectives in tandem build upon prior research (e.g., Ho et al.,

2016; Toma & Handcock, 2010; 2012; Zhou et al., 2002). I hypothesize the total number of messages sent by offender victims is negatively correlated with the total number of messages sent by the offender after a fraud event. Specific to the development of a fraud event, I hypothesize the number of messages sent by offender victims is negatively correlated with the number of messages sent by the offender before a fraud event. While after a fraud event, I hypothesize the total number of messages sent by offender victims is negatively correlated with the total number of messages sent by the offender.

Additionally, I hypothesize even when accounting for other independent and control variables, that message frequency by the offender victim will be related to increase in the total number of messages before the fraud event, a decrease in the message frequency of offenders after the fraud event, and a decrease in the overall total number of messages of offenders.

4.2 Literature Review

4.2.a Online Fraud

Fraud is the intentional act of deception for personal and sensitive information and/or monetary gains ("Fraud," 2019). Online fraud is the use of internet services or access to defraud others (FBI, n.d.). An offender who engages in fraud online is commonly referred to as a fraudster, so an online fraudster is an offender who defrauds others using internet access or services. A ripper is a fraudster who defrauds another offender (Kigerl, 2018).

The existing body of research examining online fraud indicates these crimes are extremely profitable but offenders cannot easily cash out their monetary gains (Kigerl, 2018). For example, Kigerl's (2018) research indicates that offenders created cybercrime marketplaces to remedy this issue and communicate to trade and purchase illicit information (via online

messaging). Identity theft and credit card fraud facilitate cybercrime markets because it provides offenders anonymity in their illegal transactions (Kigerl, 2018; Maimon & Louderback, 2019; Yip et al., 2013). Identify theft is the use of another person's sensitive information without the owner's permission, like social security number or credit card, for monetary gains (Internet Crime Complaint Center, 2022; "Identify theft," 2022). The unauthorized use of credit cards is credit card fraud. The slang word for credit card fraud is carding and often involves concealing illegal credit card fraud transactions (Kigerl, 2018).

Fraudsters use socially engineered (SE) tactics to influence targets into disclosing personal, sensitive, and financial information, like bank accounts and social security numbers (Hadnagy, 2010; 2018; 2019; Rege, 2009). Fraudsters often pre-text to establish legitimacy with their targets. Pre-texting involves the creation of a fake scenario to build rapport with a target for the purpose of more thoroughly comprehending the target's social and situational environment (Carnegie Mellon University, 2020; Hadnagy, 2010; 2018; 2019). For instance, a fraudster may present an employment opportunity that is too good to be true, like a remote employment opportunity with a salary of $100,000 where the employee only has to work three days a week. The offender establishes their creditability and gains trust with targets by incorporating stolen credentials[45] within their email correspondence. Fraudsters often create these elaborate scams to steal the target's sensitive and financial information and/or money launder through the target (Cole, forthcoming).

Overall, research indicates offenders successfully SE online fraud attacks with linguistic cues of urgency (e.g., "ASAP), authority (e.g., "trust me"), and delay (e.g., "wait") approach (Akins and Huang, 2013; Rouce, 2013; Alkhalil et al., 2021). Specific to offenders' attacks on

[45] Government letterhead or icons.

non-offending victims, Akins and Huang's (2013) research suggests that 71% of fraudsters used urgency cues to defraud their targets, while 100% of them used authority cues to convince the target of their legitimacy. 41% of fraudsters messages to targets (e.g., offender victims) contained delay cues after the completion of a fraud event (Cole, forthcoming). Likewise, Cross and Kelly's (2016) research indicates fraudsters modify schemes "to entice the victim to continue sending money" (p. 815).

Research examining fraudsters' communication, such as linguistics cues, is not limited in scope to non-offending victims (Halder, 2014; Kigeral, 2018). An example of this is Kigeral's (2018) research demonstrating how offenders communicate with each other to defraud or warn other offenders of a fraudster (i.e., ripper). Specifically, fraudsters who defraud other offenders will be labeled as a “ripper” and/or given negative reviews on online cybercrime marketplaces. Similarly, empirical evidence from Yip et al.'s (2013) research suggests offenders on cybercrime marketplaces communicate at a higher frequency than those who have not been verified as actual offenders; this highlights the importance of importance of micro-level interactions (i.e., situational context) observed through offenders interactions with other offenders).

A considerable amount of literature has been published exploring the situational context surrounding criminality within the physical environment (Anderson & Meier, 2004, p. 420; Benson et al., 2009, p. 183; Jacobs & Wright, 2006, p. 7, Konkel et al., 2021; Topalli et al., 2002). These studies indicate offenders are influenced by the “microgeographic” (i.e., situational) environment (Jacobs & Wright, 2006, p. 7, Konkel et al., 2021). Additionally, the availability of monetary gains or a specific illicit product or service may influence an offenders’ decision to engage in crime (Benson et al., 2009, p. 183; Cornish & Clarke, 2003). For example, Cornish and Clarke’s (2003) research suggests an association between an offender’s operations

and the contextual environment. Specifically, Cornish and Clarke (2003) assert the opportunity for crime, along with the offenders' ability to control the situation, or in this case, communication (i.e., dialogue), is key to the completion of a criminal event. An example of this in the physical environment is illustrated by who and how offenders sell drugs (Dickinson & Wright, 2015; Topalli et al., 2002). Dickinson and Wright's (2015) research highlights this point by showing with how drug dealers will continue social relationships (via communication) but stop selling drugs to specific clientele to evade law enforcement detection. Similarly, Topalli et al.'s (2002) research suggests offenders "code switch" depending on with whom they interact.

So far, however, there has been limited research into the influence of the situational context on offenders' decision-making processes, specifically with whom they interact (i.e., non-offending victims and offending victims) in the cybercrime ecosystem (Kigerl, 2018; Maimon et al. 2019, Maimon et al. 2020). The limited research suggest fraudsters communicate on average with 378.8 words per email to defraud targets on the clear web (via classified advertisements) but failed to account for the average number of words per email from non-deceptive targets to fraudsters (Maimon et al., 2019). Specific to offender and offender victim interactions, Kigerl's (2018) research indicates offender victims will communicate at a high frequency about offenders who have defrauded them through illicit online marketplaces. These findings demonstrate offenders will modify their behaviors, specifically their communications, with whom they target online.

No previous study has addressed the question, "How does the situational environment influence offenders during the development of an online fraud event against offending victims?" The current study fulfills this empirical gap by exploring offenders' decision-making processes in cybercrime marketplaces using the criminal event perspective (CEP) to frame communications

between offenders (i.e., fraudsters) and offender victims (Short, 1998). Specifically, interpersonal deception theory (IDT) and CEP are used together to analyze fraudsters' characteristics and tactics through the frequency of messages offenders use to understand the contextual environment of their targets (Buller & Burgoon, 1996; Maimon et al., 2019; Short, 1998). Taken together, these theoretical perspectives build on previous research that indicates the situational context (e.g., frequency of deceptive users' words and messages (i.e., communications, see Toma & Handcock, 2010; 2012; Zhou et al., 2002) influences offenders' decision-making processes.

IDT helps examine the influence of offenders' communications that develop during criminal interactions depicted in CEP, which allows for the exploration, identification, and explanation of criminality (Short, 1998). IDT benefits CEP because it provides further insight into the verbal and non-verbal actions involved in communications and this is beneficial for the observation of online fraud events specifically.

4.3 Theoretical Framework

4.3.a The Criminal Event Perspective (CEP)

Existing research recognizes the critical role social interactions have on all actors (Goffman, 1955). Specifically, Goffman's (1955) social interaction perspective proposes all actors manage their reputations by presenting themselves as how they want others to perceive them. The CEP, proposed by Short (1998), expands upon Goffman's (1955) social interaction perspective by asserting offenders will adapt their behaviors depending on their environment. CEP explores the microsocial environment of offenders through the identification, exploration,

and explanation of criminality. In other words, CEP focuses on the microsocial interactions between offenders and victims during the development of a crime.

The concepts proposed in CEP have been explored within criminology to illustrate the influence of the situational context on offenders' engagement (Dickinson and Wright, 2015; Horney, Osgood, & Marshall, 1995; Shaw & McKay, 1942). Specifically, some concepts of the CEP have been used to explore the age, demographics, locations, and interactions of individuals engaged in criminality (Dickinson & Wright, 2015; Horny et al., 1995; Shaw & McKay, 1942). For example, Horney, Osgood, and Marshall's (1995) research suggests offenders' life changes, such as marriage and employment, disrupt an individual's engagement in criminality. In this instance, offenders' micro-level interactions with a partner that leads to marriage with another person may affect their ability to conduct crime.[46] Dickinson and Wright's (2015) research suggests that some offenders would completely quit selling drugs if they heard gossip from other offenders about law enforcement potentially detecting crimes associated with their criminality. Together, these examples from the research provide important insights into the situational context that influence an offender's decision to disengage from criminality.

The criminological literature thoroughly describes a link between offenders' interactions and the "microgeographic" or direct contextual and situational environment surrounding the crime, including who offenders target within the physical environment (Konkel et al., 2021). For example, offenders' location (i.e., contextual environment) can influence criminality engagement (Anderson & Meier, 2004; Benson et al., 2009). Benson et al. (2009) research suggests white-collar criminals use their place of employment to select targets to defraud. Specifically, white-

[46]A married individual may not be able to conduct crime because their partner influences (or controls) with whom they interact. Therefore, they could limit their interactions with devious or criminal people they previously had contact.

collar criminals target customers to defraud based on the sensitive and financial information accessible to them (Benson et al., 2009). Similarly, Anderson and Meier's (2004) research indicates that the location (i.e., educational institutions) influences delinquency, including the situational context associated with the location. Specifically, there is a positive association between students in urban areas and delinquency, with researchers attributing students' delinquency to lack of supervision (Anderson & Meier, 2004).

Several studies suggest an association between the situational context and criminality (Anderson & Meier, 2004; Cornish & Clarke, 2003; Madarie et al., 2019). By way of illustration, Cornish and Clarke (2003) note how "the existence of opportunities to carry out the offense" must be present (p. 59). The offender, for example, must have the time to commit the crime(s). Another observation within offenders' situational environment is their motivational cues. Cornish and Clarke (2003) illustrated how offenders employment positions could motivate them into criminal engagement. For example, white-collar criminals deploy motivational cues for financial gain to exploit their targets Benson et al., 2009) (p. 52). Still, in order to assess offenders' motivational cues, scholars must be able to assess for offenders' technique to conduct crime a criminal event (Cornish & Clarke 2003, p. 52). Specific to the contextual and situational environment associated with cybercrimes, CEP has helped explain criminality on dark web forums (Madarie et al., 2019). Madarie et al. (2019) research indicates offenders learn how to maintain anonymity through encryption and garner support from other offenders through the frequency of written positive website ratings and negative website ratings, as previously highlighted in Kigeral's (2018) research.

Research exploring offenders' interactions with CEP mainly focuses on samples within the physical environment or is limited within the cybercrime ecosystem to certain websites, like

classified advertisements and darkweb forums (Madarie et al., 2019; Maimon, Santos, & Park, 2019). Therefore, much less research explains the influence of offenders' decision-making processes among offending victims outside of the physical environment. The inclusion of Buller and Burgoon's (1996) IDT helps fulfill this void, specifically with the examination of offenders and offender victims' written text frequency.

4.3.b Interpersonal Deception Theory (IDT)

Buller and Burgoon's (1996) IDT is a communication theory researchers use to explain the microsocial communications between deceivers and truth-tellers. According to Buller and Burgoon (1996), all communication involves non-strategic and strategic behaviors, especially deceptive communication. Non-strategic behaviors include individuals' unconscious and unintentional actions. Alternatively, strategic behaviors include individuals' conscious and intentional actions. IDT is a detailed explanation with 18 Propositions that thoroughly depict deceivers' deceptive processes in communication with truth-tellers. One process is crime scripts, which guides the deceivers' behaviors in instances of criminal engagement; however, this process in particular does not account for decision-making.

A fundamental proposition is Proposition 18, which presumes the success of a sender's (e.g., deceiver's) deception depends on the sender's cognition and behavior throughout communications with the target. Zhou et al.'s (2002) research support this contention among those who deceive truth-tellers with computer-mediated communication. Specifically, Zhou et al. (2002) suggest individuals who are deceitful in online communications use a higher frequency of words to persuade the receiver of their legitimacy and are more emotionally charged within their communications than truth-tellers. In other words, Zhou, and colleagues (2002) are implying that

word frequency and the use of emotionally-charged words are reflections of cognition and behavior. An example of what is meant by emotionally-charged communications is words that provoke action, like the word anticipate or secret (Carlson and Zmud, 1999).

Offenders are frequently deceptive when engaging in criminality and although deceit is not illegal, it is often used by fraudsters to successfully commit a crime. A well-known example of criminal deceit from the communication field is illustrated by individuals who lied to 911 callers (Burns & Moffitt, 2014; O.C.G.A. § 16-10-20 (2010)). Burns and Moffitt's (2014) research demonstrates how criminals adapt their behaviors through communications. Specifically, deceptive callers, compared to callers who told the truth, used a higher frequency of positive affirming words (i.e., “vow” and “promise”) in communication with 911 operators (Burns & Moffitt, 2014).

As previously stated, offenders’ decision-making processes during the development of an online fraud event are critical to explore, considering the increased monetary losses in the United States and worldwide to online fraud along with technological advances affording fraudsters’ risk mitigation (Maimon & Louderback, 2019). Nevertheless, there is limited research exploring online fraudsters' decision-making processes (i.e., modus operandi) (Maimon et al., 2020). To fulfill this void, IDT in tandem with CEP will be used to extend the research exploring offenders’ decision-making processes during the development of an online fraud incident.

4.4 The Current Study

Based on a review of the literature along with considering the IDT and CEP, the following hypothesis was developed. Specifically, the framework detailed above was used to account and examine offenders’ interactive decision-making processes among both offender

victims that researchers frequently attributed to “crime scripts” (Lavorgna, 2014). Although “crime scripts” have helped researchers explore offenders’ criminal engagement, it is not sufficient for researchers to merely rely on “crime scripts” because they do not account for offenders’ decision-making processes (Lavorgna, 2014; Leclerc, 2013; Gilmore, 2014). Consequently, I inform “crime scripts” with additional research by accounting for and reporting offenders’ decision-making processes among offender victims with IDT and the CEP.

The following study accounts for offenders’ decision-making processes among offenders and offender victims during the development of an online fraud event. Specifically, I observe offenders involved in online fraud without fragmentation through the frequency of their communications (i.e., contextual environment). In doing so, I accounted for the influence of the situational environment, such as offender motivations (i.e., money and produced stolen) and the average number of Telegram users (i.e., subscribers) on the channel the fraud conversation was reported (Anderson & Meier, 2004; Cornish & Clarke, 2003; Madarie et al., 2019; Kigeral, 2018; 2020; Zhou et al., 2002; 2004; 2008). I hypothesize, by observing Proposition 18 of IDT in tandem with the CEP, fraudsters intentionally act and interact with targets depending on their targets’ contextual and situational environment, such as the frequency of a target’s communications to the offender. Additionally, the situational context associated with the duration of time the channel has been active and/or the average number of subscribers on the channel may influence the offenders’ interactions with targets (Maimon et al., 2019; Maimon et al., 2020; Topalli et al., 2002; Zhou et al., 2002). Specifically, offenders will strategically interact in written communications observable via the frequency of messages to offender victims to elicit information related to finances or products (i.e., services) from targets while avoiding detection (Anderson & Meier, 2004, p. 420; Benson et al., 2009, p. 183; Zhou et al., 2002; 2004; 2008).

Thus, using Proposition 18 encompassed by CEP and building upon research (i.e., Zhou et al., 2002), I hypothesize the total count of messages sent by offender victims is negatively correlated with the total number of messages sent by the offender event after a fraud event. Specifically, I hypothesize the total number of messages sent by offender victims is negatively correlated with the total number of messages sent by the offender after a fraud event. Specific to the development of a fraud event, I hypothesize the number of messages sent by offender victims is negatively correlated with the number of messages sent by the offender before a fraud event. While after a fraud event, I hypothesize the total number of messages sent by offender victims is negatively correlated with the total number of messages sent by the offender.

Additionally, I hypothesize even when accounting for other independent and control variables, that message frequency by the offender victim will be related to increase in the total number of messages before the fraud event, a decrease in the message frequency of offenders after the fraud event, and a decrease in the overall total number of messages of offenders.

4.4.a Methodology

A manifest content analysis approach was used to examine the development of an online fraud event (Leech & Onwuegbuzie, 2008; Maruna; 2010; Zhu et al., 2013). A manifest content analysis is one of the most widely used tools for analyzing a specific data point, such as the frequency of words and messages (i.e., conversations) and linguistic cues deployed by actors (Leech & Onwuegbuzie, 2008; Maruna, 2010). Maruna's (2010) manifest content analysis is a research tool helping researchers code content observed in qualitative data (e.g., crime scripts). This methodology helped me identify a theme of frequency of messages sent by offenders to offender victims and vice versa as I observed the collected data. Therefore, I used a manifest

content analysis to explore the qualitative and quantitative data presented in this study. I received approval from the Georgia State University's Internal Review Board (IRB) to use the following two datasets used in this study.

4.4.b Procedure

Research indicates that targets' attractiveness influences offenders' behaviors (Kshetri, 2010). Specifically, Kshetri's (2010) research suggests internet users displaying lower SES online are less appealing to offenders to target. I am investigating offenders' decision-making processes within cybercrime ecosystems (i.e., across marketplaces) within this study and, therefore, needed the comparison of the cybercrime ecosystems for analysis. Accordingly, I systematically selected 55 Telegram channels where reported online fraud information and materials are distributed to collect data on online offenders' decision-making processes. I used search terms associated with online fraud to identify these channels (Kigeral, 2018; Kigeral, 2020). Specifically, I listed the following search terms in alphabetical order: 1) Carding, 2) Fraud, 3) Rip, and 4) Scam. Then, I searched each term once, explored the results, and joined the top yielded, relevant channel. If the channel I joined advertised (i.e., promoted) other channels within the last 24 hours, I joined the most recently promoted channel. When I reached the end of the alphabetized list, I repeated this pattern starting again at the beginning of the alphabetized list

until I had a list of 55 channels.[47] Language barriers and technical issues prevented me from examining all 55 channels, and therefore, only 52 channels could be analyzed.[48]

The purpose of the current study is to examine the situational context influence of online fraudsters' decision-making processes during the development of a fraud incident associated with active illicit fraud forums online. Therefore, I selected 39 of the 52 channels to examine because those channels were where offenders were actively promoting and selling financial fraud information stolen from non-offending victims (i.e., individuals, companies, and organizations) (Cole, Forthcoming; Internet Crime Complaint Center, 2022). Reported fraud instances and conversations within these channels were identified with the search terms: (1) Fraud, (2) Rip, and (3) Scam. The selected search terms allowed me to identify iterations of reported instances of fraud, such as when an offender called out another offender for defrauding them or an acquaintance with words including but not limited to “fraud” alert, “fraudster,” “ripper,” “rip” alert, “scam” alert, or “scammer.” Frequently, the reported fraud instances included “proof” (i.e., an image of the conversation between the defrauded offender victim and the offender). Consequently, my data collection within this sample includes photographs and written texts uploaded by active users on these 39 channels that I manually downloaded every Friday for twelve weeks.

[47] Offenders upload a massive amount of data (i.e., images including both pictures and videos and text) to Telegram channels. I was the only person to consistently monitor the selected Telegram channels; thus, because of the amount of information uploaded by offenders to each channel, I could only monitor 55 channels. These observed channels were some of the busiest channels identified and, therefore, I suspect are likely to represent offenders involved in illicit online fraud transactions.

[48] One of these channels was in a foreign language (i.e., Chinese) and a number of channels would not completely download each week.

4.4.c Sample

The unit of analysis is *fraud conversations* (N=93) because I am investigating the contextual and situational environment of offenders' decision-making processes during the development of an online fraud event where personal, sensitive, and financial information is actively distributed. The variable *user* was constructed to account for the dependence of Telegram users who may offend but also become victimized and vice versa. Each distinct, *user,* was assigned a unique identifier. There were 84 unique victims and 81 unique offenders.

As previously stated, research suggests offenders are influenced by their contextual and situational environment (Anderson & Meier, 2004; Benson et al., 2009; Cornish & Clarke, 2003, p. 52). To account for the influence of offenders' contextual and situational environment, Maruna's (2010) "manifest content analysis" approach was used to document and analyze each conversation by (1) unique offender, (2) unique offender victims (including offender victims' advocates),[49] (3) offenders' frequency of messages, specifically the count of offenders' messages before, after and total during the development of an online fraud event, (4) offender victims' frequency of messages, specifically the total count of messages before, after and combined during the development of an online fraud event, (5) average number of subscribers (i.e., users) present on a channel, (6) reported financial amount lost (in USD), (7) stolen product and/or service and (8) week fraud reported on channel.

4.4.c.a Dependent Independent Measures. Research indicates offenders intentionally act with and interact with targets (Maimon et al., 2019; Maimon et al., 2020; Topalli et al., 2002;

[49] A victim advocate is another user who reports the fraud victimization on behalf of the victim, which would occur in circumstances where the victim had their account taken over or could no longer access that specific Telegram board.

Zhou et al., 2002). To examine this theoretical assumption within the cybercrime ecosystem, fraud conversations communications, including the picture threads (i.e., pictures of the message communication between the offenders and offender victims), are the unit of analysis in this study. The variables, *offenders' frequency of total messages*, *offenders' frequency of messages before fraud event,* and *offenders' frequency of messages after fraud event*, were constructed and measured on a continuous scale (ranging from 0 to 70).

4.4.c.b Key Independent Measures. Research indicates that the situational context influences offenders' decision-making processes (Dickinson and Wright, 2015; Maimon et al., 2019; Maimon et al., 2020; Topalli et al., 2002;). Additionally, prior research suggests deceivers will communicate less frequently than truth-tellers (Ho et al., 2016; Toma & Handcock, 2010; 2012; Zhou et al., 2002). It is challenging to differentiate between the contextual and situational environments surrounding offenders' criminality (Cornish and Clark, 2003, p. 45; Wortley, 1997). Therefore, I assessed several aspects within the contextual and situational environments of offenders' during the development of an online fraud event, including with whom they interact with (Cornish & Clark, 2003; Wortley, 1997). To achieve this, I created the following variables, *offender victims' frequency of total messages*, *offender victims' frequency of messages before fraud event*, *offender victims' frequency of messages after fraud event,* and *stolen product and/or service.* The variables, *offender victims' frequency of total messages*, *offender victims' frequency of messages before fraud event* and *offender victims' frequency of messages after fraud event*, were measured on a continuous scale (ranging from 0 to 62). Additionally, the variables, *average number of subscribers, duration of time channel has been in operation,* and *financial amount lost (in USD)* are included. The number of subscribers on each channel were

documented every Friday of the study. I constructed, *average number of subscribers,* by averaging the documented number of subscribers respective to each channel and measured it on a continuous scale. I constructed the variable, *financial amount lost (in USD),* by converting all the reported losses into United States Dollars (USD) and measuring the losses on a continuous scale. The variable, *stolen product and/or service*, was measured on a categorical scale (not stated= 0; non-offending victims' stolen personal, sensitive and financial information = 1; documents ((i.e., online theft methods, PPP forms[50]) = 2).

4.4.c.c Control Variables. The variable, *week*, was constructed to control for the contextual and situational influence of time. *Week* was measured on a seven-day increment from Friday to Friday for 12 weeks on a continuous scale and helped account for when an offender victim (or a victim advocate) reported a ripper (i.e., fraudster) while I was monitoring the channels (coded 1 to 12 for each week).

4.5 Analytic Strategy

In the first step of the analysis, a series of bivariate correlations were run to examine the relationship between the independent variables and the three dependent variables (i.e., *Offenders' Frequency of Total Messages*, *Offenders' Frequency of Messages Before Fraud Event,* and *Offenders' Frequency of Messages After Fraud Event*). Then, a series of negative binomial regression models were used to estimate the relationship between the dependent and independent variables. Negative binomial regressions are a form of a Poisson regression used to estimate the relationship between dependent and independent variables when the outcomes are counts (e.g.,

[50] PPP is an abbreviation for the "Payback Protection Program" enacted under the Small Business Administration (SBA) during the height of COVID-19 to assist employers and employees who were financially struggling.

frequencies) and the dependent variable is not normally distributed (Hilbe, 2011). A series of negative binomial regressions with the estimated rate ratio (IRR)[51] were selected because the data under examination was over-dispersed.

4.6 Results

Table 8 presents the descriptive analysis of this study. Specifically, the mean number of messages sent by offenders to offender victims total, before, and after the development of an online fraud event was 7.18 (SD =9.79), 4.80 (SD=4.94), and 3.59 (SD=8.32), respectively. The mean number of messages sent by offender victims to offenders before, after, and in total during the development of an online fraud event was 8.36, 4.38, and 5.10, respectively. Stolen product and/or service is a categorical variable (i.e., not stated= 0; non-offending victims' stolen personal, sensitive and financial information = 1; documents (i.e., online theft methods, PPP forms) = 2). It was unknown in 46.25% of the conversations what the offender victim was defrauded of. Thirty percent of offender victims were defrauded of their personal, sensitive and financial information while attempting to purchase from offenders (i.e., fraudsters), while 23.75% offenders victims reported being defrauded with documents (i.e., online theft methods; PPP). The average number of subscribers on Telegram boards where offender victims reported being ripped off was 15,340.05 (SD= 11,000.63). Victims reported an average amount of losses of $92,268.86. The variable, week, was measured on a continuous scale for a total of twelve weeks (M= 6.23; SD= 3.27).

[51] IRR is the estimated rate ratio holding all the other variables constant (Hilbe, 2011).

Table 8. Descriptive Statistics (N= 80 Fraudulent Conversations)

Variables			**Minimum-Maximum**
Dependent Variables	**M**	**SD**	
Message Frequency			
Offenders' Frequency of Total Messages	7.18	9.79	1-70
Offenders' Frequency of Messages Before Fraud Event	4.80	4.94	1-31
Offenders' Frequency of Messages After Fraud Event	3.59	8.32	0-59
Independent Variables			
Message Frequency			
Offender victims' Frequency of Total Messages	8.36	8.47	1-62
Offender victims' Frequency of Messages Before Fraud Event	4.38	4.56	1-27
Offender victims' Frequency of Messages After Fraud Event	5.10	6.97	0-52
Stolen Product and/or Service	**%**	**N**	0-2
Not Stated	46.25	37	
Non-offending victims' personal, sensitive and financial information	30.00	24	
Documents (i.e., online theft methods; PPP[52])	23.75	19	
	M	**SD**	
Average # of Subscribers	15,982.63	11,330.37	1,132.85 to 33,175.50
Financial Amount Lost (in USD) (N=33)	$ 97,852.58	$ 420,333.70	$4.23-$ 2,294,719.00
Control			
Week	6.19	3.31	1-12

[52] PPP is an abbreviation for the "Payback Protection Program" enacted under the Small Business Administration (SBA) during the height of COVID-19 to assist employers and employees who were financially struggling.

The results of the correlational analysis are presented in Tables 2, 3 and 4. As shown in Table 9, the total overall (i.e., before and after the fraud event) count of messages sent by offender victims is positively correlated with the total number of messages sent by the offender ($p<0.05$). Additionally, offender total frequency of messages and week are positively correlated ($p<0.10$). The offender victims' total frequency of messages and week are positively correlated ($p<0.01$). Lastly, stolen product and/or service and week are positively correlated ($p<0.10$).

Table 9. Correlation of Offenders' Total Frequency of Messages with Situational Contextual Variables of Interests.

Variables	Offenders' Frequency of Total Messages	Offender Victims' Frequency of Total Messages	Stolen Product and/or Service	Average # of Subscribers	Financial Amount Lost (in USD)	Week
Offenders' Frequency of Total Messages	1					
Offender Victims' Frequency of Total Messages	.4144*	1				
Stolen Product and/or Service	.1532	.0937	1			
Average # of Subscribers[a]	.0236	.0628	.0320	1		
Financial Amount Lost (in USD)	-.0284	.2244	.0426	.1679	1	
Week[a]	.2086+	.2743**	.1944+	.0710	-.0170	1

+p < 0.10; *p < 0.05; ** p < 0.01; *** p < 0.001; [a] Pearson's correlations for normally distributed variables: Average # of Subscribers and Week. Spearman's Correlation used for all other variables because those variables were not normally distributed.

As observed in Table 10, the count of messages sent by the offender before a fraud event is positively correlated with the count of messages sent by the offender victim before the fraud event ($p<0.001$). The frequency of messages sent by the offender before a fraud event and the average number of subscribers are positively correlated ($p<0.10$). The frequency of messages sent by the offender before a fraud event and week are positively correlated ($p<0.05$). Lastly, stolen product and/or service and week are positively correlated ($p<0.10$).

Table 10. Correlation of Offenders' Frequency of Messages Before Fraud Event with Situational Contextual Variables of Interests.

Variables	Offenders' Frequency of Messages Before a Fraud Even	Offender Victims' Frequency of Messages Before a Fraud Even	Stolen Product and/or Service	Average # of Subscribers[a]	Financial Amount Lost (in USD)	Week[a]
Offenders' Frequency of Messages Before a Fraud Event	1					
Offender Victims' Frequency of Messages Before a Fraud Event	.6664***	1				
Stolen Product and/or Service	.2485	0.2775	1			
Average # of Subscribers[a]	-.0745+	-.0519	.0320	1		
Financial Amount Lost (in USD)	-.1712	.0804	.1283	.0684	1	
Week[a]	.0585	.2581*	.1944+	.0710	-.0170	1

+p < 0.10; *p < 0.05; ** p < 0.01; *** p < 0.001; [a] Pearson's correlations for normally distributed variables: Average # of Subscribers and Week. Spearman's Correlation used for all other variables because those variables were not normally distributed.

As observed in Table 11, the count of messages sent by offender victims is positively correlated with the total number of messages sent by the offender after a fraud event. Lastly, stolen product and/or service and week are positively correlated (p<0.10).

The relationship between offender victims' total frequency of messaging and offender total frequency of messaging is examined. In model 1, multivariate negative binominal regression analysis with only the frequency of messages along with the control variable is presented. As shown, for every additional message from the offender victim, the offender's messaging rate is expected to increase by a factor of 1.06 (CI= 1.08-1.17, p < .001) when holding week constant. Model 2 is the same analysis but includes the other independent variables. As can be seen, for every additional message from the offender victim, the rate of messaging by the

offender is expected to increase by a factor of 1.04 (CI= 1.08-1.19, p < .001) when accounting for the independent variables and holding week constant.

Table 11. Correlation of Offenders' Frequency of Messages After Fraud Event with Situational Contextual Variables of Interests.

Variables	Offenders' Frequency of Messages After the Fraud Event	Offender Victims' Frequency of Messages After the Fraud Event	Stolen Product and/or Service	Average # of Subscribers[a]	Financial Amount Lost (in USD)	Week[a]
Offenders' Frequency of Messages After the Fraud Event	1					
Offender Victims' Frequency of messages After the Fraud Event	.4497**	1				
Stolen Product and/or Service	-.1230	-.3617	1			
Average # of Subscribers[a]	.0416	.0868	.0320	1		
Financial Amount Lost (in USD)	-.0991	-.0185	.0426	.1679	1	
Week[a]	.1378	.1336	.1944+	.0170	.0170	1

+p < .10; *p < .05; ** p < .01; *** p < .001; [a] Pearson's correlations for normally distributed variables: Average # of Subscribers and Week. Spearman's Correlation used for all other variables because those variables were not normally distributed.

Model 3 presents analyses of a multivariate negative binomial regression analyses examining the relationship between offender victim messages before a fraud event and offender messages before a fraud event, accounting for the control variable. As presented, for every additional message from the offender victim, the rate of messaging by the offender is expected to increase by a factor of 1.12 (CI= 1.08-1.16, p < .001) when holding week constant. The same analysis is included in Model 4 but includes the other independent variables. As shown, for every additional message from the offender victim, the offender's messaging rate is expected to

increase by a factor of 1.14 (CI= 1.08-1.19, p < .001) when accounting for the other independent variables and holding week constant.

Model 5 shows the results from multivariate negative binomial regression analysis with only frequency of messages after a fraud event, along with the control variable. As presented, for every additional message from the offender victim, the rate of messaging by the offender is expected to increase by a factor of 1.11 (CI= 1.07-1.16, p < .001), when holding week constant. Model 6 presents the same analysis but includes the other independent variables. For every additional message from the offender victim, the offender's messaging rate is expected to increase by a factor of 1.09 (CI= 1.06-1.12, p < .001) when accounting for the other independent variables and week.

Table 12. Negative Binomial Regressions (IRR) of Offenders' Frequency of Messages and the Situational Contextual Variables of Interests.

	Offenders' Total Messages		**Offenders' Messages Before Fraud**		**Offenders' Messages After Fraud**	
	Model 1 (N=80)	**Model 2 (N=33)**	**Model 3 (N= 60)**	**Model 4 (N=27)**	**Model 5 (N=78)**	**Model 6 (N= 33)**
	IRR (CI)	**IRR (CI)**	**IRR (CI)**	**IRR (CI)**	**IRR (CI)**	**IRR (CI)**
Frequency of Messages						
Offender victims' Frequency of Total Messages	1.06*** (1.08-1.17)	1.04*** (1.08-1.19)	--	--	--	--
Offender victims' Frequency of Messages Before Fraud Event	--	--	1.12*** (1.08-1.16)	1.14*** (1.08-1.19)	--	--
Offender victims' Frequency of Messages After Fraud Event	--	--	--	--	1.11*** (1.07-1.16)	1.09*** (1.06-1.12)
Telegram Channel	--					
Average # of Subscribers	--	1.00 (.99-1.00)	--	1.00 (.99-1.00)		1.00 (.99-1.00)
Motivations						
Reported Losses (in USD)	--	1.00 (.99-1)	--	1.00 (.99-1.00)	--	1.00 (.99-1.00)
Stolen Product and/or Service	--	0.97 (.72-1.09)	--	0.89 (.73-1.10)	--	0.96 (.68-1.35)
Control(s)						
Week	1.01 (.92-1.02)	1.05 (.97-1.13)	.97 (.92-1.02)	1.04 (.97-1.13)	.95 (.88-1.03)	.89* (.80-.99)
Constant	3.35*** (2.04-4.68)	3.178*** (1.13-3.63)	3.09*** (2.05-4.68)	2.023* (1.13-3.63)	1.745* (1.04-2.90)	2.10* (.1.10-4.02)
Ln Alpha	-1.11	-1.64	-1.55	-2.57	-0.155	-1.18
Pseudo-R^2	.10	.1658	.1070	.1703	.1164	.2375
Log likelihood	-216.54	-85.6999	-138.089	-60.01	-160.36	-56.23

+p ≤ .10; *p ≤ .05; ** p < .01; *** p < .001

4.7 Discussion and Conclusion

To date, little research has explored offenders' decision-making processes for the development of an online fraud event (Maimon et al., 2019). The current study fills this void by examining offenders' decision-making processes when targeting offender victims because these actors comprise and facilitate a significant portion of the cybercrime ecosystem (Maimon et al., 2019). Specifically, the current study bridges an empirical gap across disciplines to explore fraudsters' decision-making processes more thoroughly via digital interactions with targets using IDT in tandem with CEP (Buller & Burgoon, 1996; Short, 1998). The findings collected from these illicit online marketplace forums emphasized several significant findings.

First, surprisingly the bivariate analysis shows a positive relationship between offenders' and offender victims' frequency of messages before, after, and overall (i.e., total) during an online fraud event. This is opposite of the stated hypothesis. The findings support previous research suggesting the contextual environmental influences offenders' interactions (Dickinson & Wright, 2015; Topalli et al., 2002). However, in contrast to previous research (Toma & Handcock, 2010; 2012; Ho et al., 2016) and the hypothesis, the situational context of offenders positively influences the frequency of messages deployed. Nevertheless, this counterintuitive result may depend on the offenders' cognition and behavior (e.g., Proposition 18 of IDT), which influence their decision-making processes (i.e., sophistication) when interacting with targets because ultimately, the success of an online fraud event depends on the offender (senders) ability to deceive their target(s) (Buller & Burgoon, 1996; Short, 1998). Therefore, it is important to examine the offenders' decision-making processes within their contextual and situational environment (Maimon & Louderback, 2019).

Offenders' messages are positively correlated with offender victim messages. Perhaps, there is not a negative correlation because offenders are trying to appeal to individuals' cognition by blending into the situational context in ongoing message communications with their targets. For example, the offender may be mirroring or mimicking the actions and interactions of the target by sending a similar count of messages to conform to the "social norms" and consequently avoid detection. This interaction is important because it can help practitioners, researchers, and agencies understand that fraudsters are human beings that display the same characteristics as victims (e.g., communication tactics/cues) (Cole, forthcoming). Additionally, this observed interaction can educate and bring awareness to these professions as well as the general population about how easy it is to fall victim to online fraud; because it suggests the more offenders can communicate with the target, the more information (e.g., money) they are able to receive from the victim.

This finding suggests that offenders use their cognitive skills to successfully attack their targets. For example, the type of attack was not related to message frequency. Therefore, it appears that offenders are using cues from the victim, such as message frequency, and mirroring that to be successful. These findings will allow us to identify fraudsters (e.g., use of cues, reciprocated rates of message frequency) which can lead to more effective preventative and combative strategies to lessen online fraud events and overall victimizations.

Second, the frequency of messaging by offender victims is related to offender message frequency before, after and overall (i.e., total) during an online fraud event and are statistically significant in the multivariate models. Several factors could explain these observations. It is possible offenders and offender victims' may be responding not just to frequency but also to linguistics cues (i.e., urgency and delay cues). However, the frequency of messages does not

account for this intrinsic humanistic exchange. Offenders' interactions with offender victims support Proposition 18 of IDT that suggests the success of a deceptive (i.e., fraud) event depends on the senders' (i.e., offenders) cognition and behavior throughout the target conversation. Offenders who are successful in defrauding offenders' victims, observable through offenders' microsocial interactions (i.e., CEP), are able to process the situational context and adjust their behaviors (in this examination, message count) accordingly to successfully defraud targets. These results provide important insights into offenders' decision-making processes and emphasize the importance of human dominance over computational tools (Lavorgna, 2014; Leclerc, 2013; Gilmore, 2014; Zhu et al., 2013).

The current study is not without limitations. Prior research emphasizes that it is impossible to perfectly categorize the contextual and situational environment variables involved during a criminal event (Clark & Cornish, 2003, p. 51; Wortley, 2001, p.75). Additionally, the situational context could be influenced by the count of messages sent by both offender victims and offenders. An observer, for example, could not be shown the entire history (i.e., log) of messages. This result could be attributed to the sophistication of online offenders, as suggested by prior research. In addition, other factors may be related to message frequency such as personality traits (Chan et al., 2014) and demographic characteristics (Chang & Chang, 2014), along with their decision-making processes in the midst of an online fraud event. Further research should attempt to account for these other factors.

Furthermore, the study is limited by the researcher's inability to know for certain the actors' intentions or reactions during the development of a fraud event. This inability may mean that there are additional messages that are not detected, which would mean that the entire situational context is not considered. In addition, a more thorough examination of the key actors

regulating the cybercrime ecosystem is imperative (Kigerl, 2018; Kigerl, 2020; Maimon & Louderback, 2019). Another limitation of this study was the small sample size, which could be influenced by offenders' discrete nature online. Even with a small sample, message frequency was consistently significant across models.

This study aimed to examine the offenders' decision-making processes (via digital communications) with targets/victims. The findings suggest the situational environment influences offenders' cognition and behavior during the development of an online fraud event. Overall, this study strengthens the presumption that offenders' communications with other offenders (victims) differ based on their situational and contextual environment (Topalli et al., 2002). It consequently emphasizes offenders' strategic online interactions and, within this situational context, the code of the keyboard between offenders and offender victims. Although there is room for further progress in determining the variations in offenders' decision-making processes, these findings provide support for prior research examining offenders' interactions (via CEP) within the physical environment (Dickinson & Wright, 2015; Jacobs & Wright, 2006; Topalli et al., 2002). To develop upon offenders' decision-making, the inclusion of important theoretical issues within the criminological field that have a bearing on the micro-level analysis of offenders should guide academics, policymakers, and others in future research.

Chapter 5: Conclusion

5.1. Introduction

The main goal of this dissertation was to determine to what extent online fraudsters employed different approaches, tactics, and strategies based on their perception of the targets' (or victims') situational environment. To examine the influence of the situational environment on online fraudsters' various approaches, tactics, and strategies, this dissertation presented three studies to explore offenders' decision-making processes (via SE characteristics and tactics) against other offenders online. Based on prior research, it was expected that the situational environment would influence offenders' decision-making processes when targeting other offenders (see Erdmann & Reinecke, 2021, Reiss, 1981 and Berg & Schreck, 2021) online (Kigerl, 2018; Kigerl, 2020).

The criminal event perspective (CEP) and interpersonal deception theory (IDT) were used in tandem to examine offenders' and offender victims' interactions during the development of an online fraud event throughout this dissertation (Buller & Burgoon, 1996; Short, 1998). Specifically, CEP was used to explore, identify, and explain the microsocial development of a fraud event online. While interpersonal deception theory (IDT), a communications theory, was used to examine the social interactions (via written communications) between online fraudsters and their targets (Buller & Burgoon, 1996; Short, 1998).

To examine offenders' decision-making processes, I conducted a scoping review of the situational factors supporting offenders' socially engineered (SE) attacks (via characteristics and tactics) and analyzed offenders' decision-making processes through fraudsters' interactions with other offenders in two independent studies using self-collected data from Telegram. Telegram is an encrypted social media platform where I identified channels (i.e., online forums) where

offenders sold victims' (both non-offending and offending victims) personal, sensitive, and financial information. I systemically monitored 52 Telegram channels for twelve weeks for reports (via screenshotted conversations of the fraud attacks) of successful online fraud attacks among offenders.

The channels were divided into "exposure channels" and "ripping channels." Exposure channels, commonly referred to as "Ripper Walls," were dedicated to exposing offenders who had "ripped off" or defrauded other Telegram users and contained minimal to no active sales of stolen or illicit content. "Ripping channels" were forums dedicated to selling illicit fraud services and products. I separated and used data from the "Ripping Channels" and "Ripper Walls" in different studies to systematically examine aspects of my research questions.

The "Ripper Walls" provided me with more data (i.e., message screenshots between offenders and offender victims); therefore, those channels were used to analyze linguistic cues among offenders. A total of 225 conversations were examined from these channels. The "Ripping Channels" did not provide me with as much data (e.g., message screenshots between offenders and offender victims) because they were dedicated to actively selling illicit information. Therefore, they were used to examine the frequency of messaging between offenders and offender victims. A total of 80 conversations were analyzed from these channels. The abundance of information related to online fraud and other illicit activities associated with fraud on Telegram demonstrates that additional research could be conducted and or assessing the prevalence of the offender victim overlap online.

5.2 Chapter 2 (Study 1)

The first study of the dissertation (scoping review) contributed to the criminological field by providing a conceptualization of offenders' SE characteristics and tactics deployed during online fraud attacks. I achieved this by deploying Boolean logic across nine databases to collect literature on offenders' decision-making processes against non-offending and offending victims.[53] Additionally, I consulted grey literature to ensure a thorough review of offenders' online fraud attacks (via their SE characteristics and/or tactics). The search yielded 25 relevant results that helped me answer the question, "What situational factors support the development of a successful online fraud event against targets?"

The findings from the scoping review emphasized the influence of the situational environment on offenders by depicting the various online fraud attacks utilized to defraud targets (e.g., non-offending and offending victims). This was important to examine considering the ever-increasing prevalence of monetary losses attributed to and victims of fraudsters schemes. Furthermore, the study demonstrates how critical micro-social interactions are overlooked by researchers, practitioners, and law enforcement agencies. For example, most studies excluded from the scoping review associated with online fraudsters focused on quantifying offenders' actions online instead of examining their interactions with targets that provide fraudsters with the information that enables a successful fraud event. Arguably, the absence of analyzing the micro-social level of offenders online has ultimately negatively impacted the ability to track offenders, creating ambiguity about the importance of the human interaction involved in online crime.

[53] The yielded search included offenders' decision-making processes against non-offending because of the limited amount of published research examining the microsocial interactions between online fraudsters and their targets.

5.3 Chapter 3 (Study 2)

The second study of this dissertation examined the influence of offenders' interactions with targets during the development of an online fraud event. The question "What are the SE characteristics and tactics offenders develop for successful online fraud events against other offenders?" guided me in analyzing the offenders' microsocial interactions via their tactical deployed linguistic cues. Specifically, offenders' socially engineered (SE) characteristics (i.e., linguistic cues), such as delay and urgency cues, used when interacting with other targets observed in 225 conversations were examined. Proposition 3 of IDT indicates the success of a deceitful event relies upon the deceiver's non-strategic arousal cues and non-involvement. Thus, it was hypothesized that offenders (i.e., fraudsters) use specific non-strategic arousal cues and non-involvement during the development of an online fraud event to successfully defraud their targets. Specifically, I hypothesized the frequency of offenders' [rippers] linguistic tactical urgency cues would be more prevalent before the completion of an online fraud event compared to offender victims' [fraudsters] cues of urgency (e.g., "now"). Alternatively, urgency cues will be used more frequently by offender victims' [fraudsters] than offenders' [rippers] after the completion of an online fraud event.

I examined these hypotheses by examining 225 fraudulent conversations from "Ripper Walls," where offenders reported online fraud perpetration by other offenders. The preliminary findings from a series of chi-square analyses and independent group t-tests suggest a relationship between written linguistic cues used by offenders and offender victims during the development of an online fraud event. Specifically, offenders' use of tactical urgency cues before the fraud is associated with offender victims' presentational cues of urgency. For example, 9.78% of written communications from fraudsters before a fraud event contain urgency cues, but only 1.33% of

written communications from offender victims before a fraud event contain urgency cues ($p < 0.001$). These findings suggest that offenders strategically deploy tactical urgency and delay cues to successfully defraud their targets.

Additional independent variables related to the situational context indicate that the development of an online fraud event influences offenders' decision-making processes. For instance, offender victims' use of urgency cues before the completion of an online fraud event appears to be related to a higher mean number of offenders' messages to offender victims (M=42.33, SD=54.47) compared to when offender victims' do not send urgency cues to offenders (M=16.08, SD=24.27). The difference illustrates how offenders respond to targets depending on what the target relays to them; thus, highlighting offenders' strategic decision-making processes during an online fraud event (see Proposition 3 of IDT, Buller & Burgoon, 1996). Therefore, identifying the use of offenders' linguistic cues is important because it emphasizes how the situational context influences how offenders interact with targets in the most subtle way, to which a computer often cannot adjust (Lavorgna, 2014; Leclerc, 2013).

5.4 Chapter 4 (Study 3)

Lastly, the third study of this dissertation examined the influence of the situational context on offenders' decision-making processes within active illicit online fraud forums. The question "How does the situational environment influence offenders' SE characteristics and tactics during the development of an online fraud event against offending victims?" was created and assisted me in analyzing the offenders' microsocial interactions via the deployed frequency of messages. Based on Proposition 18 of IDT, it was hypothesized that the offender's cognition and behavior (i.e., decision-making processes) observed through the count of messages sent by

the offender victim before a fraud event is negatively correlated with the count of messages sent by the offender before the fraud event. Additionally, it was hypothesized that the count of messages sent by the offender victim after a fraud event is negatively correlated with the count of messages sent by the offender after the fraud event (e.g., microsocial interactions via written communications, see Short, 1998) (Buller & Burgoon, 1996).

The findings in this study suggest offenders strategically adapt their actions based on their microsocial interactions with targets. For instance, the findings indicate that offenders' and offender victims' interactions are positively correlated. Specifically, the bivariate and multivariate findings indicate that (via offender victims' messages influence offenders' message frequency) the situational context in which offenders act influences their decision-making processes. Specifically, the counts of messages by offender victims and offenders are positively correlated before, after, and combined (e.g., total) during a fraud event in the bivariate analyses.

The multivariate analyses presented the relationship between offender victims' frequency of messaging and offender frequency of messaging. The findings indicate that the number of offender victim messages was related to an increase in the expected count of messages by the offender, even when accounting for other proposed relevant factors. Taken together, these findings highlight that when offenders successfully defraud targets (i.e., offender victims), it involves them processing their situational context and adjusting their behaviors (in this examination, message count) accordingly.

Considering the findings presented in chapter 3, it seems that the situational context influences offenders' decision-making processes during the development of an online fraud event. Offenders, for example, strategically interact with targets in written communications to gather the necessary information to successfully complete an online fraud attack. This finding is

important because it emphasizes how critical offenders' communications, not the tool they use (e.g., computers), are to a successful online fraud event.

5.5 Implications

The current research presented in this dissertation can be used as a blueprint for policy, prevention, practice, and theory. For example, offenders' decision-making process (assessed via linguistic cues and tactics) used to defraud targets identified in chapter 2 and examined in chapters 3 and 4 can train actors on what to look for in their digital interactions (e.g., text messages and emails) to detect nefarious actors. It can also be used to hold those overseeing the interactions between fraudsters and their targets to a higher standard. Specifically, Telegram and other website domains that allow offenders to sell illicit sensitive and financial information could be held liable and financially penalized if they identify offenders deploying these characteristics (i.e., linguistic cues) and tactics to conduct fraud and allow offenders to operate on their websites freely.

These findings raise important theoretical issues that have a bearing on the communications offenders exchange with targets during their microsocial interactions. Although CEP helps explain the micro-social interactions of offenders and their targets, there is no criminological theoretical perspective that demonstrates the influence of offenders' communication among targets. Specifically, the use of IDT, a communications theory, in tandem with CEP, highlights that criminological theory does not adequately explain how the situational context influences offenders' interactions, specifically their decision-making processes in an online fraud event. Further theoretical development is needed to more clearly articulate how online fraudsters are able to successfully engage in their criminal activity. To that end, additional

conversation coding could allow for examining the frequency of messages before and after a fraud event. Also, offenders should be interviewed to assess their self-perceived use of linguistic cues and target selection. These interviews could more thoroughly explain offenders' modus operandi and assist in preventing online fraud by using the offenders' perspective to use in training actors on what to identify and avoid.

In addition, the findings of this study have several important implications for future practice. First, it is insufficient to merely quantify the prevalence of online offenders' crimes. Knowing the prevalence of losses and victims (and offender victims) to online fraud only illustrates the problem, but it does not explain how to combat against it. Since offenders are the key element that must be combatted against, researchers, practitioners, and law enforcement agencies must be willing to more thoroughly examine offenders on a micro-social level since the success of an online fraud attack depends on an offenders' decision-making processes. Specific to the prevalence of online offenders' crimes, the current study highlights how current estimates are likely inaccurate. For instance, it is unlikely criminals report when they have been defrauded of stolen sensitive and financial information by other offenders; thus, there is a "hidden" figure of losses associated with online fraud that is unaccounted for.

Second, the completion (e.g., success) of a fraud attack online relies on the offenders' decision-making processes through their ability to strategically interact with the target not the tool. Therefore, this highlights that computational tools (e.g., anti-virus software) preventing online fraudsters will ultimately fail because an event's success depends on the interaction between offenders and victims. Furthermore, unless academics, policymakers, and agencies examine offenders conducting online fraud, the number of losses and victims will likely continue to increase because the focus will remain on irrelevant variables. It is recommended academics,

policymakers, and agencies use public service announcements, similar to the money mulling[54] public service announcements often posted in financial institutions. Additionally, public service announcements and/or updates should be posted to educate users about fraudsters' SE characteristics and tactics to defraud targets on social media forums, akin to the COVID postings the United States government posted on Facebook and Instagram to update citizens on the portals associated with the virus and to remind targets of fraudsters common schemes used to defraud victims (both non-offending and offending victims) (Chen et al., 2020; Cheong-Iao et al., 2021). Therefore, this dissertation significantly contributes to the criminological field by providing a blueprint for future research and policymakers as they attempt to combat online fraud.

5.5.a Limitations

One issue with the current studies was the sample. First, the sample sizes across all the studies were small; thus, the types of analyses able to be performed were limited. Despite the small sample, some statistically significant findings emerged.

Second, some conversations could not be used because the offender and/or offender victim would delete part of or the entire conversations thread that the reporter (i.e., offender and/or offender victim) was attempting to take a picture (e.g., screenshot). The inability to account for all the interactions between offenders and/or offender victims could raise questions related to the reliability of the results.

Third, offenders written communications between each other were challenging to analyze at times due to grammar errors (e.g., style and syntax) and jargon. Furthermore, the use of emojis during conversations could have influenced the perceived meaning of the communication.

[54] Money mulling is when an individual transfers financial funds associated with criminal activity on behalf of another individual(s). Frequently, a money mule is paid with a portion of the illicit funds.

Nevertheless, the SE characteristics and tactics observed in offenders' and offender victims' messages (e.g., clearing of chats) provide context to the presented inferences in data.

5.6 Conclusion

The research examining the influence of the situational environment on offenders' decision-making processes online was mainly anecdotal before this dissertation. The current dissertation fills this void by comprehensively examining offenders' SE characteristics and tactics deployed during online fraud attacks against victims (i.e., victims and offender victims). The findings from all the studies highlight the critical role offenders' decision-making processes play during the development of an online event. Specifically, offenders' written communications (via linguistic cues and frequency of messages) to offender victims emphasize the critical role offenders' strategic interactions play in a successful online fraud attack; this is important because it underscores how computers are only a tool ordinary offenders use to conduct crime but most importantly that anyone can be a victim even the professional fraudsters (i.e., offender victims). Furthermore, these communications are beneficial because they provide insight into offenders' behavior online that effects all targets (e.g., non-offending and offending victims). Additionally, it highlights offenders ever-evolving SE tactics that negatively influence us all.

APPENDICES

Appendix A. High Profile Cyber Fraud Methods Defined

Online fraud has been defined as the use of "Internet services or software with Internet access to intentionally defraud individuals, organizations or entities" and conceptualized into seven high-profile methods as termed by the FBI (n.d.). These seven high-profile methods are (1) *business email compromise and* (2) *email account compromise (BEC/EAC) scams,* (3) *data breach,* (4) *denial of service attacks,* (5) *malware/scareware,* (6) *phishing spoofing, vishing, and pharming* and (7) *ransomware* with criminals who are central to the operations of these schemes (Federal Bureau of Investigation, n.d.).

1.) *Business email compromise (BEC) scams:* criminals steal monetary funds through unauthorized wire payments from businesses and companies.

2.) *Email account compromise (EAC) scams:* a criminal steals monetary funds through unauthorized wire payments from individual people.

3.) *Data breach scams*: an offender compromises sensitive data and subsequently transfers it from a "secure location to an untrusted environment" (Internet Crime Complaint Center, 2019, p. 25).

4.) *Denial of service attacks:* a criminal floods a network or system with more requests with web traffic than the system can handle.

5.) *Malware/scareware scams:* a criminal demands monetary funds or goods through threats of violence or public exposure.

6.) *Phishing spoofing, vishing, and pharming:* are measured by the IC3 in unison but vary in operation slightly.

7.) *Phishing:* unsolicited emails are sent from criminals who impersonate legitimate companies requesting sensitive, financial, and login credentials.

8.) *Spoofing:* unsolicited SMS text messages are deployed by criminals who impersonate legitimate companies requesting sensitive, financial, and login credentials.

9.) *Vishing:* unsolicited telephone calls are sent from criminals who impersonate legitimate companies requesting sensitive, financial, and login credentials.

10.) *Pharming*: a criminal redirects a website's traffic from a legitimate to an illegitimate website.

11.) *Ransomware scams:* criminals use malicious software to block or deny a person's access to their computer system until money is paid.

Appendix B. Urgency and Delay Linguistic Cues Categized

Psychological research indicates actors desire scarce items, products, and services and consequently will act to serve their completive needs in response to "threat/opportunities." A "threat/opportunity" is when an actor is rewarded or penalized based on their response (i.e., text and email) (Naidoo, 2015; Sidi et al., 2021; Workman, 2007). Below is a table illustrating how the qualitative data was used to create and support the findings. Specifically, I used the unstructured conversations to inform and thus construct the analyzed variables, such as offenders' tactics and offender victims' presented cues. I achieved this by clustering offenders' tactical cues and offender victims' presentation cues into two distinct categories based on previous research, urgency and delay (Atkins & Huang, 2013; Pellon & Anesa, 2019).

Theme Categories	Related Sub-thematic codes	Theme Description	Evidence from data
Urgency Tactical Cues (Cuddy et al., 2011; Naidoo, 2015; Workman, 2007).	- Opportunity (Threat, time-sensitive/expectation)	-Action cues:	- Urgency Words Focused on: "Now," "ASAP," and "immediately" but did not limit my search to those words due to linguistical expressions. - Linguistic singular word cues nudging acting such as "send now," "ASAP," "immediately," and "now."
	- Transaction Salience (i.e., what nudges an actor during a transaction (Naidoo, 2015)).	-Expressive and/or Paralinguistic cues:	- Linguistic sentences w nudging acting such as, "im waiting for you" or threats stating "You going on both ripper walls if u dont send" - Punctuation violating expression norms, such as "????" after a message was sent that stated "Yooo" (Vareberg & Westerman, 2020).
Delay Tactical Cues (Atkins & Huang, 2013)	-Opportunity (Threat, time-sensitive/expectation)	-Pause linguistic cues:	-Urgency Words Focused on: "wait," "hold/,"g," "load/ing," but I did not limit my search to those words due to linguistical expressions.
	-Transaction Salience (i.e., what nudges an actor during a transaction (Naidoo, 2015)).	-Expressive and/or Paralinguistic cues:	-Linguistic singular word cues nudging acting such as "wait," "hold," "load/ing." -Linguistic sentences with nudging actions such as, "We file you sit back" and "I was sleep bro."

REFERENCES

Akers, R. (2009). Social Learning and Social Structure: A General Theory of Crime and Deviance. New Brunswick, NJ: Transaction Publishers.

Aleem, A., & Antwi-Boasiako, A. (2011). Internet auction fraud: The evolving nature of online auctions criminality and the mitigating framework to address the threat. International Journal of Law, Crime and Justice, 39(3), 140-160. doi:10.1016/j.ijlcj.2011.05.003.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3. doi:10.3389/fcomp.2021.563060

Almendra, V., & Enachescu, D. (2012). A Fraudster in a Haystack: Crafting a Classifier for Non-delivery Fraud Prediction at Online Auction Sites. Paper presented at the 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing.

Anderson, A. L., & Meier, R. (2004). Interactions and the Criminal Event Perspective. Journal of Contemporary Criminal Justice.

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. International Journal of Social Research Methodology, 8(1), 19-32. doi:10.1080/1364557032000119616

Atkins, B., & Huang, W. (2013). A Study of Social Engineering in Online Frauds. Open Journal of Social Sciences, 01(03), 23-32. doi:10.4236/jss.2013.13004.

Barlow, J., Warkentin, M., Ormond, D., & Dennis, A. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. Computer Security 39, 145–159.

Beccaria, C. (1764). On Crimes and Punishments: Transaction Publishers.

Benjamin, V., Valacich, J., & Chen, H. (2019). Dice-E: A framework for conducting darkness identification, collection, evaluation with ethics. MIS Quarterly, 43, 1-22.

Benjamin, V., Zhang, B., Nunamaker, J. F., & Chen, H. (2016). Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities. Journal of Management Information Systems, 33(2), 482-510. doi:10.1080/07421222.2016.1205918.

Benson, M. L., Madensen, T. D., & Eck, J. (2009). White-Collar Crime from an Opportunity Perspective. In S. Simpson & D. Weisburd (Eds.), The Criminology of White-Collar Crime Springer.

Benson, S. S. (2009). Recognizing the Red Flags of a Ponzi Scheme. The CPA Journal, 79(6),

18. Retrieved from https://www.proquest.com/docview/212321198?accountid=11226&bdid=14659&_bd=7nDajej3Vp0jsCC7T8fr35cF%2B70%3D.

Berg, M., & Schreck, C. (2021). The meaning of the victim-offender overlap for criminological theory and crime prevention policy. Annual Review of Criminology, 5, 277-297.

Berg, M. T., & Schreck, C. J. (2021). the Meaning of the Victim-Offender Overlap for Criminological Theory and Crime Prevention Policy. Annual Review of Criminology, 5, 277-297.

Bierie, D. M., Detar, P. J., & Craun, S. W. (2013). Firearm Violence Directed at Police. Crime & Delinquency, 62(4), 501-524. doi:10.1177/0011128713498330.

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499. doi:10.1080/0735648x.2019.1692426.

Blommaert, J., & Omoniyi, T. (2006). Email Fraud: Language, Technology, and the Indexical of Globalisation. Social Semiotics, 16(4).

Bowe, M., & Jobome, G. (2001). Fraudulent Activity in Financial Institutions and Optimal Incentive Structures for Managing Operational Risk. Valletta Review, 24, 1-19.

Buller, D., & Burgoon, J. (1996). Interpersonal Deception Theory. Communication Theory, 203-242.

Burns, M., & Moffitt, K. (2014). Automated deception detection of 911 call transcripts. Security Informatics, 3(8).

Carnegie Mellon University. (2020). Information Security Office: Computing Services. Retrieved from https://www.cmu.edu/iso/news/2020/pretexting.html.

Chan, V., Chow, K.-P., Kwan, M., Fong, G., Hui, M., & Tang, J. (2014). An exploratory profiling study of online auction fraudsters. In Advances in Digital Forensics (pp. 43-56).

Chang, J.-S., & Chang, W.-H. (2014). Analysis of fraudulent behavior strategies in online auctions for detecting latent fraudsters. Electronic Commerce Research and Applications, 13(2), 79-97. doi:10.1016/j.elerap.2013.10.004.

Chen, Q., Chen, M., Zhang, W., Wang, G., Xiaoyue, M., & Evans, R. (2020). Unpacking the black box: How to promote citizen engagement through government social media during the COVID-19 crisis. Computers in Human Behavior.

Cheong-Iao Pang, P., Cai, Q., Jiang, W., & Chan, K. (2021). Engagement of Government Social Media on Facebook during the COVID-19 Pandemic in Macao. J Environ Res Public Health, 7.

Chiuwa, I., & Anurudu, S. (2020). Expressing (Un)certainty through Modal Verbs in Advance Fee Fraud Emails. Covenant Journal of Language Studies (CJLS) 8.

Choi, K.-s. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. International Journal of Cyber Criminology, 2(1), 308-333.

Clarivate. (n.d.). Endnote Retrieved from https://clarivate.com/innovation-exchange/solution/endnote/.

Clarke, R., & Cornish, D. (1985). Modeling Offenders' Decisions: A Framework for Research and Policy.

Cohen, L., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588-608.

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. Clin Pract Epidemiol Ment Health, 16, 24-35. doi:10.2174/1745017902016010024.

Conradt, C. (2012). Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. International Journal of Cyber Criminology, 6.

Cornish, D., & Clarke, R. Crime Specialization, Crime Displacement and Rational Choice Theory. Criminal Behavior and the Justice System 103-117.

Cornish, D., & Clarke, R. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. Crime Prevention Studies, 16.

Costin, A., Isacenkova, J., Balduzzi, M., Francillon, A., & Balzarotti, D. (2013, 10-12 July 2013). The role of phone numbers in understanding cyber-crime schemes. Paper presented at the 2013 Eleventh Annual Conference on Privacy, Security and Trust.

Dahlqvist, F., Patel, M., Rajko, A., & Shulman, J. (2019). Growing opportunities in the Internet of Things.

Daudt, H., Mossel, C., & Scott Lee, D. (2013). Enhancing the scoping study methodology: a large, inter-professional team's experience with Arksey and O'Malley's framework. BMC Med Res Methodol, 13.

Deibert, G. R., & Miethe, T. D. (2003). Character contests and dispute-related offenses. Deviant Behavior, 24(3), 245-267. doi:10.1080/713840200.

Dickinson, T. (2014). Exploring the Drugs/Violence Nexus Among Active Offenders. Criminal Justice Review, 40(1), 67-86. doi:10.1177/0734016814562422.

Dickinson, T., & Wright, R. (2015). Gossip, Decision-making and Deterrence in Drug Markets. British Journal of Criminology, 55(6), 1263-1281. doi:10.1093/bjc/azv010.

Diekmann, A., Jann, B., & Wyder, D. (2004). Trust and Reputation in Internet Auctions. In. Dupont, B., Cote, A., Boutin, J., & Fernande, J. M. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World." American Behavioral Scientist, 61, 1219-1243.

Dupont, B., Cote, A., Boutin, J., & Fernande, J. M. (2017). Darkode: Recruitment Patterns and Transactional Features of "the Most Dangerous Cybercrime Forum in the World." American
Behavioral Scientist, 61, 1219-1243.

Dupont, B., & Whelan, C. Enhancing relationships between criminology and cybersecurity. Journal of Criminology, 0(0), 00048658211003925. doi:10.1177/00048658211003925.

Erdmann, A., & Reinecke, J. (2021). What Influences the Victimization of High-Level Offenders? A Dual Trajectory Analysis of the Victim-Offender Overlap From the Perspective of Routine Activities With Peer Groups. Journal of Interpersonal Violence.

Fagan, J., & Wilkinson, D. (1998). Guns, Youth Violence, and Social Identity in Inner Cities. Crime & Justice, 105-188.

"Fraud," 2019.

Federal Bureau of Investigation (n.d.). Scams and Safety. Retrieved from https://www.fbi.gov/scams-and-safety/common-fraud-schemes/internet-fraud.

Federal Bureau of Investigation. (2007). Financial Crimes Report 2007: Financial Crimes Report to the Public 2007. Retrieved from https://www.fbi.gov/stats-services/publications/fcs_report2007

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in Social Engineering and Their Use in Phishing. Paper presented at the Human Aspects of Information Security, Privacy, and Trust.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. (2007). An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants∗. Paper presented at the CCS, Alexandria, Virginia.

Garg, V., Afroz, S., Overdorf, R., & Greenstadt, R. (2015). Computer-Supported Cooperative Crime.

Gaspareniene, L., & Remeikiene, R. (2015). Digital Shadow Economy: a Critical Review of the Literature. Mediterranean Journal of Social Sciences, 6.

Gilmore, N. (2014). Understanding Money Laundering –A Crime Script Approach. The European Review of Organised Crime.

Goffman, E. (1955). On Face-Work: An Analysis of Ritual Elements in Social Interaction. In Paradigm Development: 1950s-1970s (pp. 222-247).

Grabosky, P. N. (2016). The evolution of cybercrime, 2006–2016. In P. N. Grabosky (Ed.), Cybercrime Through an Interdisciplinary Lens: Routledge.

Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking: Wiley.

Hadnagy, C. (2010). Social Engineering: The Art Of Human Hacking.

Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking.

Hadnagy, C. (2019). Social Engineering: The Science of Human Hacking. Indianapolis, IN: Wiley.

Halder, A. (2019). Perception of Imperialism: American Hegemony and Vulnerability Due to Cyber Threats in the Global Age.

Handa, K., & Dhawan, S. (2012). Fault Detection and Deployment of Security Mechanisms in E-mail Systems. International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS).

Ho, S. M., Hancock, J. T., Booth, C., Liu, X., Liu, M., Timmarajus, S. S., & Burmester, M. (2016). Real or Spiel? A Decision Tree Approach for Automated Detection of Deceptive Language-Action Cues. Paper presented at the Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS).

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. Social Science Computer Review, 31, 165–177.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. Criminal Justice Studies, 23(1), 33-50. doi:10.1080/14786011003634415.

Horney, J., Osgood, W., & Marhsall, I. (1995). Criminal Careers in the Short-Term: Intra-Individual Variability in Crime and Its Relation to Local Life Circumstances. American sociological review, 60, 655-673.

Huang, J., Stringhini, G., & Yong, P. (2015). Quit Playing Games With My Heart: Understanding Online Dating Scams.

Hutchings, A., & Clayton, R. (2016). Exploring the Provision of Online Booter Services. Deviant Behavior, 37(10), 1163-1178. doi:10.1080/01639625.2016.1169829.

Hutchings, A., & Holt, T. J. (2015). A Crime Script Analysis of the Online Stolen Data Market: Table 1. British Journal of Criminology, 55(3), 596-614. doi:10.1093/bjc/azu106.

“Identity Theft," 2022.

Internet Crime Complaint Center. (2017). 2016 Internet Crime Report.

Internet Crime Complaint Center. (2018). 2017 Internet Crime Report.

Internet Crime Complaint Center. (2021). Internet Crime Report 2020.

Internet Crime Complaint Center. (2022). Internet Crime Report 2021.

Isacenkova, J., Thonnard, O., Costin, A., Balzarotti, D., & Francillon, A. (2013, 23-24 May 2013). Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations. Paper presented at the 2013 IEEE Security and Privacy Workshops.

Jacobs, B. A., & Wright, R. (2006). Street justice: Retaliation in the criminal underworld. New York, NY: Cambridge University Press.

Jacques, S. (2010). The necessary conditions for retaliation: Toward a theory of non-violent and violent forms in drug markets. Justice Quarterly, 27, 186-205.

Jacques, S., & Reynald, D. M. (2011). The Offenders' Perspective on Prevention. Journal of Research in crime and delinquency, 49(2), 269-294. doi:10.1177/0022427811408433

Jacques, S., & Wright, R. (2008). The Victimization-Termination Link. Criminology 46.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Chapter 12 - Cybercrime classification and characteristics. In B. Akhgar, A. Staniforth, & F. Bosco (Eds.), Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 149-164): Syngress.

Janankhani, H., Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator’s Handbook (pp. 149-164).

Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I., & Olorunyomi, B. R. (2016). Gendered Alternative to Cyber Fraud Participation: an Assessment of Technological Driven Crime in Lagos State, Nigeria. Gender & Behaviour, 14.

Jones, J., & McCoy, D. (2014, 23-25 Sept. 2014). The check is in the mail: Monetization of Craigslist buyer scams. Paper presented at the 2014 APWG Symposium on Electronic Crime Research (eCrime).

Khandelwal, R. (2019). Taxation of Cryptocurrency Hard Forks. The Contemporary Tax Journal, 8.

Kigerl, A. (2017). Profiling Cybercriminals. Social Science Computer Review, 36(5), 591-609.

doi:10.1177/0894439317730296.

Kigerl, A. (2018). Profiling Cybercriminals:Topic Model Clustering of Carding Forum Member Comment Histories. Social Science Computer Review, 36(5), 591-609. doi:10.1177/0894439317730296.

Kigerl, A. (2020). Behind the Scenes of the Underworld: Hierarchical Clustering of Two Leaked Carding Forum Databases. Social Science Computer Review. doi:10.1177/0894439320924735.

Koch, C. (2017). To Catch a Catfish: A Statutory Solution for Victims of Online Impersonation. . University of Colorado Law Review.

Konkel, R., Hafemeister, A., & Daigle, L. E. (2021). The Effects of Risky Places, Motivated Offenders, and Social Disorganization on Sexual Victimization:A Microgeographic- and Neighborhood-Level Examination. Journal of Interpersonal Violence, 36.

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), 541-562. doi:https://doi.org/10.1016/j.intman.2005.09.009.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. Crime Science, 3.

Lavorgna, A. (2014). Internet-mediated drug trafficking: towards a better understanding of new criminal dynamics. Trends in Organized Crime, 17(4), 250-270. doi:10.1007/s12117-014-9226-8.

Lavorgna, A. (2014). Wildlife trafficking in the Internet age. Crime Science, 3.

Lazarus, S. (2018). Birds of a Feather Flock Together: The Nigerian Cyber Fraudster (Yahoo Boys) and Hip Hop Artists. Criminology, Criminal Justice, Law & Society, 19(2), 63-80.

Leech, N. L., & Onwuegbuzie, A. J. (2008). Qualitative data analysis: A compendium of techniques and a framework for selection for school psychology research and beyond. School Psychology Quarterly, 23(4), 587-604. doi:10.1037/1045-3830.23.4.587.

Leclerc, B. (2013). New developments in script analysis for situational crime prevention: moving beyond offender scripts. In B. Leclerc & R. Wortley (Eds.), Cognition and Crime.

Leclerc, B. (2013). Script analysis for crime controllers: Extending the reach of situational prevention. In S. Caneppele & F. Calderoni (Eds.), Organized Crime, Corruption, and Crime Prevention - Essays in honours of Ernesto U. Savona. New York: Springer.

Leukfeldt, E. (2014). Cybercrime and social ties. Trends in Organized Crime, 17(4), 231-249. doi:10.1007/s12117-014-9229-5.

Leukfeldt, E. R., Kleemans, Edward, Stol, Wouter. (2017). The use of online crime markets by cybercriminal networks: A view from within. American Behavioral Scientist, 61(11), 1387-1402.

Leukfeldt, R., & Holt, T. (2020). The Human Factor of Cybercrime.

Lusthaus, J. (2012). Trust in the world of cybercrime. Global Crime, 71-94. doi:10.1080/17440572.2012.674183

Luangrath, A. W., Peck, J., & Barger, V. A. (2017). Textual paralanguage and its implications for marketing communications. J. Consum. Psychol. 27, 98–107.

Macinnes, I. (2005). Causes of Disputes in Online Auctions. Electronic Markets, 15(2), 146-157.

Madarie, R., Ruiter, S., Steenbeek, W., & Kleemans, E. (2019). Stolen account credentials: an empirical comparison of online dissemination on different platforms. Journal of Crime and Justice, 42(5), 551-568. doi:10.1080/0735648x.2019.1692418

Maimon, D., Howell, C. J., Moloney, M., & Park, Y. S. (2020). An Examination of Email Fraudsters' Modus Operandi. Crime & Delinquency, 1-20.

Maimon, D., & Louderback, E. R. (2018). Cyber-Dependent Crimes: An Interdisciplinary Review. The Annual Review of Criminology.

Maimon, D., Santos, M., & Park, Y. (2019). Online deception and situations conducive to the progression of non-payment fraud. Journal of Crime and Justice, 42(5), 516-535. doi:10.1080/0735648x.2019.1691857

Maruna, S. (2010). "Mixed method research in criminology: Why not go both ways?". In Handbook of quantitative criminology (pp. pp. 123-140). New York: Springer.

Mbaziira, A., & Jones, J. (2016). A Text-based Deception Detection Model for Cybercrime.

Mesch, G., & Dodel, M. (2018). Low Self-Control, Information Disclosure, and the Risk of Online Fraud. American Behavioral Scientist, 62, 1356-1371.

Mikhaylov, A., & Frank, R. (2016). Cards, Money and Two Hacking Forums: An Analysis of Online Money Laundering Schemes. Paper presented at the European Intelligence and Security Informatics Conference.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. IEEE Security & Privacy, 13(5), 99-103. doi:10.1109/msp.2015.107

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. Paper presented at the 2011 ACM SIGCOMM Conference on

Internet Measurement Conference, Berlin, German.

Mubarak, M. F., Yahya, S., & Shaazi, A. F. A. (2019, 7-7 Oct. 2019). A Review of Phone Scam Activities in Malaysia. Paper presented at the 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET).

Mubarak, M. F., Yahya, S., & Shaazi, A. F. A. (2019). A Review of Phone Scam Activities in Malaysia Paper presented at the International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia.

Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Med Res Methodol, 18(1), 143. doi:10.1186/s12874-018-0611-x.

Murad, U., & Pinkas, G. (1993). Unsupervised Profiling for Identifying Superimposed Fraud. Paper presented at the European Conference on Principles of Data Mining and Knowledge Discovery.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 5, 773- 793.

Norris, G., Brookes, A., & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. Journal of Police and Criminal Psychology, 34(3), 231-245. doi:10.1007/s11896-019-09334-5

Park, S. Y. (2016). Active Data Collection Techniques to Understand Online Scammers and Cybercriminals (Doctor of Philosophy). The University of Maryland.

Park, W., Kim, S., & Ryu, W. (2015). Detecting Malware with Similarity to Android application. IEEE, 1249-1251.

Park, Y., Jones, J., McCoy, D., Shi, E., & Jakobsson, M. (2014). Scambaiter: Understanding Targeted Nigerian Scams on Craigslist.

Pellon, I., & Anesa, P. (2019). Advance-Fee Scams: A Corpus and Genre Analysis.

Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decision Support Systems, 133. doi:10.1016/j.dss.2020.113303.

Pratt, T. C., Cullen, F. T., Sellers, C. S., Thomas Winfree, L., Madensen, T. D., Daigle, L. E., . . . Gau, J. M. (2010). The Empirical Status of Social Learning Theory: A Meta-Analysis. Justice Quarterly, 27(6), 765-802. doi:10.1080/07418820903379610.

PRISMA. (n.d.). Welcome to the Preferred Reporting Items for Systematic Reviews and Meta-

Analyses (PRISMA) website! Retrieved from https://prisma-statement.org//.

Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. 494-512.

Rege, A., Williams, K., & Mendlein, A. (2019). A Social Engineering Course Project for Undergraduate Students Across Multiple Disciplines. Paper presented at the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK.

Reiss, K. (1981). Type, Kind and Individuality of Text: Decision Making in Translation. Poetics Today.

Reurink, A. (2018). Financial Fraud: A Literature Review. Journal of Economic Surveys, 32(5), 1292-1325. doi:10.1111/joes.12294

Riga, A. (2003 July 18, 2003). Taking on Nigerian E-mail Con Games Becomes a Crusade 'Scam Baiters': Web Sites Describe Tricks Played on Fraud Artists Who Bilk People of Millions. The Gazette [Montreal, Quebec].

Rogers, M., Smoak, N. D., & Liu, J. (2006). Self-reported Deviant Computer Behavior: A Big-5, Moral Choice, and Manipulative Exploitive Behavior Analysis. Deviant Behavior, 245-268.

Schaffer, D. (2012). The Language of Scam Spams: Linguistic Features of "Nigerian Fraud" E-Mails. ETC: A Review of General Semantics, 69(2), 157-179.

Shaw, C. R., & McKay, H. D. (1942). Juvenile Delinquency and Urban Areas: University of Chicago Press.

Short, J. (1998). The level of explanation problem revisited—The American Society of Criminology 1997 presidential address. Criminology, 36, 3-36.

Sidi, Y., Glikson, E., & Cheshin, A. (2021). Do You Get What I Mean?!? The Undesirable Outcomes of (Ab)Using Paralinguistic Cues in Computer-Mediated Communication. Front Psychol, 12.

Siering, M., Koch, J. A., & Deokar, A. V. (2016). Detecting Fraudulent Behavior on Crowdfunding Platforms: The Role of Linguistic and Content-Based Cues in Static and Dynamic Contexts. Journal of Management Information Systems, 33(421-455).

Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. Trends in Organized Crime, 15, 111–129.

Stanelyte, D., Radziukyniene, N., & Radziukynas, V. (2022). Overview of Demand-Response Services: A Review. Energies, 15(5), 1659. Retrieved from

https://www.proquest.com/docview/2637651085?accountid=11226&bdid=14659&_bd=1jBfI7vMknspVmbSlj1Ws68pd3I%3D

Statista. (2022, July 6). Internet usage in the United States - statistics & facts. Retrieved from Internet: https://www.statista.com/topics/2237/internet-usage-in-the-united-states/#dossierKeyfigures.

Telegram. (n.d.). Telegram Privacy Policy. Retrieved from https://telegram.org/privacy.

Toma, C., & Hancock, J. (2010). Reading between the Lines: Linguistic Cues to Deception in Online Dating Profiles. Paper presented at the Proceedings of the 2010 ACM conference on Computer supported cooperative work.

Toma, C., & Handcok, J. (2012). What Lies Beneath: The Linguistic Traces of Deception in Online Dating Profiles. Journal of Communication 62(1).

Topalli, V. (2005). When Being Good Is Bad: An Expansion of Neutralization Theory. Criminology, 43, 797-836.

Topalli, V., & O'Neal, E. C. (2003). Retaliatory motivation enhances attributions of hostility when people process ambiguous social stimuli. Aggressive Behavior, 29(2), 155-172. doi:10.1002/ab.10068.

Topalli, V., Wright, R., & Fornango, R. (2002). Drug Dealers, Robbery and Retaliation. Vulnerability, Deterrence and the Contagion of Violence. British Journal of Criminology, 42(2), 337-351. doi:10.1093/bjc/42.2.337.

Tsai, F., Chang, E., & Kao, D. (2018). WhatsApp Network Forensics: Discovering the Communication Payloads behind Cybercriminals. Paper presented at the International Conference on Advanced Communications Technology (ICACT).

Turanovic, J. J., & Pratt, T. C. (2013). The Consequences of Maladaptive Coping: Integrating General Strain and Self-Control Theories to Specify a Causal Pathway Between Victimization and Offending. Journal of Quantitative Criminology, 29(3), 321-345. doi:http://dx.doi.org/10.1007/s10940-012-9180-z.

Tzani-Pepelasi, C., Nilsson, M., Lester, D., Pylarinou, N., & Ioannou, M. (2020). Profiling HMRC and IRS Scammers by Utilizing Trolling Videos: Offender Characteristics. Journal of Forensic and Investigative Accounting, 12.

Urbanik, M.-M., & Haggerty, K. D. (2018). '# It's Dangerous': The online world of drug dealers, rappers and the street code. British Journal of Criminology.

Van Der Zee, S., Clayton, R., & Anderson, R. (2019). The gift of the gab: Are rental scammers skilled at the art of persuasion?

Vasek, M., & Moore, T. (2018). Analyzing the Bitcoin Ponzi Scheme Ecosystem. Paper

presented at the International Conference on Financial Cryptography and Data Security.

Verizon. (2019). 2018 Data Breach Investigations Report: 11th edition.

Verizon. (2020). 2019 Data Breach Investigations Report.

Verizon. (n.d.). Verizon Internet Security Suite Multi-Device. https://www.verizon.com/support/residential/internet/essentials/internet-security-suite

Wani, M., & Jabin, S. (2016). A sneak into the Devil's Colony - Fake Profiles in Online Social Networks. Retrieved from https://arxiv.org/abs/1705.09929.

Wang, J., Gupta, M., & Rao, H. (2015). Insider threats in a financial institution: analysis of attack-proneness of information systems applications. MIS Q, 39, 91-112.

Weber, K., Schutz, A., Fertig, T., & Muller, N. (2020). Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users. Paper presented at the International Conference on Human-Computer Interaction.

Wilsem, J. v. (2013). Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. Journal of Contemporary Criminal Justice, 29(4), 437-453. doi:10.1177/1043986213507402.

White, C., & Burgoon, J. (2001). Adaptation and Communicative Design: Patterns of Interaction in Truthful and Deceptive Conversations. Human Communication Research, 27(1), 9-37.

Wortley, R. (1997). A Classification of Techniques for Controlling Situational Precipitators of Crime. Security Journal, 14, 63-82.

Wortley, R. (1997). Reconsidering the role of opportunity in situational crime prevention. In G. Newman, R. Clark, & S. Shoham (Eds.), Rational choice and situational crime prevention.: Dartmouth Publishing Company.

Wright, R., & Topalli, V. (2013). Choosing Street Crime In F. T. Cullen & P. Wilcox (Eds.), The Oxford Handbook of Criminological Theory.

Xia, P., Wang, H., Gao, B., Su, W., Yu, Z., Luo, X., . . . Xu, G. (2021). Trade or Trick? Detecting and Characterizing Scam Tokens on Uniswap Decentralized Exchange. Paper presented at the Proc. ACM Meas. Anal. Comput. Syst.

Yip, M., Shadbolt, N., & Webber, C. (2013). Why Forums? An Empirical Analysis into the Facilitating Factors of Carding Forums. Computer & Security.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Policing and Society, 23(4), 516-539. doi:10.1080/10439463.2013.780227.

Zhang, B., Zhou, Y., & Faloutsos, C. (2008, 7-10 Jan. 2008). Toward a Comprehensive Model in Internet Auction Fraud Detection. Paper presented at the Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008).

Zhang, Y., Bian, J., & Zhu, W. (2013). Trust fraud: A crucial challenge for China's e-commerce market. Electronic Commerce Research and Applications, 12(5), 299-308. doi:https://doi.org/10.1016/j.elerap.2012.11.005.

Zhang, Y., Zhou, J., & Zhou, N. (2007). Audit committee quality, auditor independence, and internal control weaknesses. Journal of Accounting and Public Policy, 26(3), 300-327. doi:https://doi.org/10.1016/j.jaccpubpol.2007.03.001.

Zhou, H., Chai, H. F., & Qiu, M. L. (2018). Fraud detection within bankcard enrollment on mobile device-based payment using machine learning. Frontiers of Information Technology & Electronic Engineering, 19(12), 1537-1545. doi:10.1631/FITEE.1800580.

Zhou, L., Burgoon, J. K., & Twitchell, D. (2003). A Longitudinal Analysis of Language Behavior of Deception in E-mail. Paper presented at the Intelligence and Security Informatics, Tucson, AZ.

Zhou, L., Burgoon, J. K., Twitchell, D. P., Qin, T., & Nunamaker Jr, J. F. (2004). A Comparison of Classification Methods for Predicting Deception in Computer-Mediated Communication. Journal of Management Information Systems, 20(4), 139-166. doi:10.1080/07421222.2004.11045779.

Zhou, L., Twitchell, D., Qin, T., Burgoon, J. K., & Nunamaker Jr, J. F. (2002). An Exploratory Study into Deception Detection in Text-based Computer-Mediated Communication. Paper presented at the Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03).

Zhu, Y., Xi, D., Song, B., Zhuang, F., Chen, S., Gu, X., & He, Q. (2020). Modeling Users' Behavior Sequences with Hierarchical Explainable Network for Cross-domain Fraud Detection. Paper presented at the Proceedings of The Web Conference 2020

VITA

Dr. Tessa Cole was born in Anderson, South Carolina, in 1993. Dr. Cole received a bachelor's degree from Berry College in Rome, Georgia, in 2016. She continued her studies at the University of Tennessee at Chattanooga in criminal justice, where she earned her master's in science in 2018. Dr. Cole pursued a doctoral degree at Georgia State University in the criminology and criminal justice department. Dr. Cole completed this dissertation and will graduate with a Ph.D. in criminology and criminal justice from Georgia State University. Her research has examined offenders' decision-making processes online against targets. Dr. Cole's work has been published in peer-reviewed publications such as *Victims & Offenders* and *International Criminal Justice Review* with several forthcoming publications. A few of the awards Dr. Cole has received are the Department of Criminal Justice and Criminology Graduate Teaching Award at Georgia State University in 2021, the Department of Social, Cultural, and Justice Studies Outstanding Graduate Student at the University of Tennessee at Chattanooga in 2018, the Berry College Inspirational Student-Athlete of the Year in 2016 and the O. Wayne Rollins Student Work Award at Berry College in 2015. Additionally, Dr. Cole holds several certificates of completion from U.S. Immigration and Customs Enforcement for operational technology concepts and ethical hacking.

Tessa believes technology is a tool that is commonly exploited by cybercriminals to victimize unsuspecting users; Therefore, she has a desire to educate users about the risks of victimization online and combat those who have perpetrated against others online.

Dr. Cole can be contacted at: tesscole8@gmail.com.