5-1-2023

Essays on the Rationality of Online Romance Scammers

Fangzhou Wang
Georgia State University

ABSTRACT

ESSAYS ON THE RATIONALITY OF ONLINE ROMANCE SCAMMERS

By

FANGZHOU WANG

May 2023

Committee Chair: Dr. David Maimon

Major Department: Criminal Justice and Criminology

The rapid development of the internet has served an essential role in providing communication platforms for people to choose to have personal interactions. One manifestation is using social media platforms and dating services to establish social relationships. The use of online platforms has also provided unscrupulous individuals with malicious intent the ability to target vulnerable victims using bogus romantic intent to obtain money from them. This type of newly evolved cybercrime is called an online romance scamming. To date, online romance scams have spread to every part of the world (i.e., mainly in the United States, China, Canada, Australia, and the UK) and caused considerable financial and emotional damage to victims.

Prior research on online romance fraudsters provides a preliminary understanding of the operational features (stages and persuasive techniques) and their modus operandi. However, the objectivity and relevance of the victimization data in explaining offenders' behaviors may render those studies may represent significant drawbacks. To overcome the limitations, it is important to use actual offender data to generate meaningful analyses of romance fraudsters' behaviors. Consequently, this dissertation aims to use experimental data similar to that applied in my previous work (Wang et al., 2021), combined with existing criminological and communication theories, to promote a better understanding of romance fraudsters' behaviors in the online world.

This dissertation begins with a scoping review of the current online romance scam literature, intending to use a scientific strategy to address the existing scholarly gap in this field of research. Derived from rational choice theory, the criminal events perspective, interpersonal deception theory, and neutralization theory, the second and third paper uses an experimental approach to assess the influence of rewards on romance fraudsters' behaviors. The three papers' results demonstrate the rationality of online romance fraudsters when facing rewards. Moreover, such rationality can be explicitly seen from their uses of different linguistic cues. Finally, the outcomes provided in the current project also provide policymakers the information about the rationality and modus operandi of fraudsters which can be used to identify the behavioral patterns at an early phase to prevent significant harm to the victim.

ESSAYS ON THE RATIONALITY OF ONLINE ROMANCE SCAMMERS

BY

FANGZHOU WANG

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
2023

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. David Maimon

Committee: Dr. Volkan Topalli
Dr. Eric Sevigny
Dr. Timothy Dickinson

Electronic Version Approved:

Ann-Margaret Esnard, Interim Dean
Andrew Young School of Policy Studies
Georgia State University
May 2023

Acknowledgements

This dissertation would not have been possible without the financial support of the Georgia State University Department of Criminal Justice, Andrew Young School of Policy Study Provost's Dissertation Fellowship. I am especially indebted to Dr. David Maimon, Dr Volkan Topalli, Dr. Eric Sevigny, Professors at Georgia State University Department of Criminal Justice, and Dr. Timothy Dickinson, Assistant Professor at Department of Criminology & Criminal Justice at University of Alabama, who have been tirelessly and supportive of my career goals and who worked actively to provide me with the protected academic time to pursue those goals.

Specifically, I sincerely thank Dr. David Maimon for serving as my mentor and dissertation chair. He is a brilliant scholar who I have learned so much. His works in cybercrime and his class in exploring cybersecurity and online fraud set me on a great path to career in the research and investigation of fraudsters' behaviors in virtual space, a critically important but existed gaps in cybercrime, with a great potential towards improvement. I cannot thank him enough for not only his consistent financial supports but his guidance throughout this dissertation process and other projects we worked on together.

I also want to acknowledge the support of Dr. Eric Sevigny who facilitated the data collection and development of chapter 2 of this dissertation. Dr. Sevigny is extremely essential for this chapter in the way that teaches me how to use scoping review methodology to conduct a scientific rigorous review of current literature in online romance scam. He has been taking time to supervise and take care of every step I make to compose this chapter. Dr. Sevigny has been an excellent mentor and has made me a much stronger qualitative researcher.

Additionally, I appreciate Dr. Topalli for teaching me how to conduct appropriate qualitative analysis throughout my time at Georgia State University, and offering excellent advices on improving my dissertation at the defense stage. He is a skilled and intelligent scholar in qualitative analysis who I also have learned so much through doing different projects with him. I appreciate from the bottom of my heart on what he has been helping so far to my academic writing and career. Dr. Topalli's positive nature and encouragement for myself were inspiring.

My dissertation cannot reach current level of success without the consistent academic supports from Dr. Timothy Dickinson. Although Dr. Dickinson is an outside faculty member, however he treats me like his graduate student and has been tirelessly helping me in constructing chapter 3 and chapter 4. Dr. Dickinson was central to supervising the constructions of main domains in the paper and the write-up process. Besides the dissertation, he has been a great mentor in collaborating with me on various projects which have all gained certain level of success. I would like to say he is a great mentor and a collaborator. I am very excited to see what other great works we can achieve together in the future.

Finally, I am also grateful to myself who do not give up during the hardest time of the doctoral study. Without my persistent and determination, all those achievements cannot be obtained. Lastly, I would be remiss in not mentioning my family, especially my parents. Their belief in me has kept my spirits and motivation high during this process.

Table of Contents

List of Tables

List of Figures

Chapter I: Introduction

Abstract

An online romance scams is a newly evolved serious cybercrime, causing billions of dollars in losses to individuals. Understanding the behavioral patterns of the individuals perpetrating the online romance scams behavior should be the first step in developing evidence-based policies and strategies to protect Internet users. Acknowledging the preliminary background information on online romance scams is vital to unravel offenders' behaviors. Therefore, chapter 1 will introduce the definition, complexity, seriousness, and significance of online romance scams. Subsequently, this section will briefly overview the main components in the following three papers, including the theoretical frameworks, research questions, and methodology. The introduction will end with a summary of the general structure of this dissertation and a reference list.

Introduction

Cyberattacks have grown in number, sophistication, and impact—in 2021, the global cost of cybercrime exceeded $6 trillion (France-Presse, 2022). Specifically, following a recent survey report by Experian (2022), more than half the surveyed consumers expressed that they are concerned about online transactions, and 40% say that concern has increased over the past year. In addition, 58% of consumers have been a victim of online fraud. The Federal Trade Commission additionally revealed that consumer losses related to online fraud increased by 70% in 2021 to more than $5.8 billion, and the tactics employed by fraudsters continue to evolve (FTC, 2022).

In the United States, as reported by Internet Crime Complaint Center (2022), business email compromise, online investment, and confidence fraud/romance made up the first three

types of online fraud that cost the most victim loss in 2021. Among them, IC3 (2022) accounts for online romance scams as the third highest losses of cybercrime reported by victims. This type of crime engages the fraud tactics involving the most human psychology among other types of online fraud. In 2021 alone, the agency received 24,299 victim complaints due to online romance scams, with losses totaling more than $956 million. Specifically, this report demonstrated the complexity of this type of scam as it can involve investment (i.e., cryptocurrency), sextortion, and blackmail (IC3, 2022). As a result, the prevalence for this type of crime is likely to be underestimated, as there could potentially be more victims with even higher amounts of monitory losses (e.g., Potter, 2022). As such, independent of the metric or report used, it is evident that more individuals are falling victim to online fraud in general, and online romance scams in particular (Maimon & Louderback, 2019).

In brief, online romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim (FBI, n.d.). Online romance scams are a newly evolved cyber-enabled form of crime that appeared roughly around 2014 and became rampant in the United States and around the globe starting around 2016 (Whitty, 2013a). During the fraud process, romance scammers either ask victims to send money directly to their bank accounts or persuade them to make advance payments in exchange for other emotional or financial benefits. Whitty (2013a) investigated the anatomy of fraudsters' operations and found that romance fraudsters generally maneuver their operations through five main stages, including the profile, the grooming, the sting, sexual abuse, and the revelation stage. In some cases, romance scammers have even involved victims in money laundering schemes by convincing them to transfer funds or goods without acknowledging the whole situation. In non-English

speaking countries, online romance scams deployed by offenders have a unique name due to a different cultural context and the deployment of a different swindling technique. This type of scam is named *Sha Zhu Pan* （杀猪盘） in Chinese or *Pig-Butchering* scam in English. It originates in Asian countries, specifically China, then extends its scamming territory to other foreign countries. In general, *Sha Zhu Pan* is defined as "a form of online fraud, in which scammers gain the trust of the victim through making friends and dating online. Through gaining victims' trust, scammers then wait for the opportunity to pull victims into scams such as gambling or financial management to defraud their money. The main feature of the *Sha Zhu Pan* scam is to cast a long-term plan for a major return. This process is like fattening the pig and then slaughtering it" (China News, 2019).

Despite different cultural contexts, online romance scams, in general, devastate the lives of millions of victims globally (Cross, 2018). A victim who reported her experience to *Stop-scammers.com*, a private online romance scams reporting platform, described that "I didn't know what a hideous and vile worldwide scam this has become, and how many unfortunate, and trusting, people have fallen victim to their traps" (*Stop-Scammers.com*, 2022 victim report). Such a quote exactly describes the aftermath of the victims' emotions. By exploiting victims online and denoting the emotional component, offenders aim to ask victims to "fund" their financial needs (Cross, 2020).

Most online romance scams incidents happen online. Fraudsters are observed to follow a five-stage operation to swindle their victims (Whitty, 2013a), involving the use of attractive but fraudulent profiles to engage in romantic conversation with the victim until they are ready to part with the money. In rare circumstances, some romance scammers choose victims on the internet and pursue their victims in the physical world. For example, John Meehan (dubbed "Dirty John"

in the media) was a well-known romance scammers. He misrepresented various aspects of his identity and developed a physical relationship with the victim to facilitate his access to various aspects of her personal and financial life, which later manifested in the form of physical threats and abuse (Dibdin, 2019). Similar experiences are described in Cross and colleagues' (2016a) study, where two romance scams victims constantly received physical threats from fraudsters even after moving to new locations. In some extreme cases, fraudsters would even come to victims' houses to collect their requested money face-to-face (Nothling, 2019) or even kill the victim after they meet up (ABC, 2014).

Regardless of the magnitude and seriousness of this type of scam, there are limited practical and consistent initiatives from the government and private sectors to combat online romance scams (e.g., Whitty and Buchanan, 2016; Cross et al., 2018). In addition, insufficient scholarly papers are able to collect first-hand datasets and use advanced methodologies to present a better understanding on this type of cybercrime, particularly the modus operandi of online romance scammers. While an emerging body of work addresses the romance scams, there are still significant gaps left to explore. As a result, this dissertation aims to demonstrate the current state of scholarships on studying romance scams, and explore the rationality of romance scammers' behaviors through deploying an experimental approach. In doing this, this work presents what we do not know about romance scams and the need for future scholarships in this area.

Definition of Online Romance Scams

Numerous definitions are offered to determine what constitutes fraud. Webster's Ninth New Collegiate Dictionary defines *fraud* as an "intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right" or as "an act of deceiving or

misrepresenting" (1990). Later, common law states that there are four main components in the definitions for “fraud”: (1) a materially false statement, (2) knowledge that the statement was false when it was uttered, (3) reliance on that false statement by the victim, (4) damages resulting from the victim's reliance on the false statement (Medallion, Inc. v. Clorox Co. (1996) 44 Cal. App.4th 1807, 1816). In legal terms, as described by Smith and colleagues, fraud is "a generic category of criminal conduct that involves the use of dishonest or deceitful means in order to obtain some unjust advantage or gain over another" (Smith et al., 2001, p.195).

As the presentation of fraud diversified, academics, professional investigators, and accountants have added more elements to the definition of fraud. Specifically, with the maturation of the internet, criminals started to displace their activities from the physical world to cyberspace to avoid detection and surveillance, causing more harm to victims. As a result, the U.S. Computer Fraud and Abuse Act (18 U.S.C. 1030) offers a clear definition of "computer fraud" as:

(a) Whoever… (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5000 in any 1-year period…

Further, criminologists, such as Cross and colleagues (2014), have developed a new scholarly definition for online fraud: "the experience of an individual who has responded through the use of the Internet to a dishonest invitation, request, notification or offer by providing personal information or money which has led to the suffering of a financial or non-financial loss of some kind." Considering these varied fraud definitions, Smith and colleagues (2010) stated

that these proposed definitions are based on the central concept suggesting that "the criminal activities based on deception and/or dishonesty alongside the achievement of some kind of financial gain." Rather than deciding a fixed terminology for fraud, Smith and colleagues (2010) further pointed out that distinguishing between its legal (narrower definition) and theoretical concept (broader definition) also matters (Smith et al., 2010).

The Complexity of Online Romance Scams

In online romance scams, offenders employ a variety of social engineering[1] techniques to deceive victims. The modern conceptualization of social engineering is related to technologically facilitated psychological techniques designed to influence or control the behaviors of other people. Although the term is value-neutral, it is most often referenced as a technique of deception and coercion. As the term "social engineering" first appeared in the early hacker magazine *2600*, it continued to evolve and generalized its core principles from human psychology and behavioral susceptibility (Cialdini, 2001; Hatfield, 2017). For example, fraudsters in advance fee fraud would use social engineering techniques to persuade victims to pay money to someone in anticipation of receiving something of more excellent value—such as a loan, contract, investment, or gift—and then receive little or nothing in return (FBI, n.d.).

Similarly, con artists in online romance scams would also use all kinds of triggers or influences, such as urging victims to make decisions in a short period in exchange for the

[1] The term "social engineer" first came into use in an 1842 book, entitled An Efficient Remedy for the Distress of Nations written by the British economist John Gray. Similar to mechanical engineers, social engineers knew how to fix social ills, however only with intelligence and expert knowledge of human behavior in society (Gray, 1842). From its coinage in 1842 to the 1960s, the term "social engineering" was used in not only political and social planning but also beyond its scope to historical analysis (Harper, 1939), cultural policy (Conkin, 1960), family counseling (Goode, 1950), technology (Weinberg, 1966), and more.

promised reward or using authoritative figures to enforce psychological stress on victims. However, an important antecedent of deploying these swindling strategies is by initially establishing a romantic and trusted relationship. To do so, fraudsters will send romantic letters and enjoyable poems to victims every day and give them all kinds of promises after their meetups, such as buying a big house or traveling around the world. The rationale of such manipulative behaviors can be explained by the Mood-Congruent Judgment theory (e.g., Berkowitz, 2000). Accordingly, human judgment is impacted largely by the mood when the judgment is taken (Mayer et al., 1992). In other word, the mood-congruent judgment effect refers to the fact that when a mood and an idea are similar in pleasantness, the idea will generally seem better in some way. For example, when people are happy, they will judge pleasant concepts as richer in their associations, pleasant attributes as more applicable, and pleasant examples of categories as more typical (Mayer and Hanson, 1995). In online romance scams, Whitty (2013) presented the fact that positive mood can lead to judgment errors, and such errors in decision making can be a major catalyst of successful persuasion from scammers (pp. 666-667). Thus, such an observation is consistent with Mood-Congruent Theory and explains why nearly all scammers attempt to establish a romantic and trusted relationship with victims in their initial encounters.

A number of consistent themes are prevalent and can be incorporated into specified models. For example, to better understand the *modus operandi* of romance scammers' operations, Whitty (2015) proposed a five-stages anatomy of the romance scams. The first stage involves baiting victims: fraudsters may use bogus profile pictures to obscure their identity (e.g., with low-quality graphics) or present a more amenable persona (e.g., the use of physically attractive faces). Scammers can use photos that range from low quality to high-quality shots – multiple

shots of the same model are often used. This approach can strengthen the credibility of the fraudulent personas by providing a limitless supply of photographic evidence upon victims' request (Ghana-pedia.org, 2009). In the second stage, fraudsters will groom victims to increase the intimacy of the relationship. Scammers will establish a strong bond with their victims through frequent online communications during this process. By generating confidence, romance, and trust between with victims, scammers set the stage for later financial exploitation. Specifically, O'key (2008) reported that this stage could last from six to eight months until a requisite amount of trust is established (as cited in Rege, 2009). The third stage is the sting, wherein fraudsters execute their plan to get money from their victims, typically by sharing a crisis story (e.g., bankruptcy, death of a parent, unable to purchase flight tickets to meetup). Rege (2009) noticed that these tragic circumstances are often conducted in succession; that is to say, offenders typically make up more crises to gain financial assistance from victims as circumstances intensify. The fourth stage is sexual abuse, which may or may not factor into the execution of financial fraud. Here, fraudsters may manipulate victims into performing sexual acts online (i.e., in front of webcams) for sexual gratification or as the basis for extortion. The final stage is the revelation, where victims discover they have been defrauded and decide how to respond.

Whitty's (2015) model demonstrates the time-intensive complexity and interactive nature of romance scams (see also, (Cross, 2020). The model also demonstrates the disparity between perpetrators and victims regarding deceptive practices and experiences. Offenders may have executed scores of such offenses and bring with them a wealth of offending knowledge they can bring to bear in manipulating and deceiving victims for whom the offending situation is novel (Cross, 2020). This asymmetric relationship between scammers and victims is a staple of other

deception-based online scams and schemes and is intensified in efficacy by built-in advantages of the internet and online communication platforms (see Topalli and Nikolovska, 2020). These offenses demonstrate powerful, lasting effects on the emotional and cognitive processing of the victims' lived experiences. In some cases, victims have difficulty accepting the objective details and outcomes of these events and may deny or reevaluate their victimization, even after the revelation of fraud.

In addition to the use of social engineering techniques, the complexity of online romance scams can also be demonstrated from its complicated supply chain. Notably, as Lemieux (2003) identified, a large-scale scamming network also exists, with a more precise division of labor. At the core of a criminal network is *an organizer,* who determines the nature and scope of activities. The *extender* is responsible for extending the scam operation by recruiting more individuals and achieving collaborations. The *executor/enforcers,* who fulfill the third role in the syndicate, are responsible for communicating with victims by composing and sending them love letters/emails. *Money movers* collect money from victims and return it to the syndicates. Typically, a money mule will move money from one bank to another.

One example of an organizer ORF syndicate, namely "*Sha Zhu Pan*," exists and continues to evolve in China. Up to date, it has posed substantial harm to victims and government interests. This syndicate is famous for its strict business-like operation and romantic schemes to lure victims into investing in fraudulent apps. A few main heads form the *Sha Zhu Pan* syndicate through recruiting individuals, especially those young individuals without a stable job but want quick money. Recruited individuals are assigned into four main groups: the "host," "resources," "IT/Telecom," and "money-laundering." The host is the most critical group responsible for communicating daily with victims. The rest of the groups offer varied resources

to the host group, such as creating fake investment apps/websites and offering customer service, offering victims' personal information, and exploring the channels that can be used to secretly launder their profits (The 315 Consumer Association, 2020).

The Seriousness of the Online Romance Scams

To date, romance fraud has involved millions of victims worldwide, many of whom were targeted because they were seeking companionship or social interaction through online services. In the United Kingdom, the amount lost to romance scams, which involves a criminal befriending the victim on an online dating site before asking for money, soared by 73% during 2021. In total, victims of such scams lost £30.9m (approximately $36,898,926) and case numbers were up 41% at 3,270 in 2022 (Clark, 2022). In the United States, the Federal Trade Commission (2021) reported losses via romance scams reached a record $304 million, up about 50% from 2019. For an individual, that meant an average dollar loss of $2,500. From 2016 to 2020, reported total dollar losses increased more than fourfold, and the number of reports nearly tripled. The recent cybercrime report published by the Federal Bureau of Investigation (2022) additionally conveyed that financial losses accruing to online romance fraud in 2021 have skyrocketed in recent years to approximately $956 million, ranking third among other cybercrimes and more than any other fraud category (e.g., advance fee fraud and identity theft). In 2021, the Canadian Anti-Fraud Centre received 1,928 reports of romance scams totaling $64,604,718 in losses, compared to 1,546 reports and $28,989,750 in losses in 2020 (Canadian Anti-Fraud Centre, 2022). Importantly, these statistics are representative of a small fraction of total cases, keeping in mind that many victims refrain from reporting their victimizations due to embarrassment or fear of self-incrimination. Moreover, these statistics are gleaned from western governments, which have dedicated resources to monitor, measure, and prevent romance scams.

There is little doubt that hundreds of thousands, perhaps millions, of other victims are unrepresented in these kinds of statistics because of the resources and cultural proscriptions regarding such offenses in their home countries (Wang and Topalli, 2022).

Victimization from online romance scams is reported in non-western countries as well. For example, online romance scams were first reported to Chinese law enforcement as early as the 2010s, and its incidents have reached a surprisingly high frequency in mainland China in 2022. As reported by the Anti-Fraud center in Hangzhou, China, there were more than 1,200 *Sha Zhu Pan* cases involving 230 million CNY ($33,067,836). The average amount involved in a particular case was close to 200,000 CNY ($28,752) in the first half of 2020 alone. Expanding the scope to the nation, only from January to August 2021, the national capital loss caused by *Sha Zhu Pan* had reached 3.88 billion CNY, accounting for 21.3% of the total loss of the national online fraud cases. Among them, the average loss was 181,000 CNY, which was 4.8 times the average loss of other cases (Sina Tech, 2021). While this scam was initially focused on victims speaking Chinese, the recent documentation indicated its expansion globally, and fraudsters were observed using both Chinese and English to target different ethnic groups (Zuo, 2021).

In addition to financial harm, online romance scams victims around the world also experience substantial psychological trauma (Buchanan & Whitty, 2014; Whitty, 2018). They may undergo distress upon learning that they are deceived, leading victims to blame themselves constantly (Cross, 2020, p. 10). Many victims reported the emotional burden as more challenging than the loss of funds (FX110, 2021). For example, Whitty and Buchanan (2016) found that most victims narrate their experience with fraudsters as traumatic, as these victims perceived the loss

of the relationship more upsetting than the financial loss. In addition to the distressed event, victims sometimes are blamed for "facilitating" the scam incident.

Specifically, romance scams victims are subsequently believed to be actively involved in the fraud discourse and are responsible for the consequence (Cross et.al, 2016). Such a statement can be reasoned from the perspective of the "ideal victim." This concept was first proposed by Christie (1986). Ideal victim refers to "a person or category of individual who – when hit by crime – most readily given the complete and legitimate status of victims". For example, an old lady who is robbed on the street on her way to the shopping center. In this case, she should never be held responsible for what happened to her because she acts as a complete passive role when crime occurs. Fraud victims, however, are not typically considered as "ideal victim" but rather a "culprit" because majority of them voluntarily send money or personal details to offenders, however under false persuasion (e.g., Christie, 1986 and Fox & Cook, 2011). In money laundering, fraudsters engage victims into transferring illegal money or goods with the purpose of holding victims responsible for partial legal culpability. In this way, victims may reduce their likelihood of reporting their fraud experience to law enforcement, or even their families/friends, as they are afraid of being betrayed, revenged and prosecuted (Cross et.al, 2016).

In sum, victims of romance scams can experience immense pressure resulting from being blamed for their "active participation" in the scam. Such pressure, coupled with their emotional and financial losses from the scam, can exacerbate the fraud impact. This can manifest from victims' reluctance to report incidents to police because they may think police will blame them for "facilitating" the scam. Moreover, victims may refuse to disclose their fraud experiences to their families or friends in consideration of the anticipated blame, embarrassment, and even the isolation from their loved ones (Cross, 2015). Without getting enough assistance, victims are

unlikely to have a fast recovery and return to a normal life. Additionally, victims' inclination of not raising attention from law enforcement can potentially result in their revictimization (Whitty, 2018).

The Significance of Studying Online Romance Scams

Acknowledging the substantial harm brought by online romance scams requires attention from law enforcement and businesses (e.g., banking and online dating applications). Despite its seriousness, current initiatives in curtailing online romance scams center mainly on raising public awareness. Few online romance scam cases or transactions are prevented or stopped. For those cases that are brought to trial, they are often sentenced under organized crime or white-collar crime statutes. With considerable attention drawn to the financial aspects of online romance scams, little weight is given in sentencing to the psychological and emotional damages to victims (Cross & Blackshaw, 2014). Notably, the negativity directed toward romance scams victims (i.e., victim-blame attitude) can add additional impediments to timely responses from police and victims' services. Specifically, the inability of law enforcement agencies to respond promptly to victims' romance scams cases can result in additional trauma, anger, and frustration among victims in the aftermath of the scam (Cross, 2018). As a result, victims may refrain from reporting or collaborating with agencies (Cross, Richards, and Smith, 2016).

Fortunately, the business/financial sector made progress in taking a few steps to prevent online romance scams, such as forming an Online Dating Association (ODA), creating a "Safety Center" for victims on dating apps, and uniting bank branches to refund money to scam victims. However, due to insufficient resources (e.g., human resources and financial support), those measures currently cannot be fulfilled in whole. Other third-party organizations actively utilize online platforms to provide data fraud detection tools. ScamAlytics provides machine learning,

real-time detection, and shared blocked lists to detect suspicious activities and personnel (2018). Moreover, scam research websites like *stop-scammers.com* and *scamdigger.com* are based on victims' reports. They organize the reports to provide free or upgraded services for victims to search for potential fraudulent photos, names, letters, and even documents. Regardless, the anonymous and transnational nature of the romance scams require additional heightened attention from society (specifically law enforcement and businesses). This can be done by deepening the understanding of offenders' modus operandi and initiating focused anti-scam strategies that are pertinent to offenders' specific behaviors/techniques.

Likewise, there needs to be more academic attention paid to the particularities of online romance scams. In China, most information on the general operation and structure of online romance scams/*Sha Zhu Pan* can only be obtained from government reports or posts from social media platforms or news outlets (e.g., WeChat Blogs, Sina News). Only a small body of research is written by Chinese scholars focusing on describing the general characteristics or legal issues of *Sha Zhu Pan* (e.g., He, 2018; Lyu, 2018; Shi, 2018; Wang, 2009; Wang, 2020; Yuan, 2020; Zhang & Wu, 2020). A few attempts have been made to understand the scam from the criminological perspective using a qualitative approach (e.g., Wu & Jian, 2014; Ye & Duan, 2020). However, scholars need to use empirical datasets and a rigorous methodology to explore critical issues pertaining to online romance scams offending and victimization patterns. Further, scholars in non-Chinese contexts tend to use interviews, surveys, or secondary data for research focusing almost exclusively on victimization and scam operations (or both) (e.g., Whitty, 2015; Rege, 2009; Cross and Holt, 2021; Whitty, 2013; Carter, 2021; Wang and Topalli, 2022).

Still, there is insufficient research using unique first-hand datasets to dive deeper into fraudsters' behaviors and their rationality during the commission of the crime by deploying

criminological theories. It should be acknowledged that such a research methodology is useful for answering a wide range of questions that could not be answered using survey research designs that focus on romance fraudsters. For example, studies seeking to understand the rationality of romance fraudsters by presenting risk and reward cues, or studies seeking to understand the actual linguistic characteristics when fraudsters chat with victims. To overcome the addressed limitations, and answer necessary research questions, additional online romance scams research should be conducted using an evidence-based approach to thoroughly examine online scammers' rationality in their interactions with victims during the progression of the scam.

A Brief Review of Theoretical Perspectives

To guide this research, I draw on four theoretical frameworks: rational choice theory (Clarke and Cornish, 1985), criminal event perspective (Meier, Kennedy, and Sacco 2001), interpersonal deception theory (Buller and Burgoon, 1996), and neutralization theory (Sykes and Matz, 1957). Rational choice theory states that offenders are rational actors who base their crime-related decisions on assessments of risk and reward (Clarke and Cornish 1985). As perceived risks increase, they are less likely to pursue contemplated crimes (e.g., Nagin 1998; Paternoster 1987); as perceived rewards inflate, they are more likely to undertake them (e.g., Baumer and Guastafson, 2007; Goldstein 1985; Cressey 1953; Loughran et al. 2016).

Derived from RCT, the second paper speculates that similar to robbers and drug dealers, romance scammers operating in cyberspace are rational decision makers who exhibit similar risk-avoidance and reward-maximization strategies (Jacques et al., 2014; Wright and Decker, 2004). In support of RCT, the second paper explores whether fraudsters modify their behavior with a fluctuation in reward. Similarly, the core concepts of RCT are used in the third paper to

support the deployment of neutralization theory, aiming to examine whether fraudsters employ a series of accounts and neutralization techniques to justify their need for money.

Originating from the symbolic interactionist perspective (Goffman, 1955), the purpose of the criminal event perspective is to explain the microsocial level of illegal behaviors, specifically emphasizing the way offenders and victims present themselves and interact, and the context of interest (i.e., environment) that may potentially shape the interactions between actors (Meier, Kennedy, and Sacco, 2001; see also, Wang and Topalli, 2022). When situated in cyberspace, CEP stresses on the convergence between offenders (senders), victims (receivers), and the channels in which crime happens (e.g., online platforms or cyberspace). Specifically, when attempting to understand the detailed interactions between offenders and victims, as well as the progression of the criminal event, interpersonal deception theory helps explain the fraudulent communication happening in cyberspace (Maimon et al., 2019). However, as pointed out by Maimon and colleagues (2019), the CEP itself is not sufficient for developing clear research hypotheses regarding the interaction between offenders and victims, and the progression of criminal event. To fill this theoretical lacuna, interpersonal deception theory proposed by Buller and Burgoon in 1996 can be used to further understand the interaction between fraudsters and targets during a criminal event.

Interpersonal deception theory (IDT) holds that deceivers exhibit strategic behaviors when attempting to swindle their targets (Buller and Burgoon, 1996). Depending on receivers' responses, deceivers modify their behaviors accordingly to further their deception, for example changing the emotions and number of words contained in the conversation (see also Buller & Burgoon, 1996; Maimon et al., 2020). Such strategic behaviors are goal-oriented in nature and aim to achieve multiple functions (Buller & Burgoon, 1996). Such recursive and iterative

patterns of communication/behaviors established between two participants can be used to inductively generate micro level research hypotheses examining behavioral changes during interactions between fraudsters and victims (Buller and Burgoon, 1996). Based on this theoretical construct, IDT will be used in the second paper to support the specifications of the expected type of responses/changes that fraudsters will deploy during the live interactions, suggesting that deceivers (fraudsters) will change their course of behaviors with the development of trust or, conversely, suspicion. In particular, IDT supports the empirical explorations concerning whether those changed behaviors/responses fluctuate as the reward fluctuates simultaneously, and if such fluctuation is consistent with the level of reward offered by the "victim."

Neutralization theory are used as a main theoretical framework in the third paper. This theory is originally used to explain a paradox for why juvenile delinquents violate norms that they believe in, while experiencing seemingly little guilt after the offense (Sykes & Matz, 1957). Sykes and Matz (1957) identified five techniques at work when offenders attempt to rationalize their illegal behaviors. The first technique is the *denial of responsibility*. This is a technique offenders use when they claim that outside forces beyond their control cause deviant acts. A second technique, *denial of injury*, views the illegal behaviors as not causing any significant harm despite being against the law. *Denial of the victim* is the third technique. The offenders accept responsibility for the deviant actions but insist that the injury is not wrong but rather a form of proper retaliation or punishment. The fourth technique, *the condemnation of the condemned*, attempts to shift the focus of attention from his deviant behavior to the motives and behaviors of those who disapprove of the violations. Finally, violators would *appeal to higher loyalties* to prioritize the needs of family and friends over abiding by the law. Following Sykes

and Matza (1957), a few other scholars introduced six additional neutralization techniques. They are the *metaphor of the ledger* (Klockars, 1974), *defense of necessity* (Minor, 1981), the *denial of the necessity of the law* (Coleman, 1994), *the claim of entitlement* (Coleman, 1994), and *the justification by comparison* (Cromwell and Thurman, 2003)

Sykes and Matza (1957) argued that neutralizations do not necessarily motivate individuals to commit crimes. However, they facilitate the offending process by "lessening the effectiveness of internal and external social controls," (see also Dickinson and Jacques, 2009). Matza (1964) describes this process as "drift," in which offenders vacillate between criminal and non-criminal activities (see also Jacobs and Copes, 2015). The use of linguistic devices (i.e., neutralization techniques) permitted such drift and offered self-rationalization for offenders/delinquents to neutralize the guilt (Matza, 1964).

Over the past decade, techniques of neutralization have been found to be associated with a wide variety of drug, property, and violent offenses (Maruna & Copes, 2005). Despite its variation, Sykes and Matza (1957) identified that neutralizations are crime-specific, implying that offenders could deploy contrasted neutralization techniques in different situations and contexts. In light of this, interrogators adopt the Reid Technique of Interviewing and Interrogation, largely informed by the common neutralization techniques used by specific suspects to elicit confessions from offenders (Copes et al., 2007). In cybercrime, criminologists have only recently started to explore offenders' use of neutralization techniques. In the study of digital piracy, previous research has concluded that several neutralization techniques were correlated with individuals' propensity to engage in online deviant behaviors (Higgins et al., 2008; Moore & McMullan, 2009; Morris & Higgins, 2009; Marcum et al., 2011). However, majority of these research focuses on offenders' use of neutralizations after the criminal

behaviors. Thus, questions remain if neutralizations can be used during the commission of crime as the major approach to obtain their illegal aims. As a result, this serves as the main focus of the third paper.

Research Goals

My three-paper dissertation aims to contribute to the body of knowledge by addressing two main gaps that currently existed in the online romance scams literature. The first gap is that there needs to be an updated/extended review study by incorporating additional missing studies that are not in the prior ORF scoping review carried out by Coluccia and colleagues (2021). The aim is to provide a comprehensive overview of the current body of literature around the issue of online romance scams. Previous scoping review study carried out by Coluccia and colleagues (2021) outlined general characteristics of ORF offending and victimization, however a few existing limitations concerning the study collection strategy and result presentation have rendered this review from presenting a complete picture of current works of ORF. This current review is a further building and extensions from that prior work, which serves as a well-designed scoping review study that examined research output across multiple languages.

The second gap points at the insufficient research on fraudsters' rational decision-making, particularly when they were communicating with the potential victim. As previously noted, the current body of ORF literature focuses heavily on using either secondary data or interview data to speculate fraudsters' modus operandi or delineate the characteristics of victimizations (i.e., vulnerability factors). Although those approaches have multiple advantages especially when the ORF studies are still at the nascent stage, however the analysis of those datasets may refrain research outcomes from extending to other aspects of online romance scams. One of the major limitations with using secondary data concern with the issue of

objectivity. Although it is feasible to use victim data to infer offenders' operations, however the use of those datasets may exaggerate certain facts and not accurately capture fraudsters authenticate behaviors to carry out certain illegal behaviors. Considering such an aspect, to overcome such a limitation posed by secondary victimization data, scholars, like me, should be encouraged to collect first-hand dataset gathered from the live interaction between offenders and the victim.

Against those backdrops, the first paper of this dissertation aims to fill the main gap by attempting to update and extend the current database containing all the current existing literature around ORF by incorporating additional studies from both Western and non-Western contexts. By using the rigorous criteria ruled by the scoping review, this study will initiate a series of rigorous data coding and analysis processes to generate a comprehensive review on the research outcomes. The main research questions are (1) *what are the current updated online romance scams literature database*, and (2) *how can we categorize based on the results of each identified study?*

The composition of the second paper aims to further understand fraudsters' behavioral changes when facing rewards instead of sanctions (Wang et al., 2021). Through identifying myself as the potential victim, I predesigned probing questions and held distinct communications with identified groups of fraudsters located through a fraudsters-exposure website (*stop-scammers.com*). The experiment followed rigorous and scientific protocols by taking fraudsters' intentions into considerations---the incentives/rewards. Following the series of probing questions and the operationalization of rewards, I collected responses from fraudsters and used a mix-methods approach to generate analysis. By extracting the main concepts per the CEP, RCT, and IDT perspectives, this dataset containing fraudsters' responses is used to answer two main

research questions: (1) *what are the main strategies fraudsters use when attempting to obtain rewards from the victim*, (2) *do fraudsters change the use of those strategies per the variations in the presented likelihood of receiving the reward?*

The third paper, which draws its inspiration from the outcomes of the second paper, aims to further understand fraudsters' use of neutralizations when presenting with reward cues. By using exactly the same research design used in second paper, the third paper used the neutralization theory (Sykes and Matz, 1957) to answer two research questions: (1) *can the use of neutralization technique observe from a group of active online romance scammers,* (2) *what are the purposes of using those neutralizations, (3) can additional neutralizations and accounts or other relevant observations reveal from the conversation?* To answer these questions, the response data I collected will be qualitatively analyzed using thematic analytical approach. Main research and practical implications will be addressed accordingly in chapter 4.

A Brief Note on the Research Methodology

A scoping review methodology is employed in the first paper, aiming to map out the current existed literature in online romance scams, identifying several key concepts, overcoming priori limitations exposed by the first scoping review on ORF (Coluccia et al., 2021) and pointing out the existed gaps in the research. With the support from the initial search of existing studies on this topic, this methodology is selected because the size of relevant studies is small and the majority of researchers employ a qualitative approach. This paper follows the rigorous process proposed by PRISMA Extensions for Scoping Reviews (Tricco et al., 2018). The set-up of the paper is constructed in a six-stage process (see also, Arksey and O'Malley, 2005): (1) identifying the research background, (2) identifying the research questions, (3) identifying

relevant studies, (4) study selection, (5) charting the data, (6) collating, summarizing and reporting the results, (7) discussion of results and potential implications.

The primary methodology used in the second and third paper is experiment. Mainly, the second paper uses a mixed method approach to better utilize the database I collect through the live interaction with fraudsters. The third paper deploys the qualitative approach to explore additional accounts and neutralizations used by romance scammers during the interaction. Notice that this research uses a combination of inductive and deductive approaches to form the research questions and hypotheses. In other word, I firstly use the theory to derive a few preliminary research questions based on the existed theoretical constructs. Additional research questions may be brought up after observing responses from active fraudsters. In this way, I am not simply testing hypotheses derived from the theory but instead evaluating the happening of the whole criminal event.

Importantly, my three papers are related with each other and are in a progressive relationship. First, they are related as the focus of both is online romance scams and both aim to answer different research questions around it. Second, the composition and sequence of these three papers are in a progressive relationship. Specifically, the first paper in this project is a scoping review. And one of the implications drawn from this review can reveal one of the knowledge gaps in online romance scams, namely using the firsthand dataset to generate analysis towards rationality of fraudsters. In order to fill this gap, the second and third papers attempt to overcome the proposed limitation by gathering conversational date using randomized experimental design by holding live chats with fraudsters. Third, paper two and paper three are interrelated as the results generated in paper two provides insights and guidance in formatting paper three. The result of paper two inform on how offenders modify their behaviors as there are

fluctuations of rewards. One of the strategies observed consistently from fraudsters' responses is their use of different justifications on their needs of money. As a result, the idea of paper three is formulated as I suspect that offenders may use different types of neutralizations that currently exist in the framework. In addition, as online romance scams are largely different from the crime happening in the physical world, I expect to observe additional neutralizations or accounts used by ORF offenders. In echo with the prior observation in paper two, paper three lastly aim to explore the ultimate purposes of fraudsters using those neutralization and accounts.

Organization of the Study

This dissertation is divided into five chapters. Chapter 1 presents the introduction, which includes a description of the phenomenon, its significance and purpose of the study (including research aims, research questions and how three papers will be linked together). Chapter 2 demonstrates the presentation of my first paper, a scoping review on the current status of romance scams literature. This chapter includes an introduction, a review of relevant literature, methods, results and conclusion. A reference and an appendix list are incorporated in this chapter. Chapter 3 follows the exact format as chapter 2, and presents the second paper focusing on conducting the first experiment studying how the presentation of reward may affect fraudsters' behaviors. Chapter 4 presents the third paper, which also uses an experimental approach to entice fraudsters' responses and analyze their linguistic characteristics from neutralization perspective. This chapter again follows the same format as chapter 2 and 3. Finally, Chapter 5 presents a discussion and conclusion based on the above findings and provides suggestions for future research and policy practices.

Chapter II: Online Romance Scammers and Victims: A Scoping Review

Abstract

Computer-mediated communication (CMC) provides myriad opportunities for online daters to seek their ideal partners online. However, the anonymous and asynchronous nature of CMC also allows malicious cybercriminals to manipulate their verbal and non-verbal cues to establish fictitious romantic relationships with victims. Through building a solid emotional bond, the ultimate purpose is to extort economic resources from targets. To better understand the current literature on online romance scams, this chapter presents a scoping review of the qualitative and quantitative evidence on this scam, focusing mainly on the offenders' aspects. Through following the rigorous scoping review steps outlined by Tricco and colleagues (2018), thirty-five studies are included and reviewed by both authors. The review outcomes reveal several themes focused on previously by prior studies from both offenders' and victims' perspectives. Implications for future research and practices are discussed.

Introduction

With the rapid development of digital communication technology, individuals have increased their social interactions through online social media and peer-to-peer platforms. Dating apps represent a major segment of this fast-growing industry. According to the Business of Apps, the number of dating app users increased 63%, from 198 million to 323 million, between 2017 and 2020 (Curry, 2022). In North America alone, Wise (2022) reported that approximately 1500 dating sites and chats were created over the last decade. The emergence and growth of the online dating industry has provided fertile ground for a new type of crime: online romance scams (ORF). Compared to other forms of fraud, ORF is relatively new and has a unique emotional component (Cross and Holt, 2021), characterized by “cybercriminals pretending to initiate a

relationship through online dating sites and then defrauding their victims of a large sum of money" (Whitty & Buchanan, 2012). These relationships are sought via email, websites, and apps, including both dating-specific and more general apps (e.g., Facebook, Twitter, Instagram, Google Hangout) (Federal Trade Commission, 2022).

The FBI's Internet Crime Complaint Center (IC3) documented approximately $6.9 billion in internet-enabled theft, fraud, and exploitation losses in 2021 (IC3, 2021). Online confidence/romance scams, which accounts for the third highest losses reported by victims, caused more than $956 million in losses in 2021 based on 24,299 victim reports (FBI, 2020). In the UK, more than £97.2 million was reported stolen in 2021 from nearly 9000 victims of online romance scams (Clark, 2022). Similarly, the Canadian Anti-Fraud Centre registered losses of nearly $64 million due to romance scams in 2021 (Duhatschek, 2022). Importantly, these statistics represent but a small fraction of total cases because many victims refrain from reporting their losses due to embarrassment and self-incrimination. Moreover, these statistics are sourced from western governments that have dedicated resources to monitor, measure, and prevent romance scams. It is therefore likely that hundreds of thousands, perhaps millions, of other victims are unrepresented in these kinds of reports because of limited enforcement resources and cultural proscriptions against online dating in their home countries.

Despite ongoing education and prevention efforts, the number of individuals who fall prey to these scams continues to grow. Existing research suggests that fraudsters follow a common yet effective modus operandi. Initially, they start a conversation with victims through online dating or social networking sites (Whitty, 2013a). Once contact is established, scammers initiate a romantic relationship with victims by using romantic illusions (e.g., love letters or poems). After this stage, fraudsters formulate their financial requests using various techniques,

such as appealing to authority, emphasizing shared interests, and deploying visceral triggers and social proofs (Lea et al., 2009a). To simplify, visceral triggers are deployed when scams exploit basic human desires and needs – such as greed, fear, or desire to be liked. Moreover, fraudsters would also use social proofs when they present fraudulent offers to victims claiming that other people have already benefited or reacted in order to increase perceptions of legitimacy and the probability of a successful swindle (Lea et al., 2009a).

Romance scammers often target middle-aged women through social media platforms. In the United States, for instance, both women and those aged 55 to 65 are reportedly more susceptible to romance scams (e.g., Whitty, 2018). In addition, victims with certain types of personality and psychological traits are more likely to attract fraudsters and increase their vulnerability to the scam. For example, victims who are more likely to score high on romantic beliefs and idealization are more likely to be scammed (Buchanan and Whitty, 2014; Kopp et al., 2016). Whitty (2018) also observed that romance scams victims are typically middle-aged, well-educated women. Moreover, these individuals tended to be more impulsive and trusting of others, while also lacking self-control and restraint.

Academic researchers have been instrumental in bringing greater attention to the problem of online romance scams. They have introduced formal definitions of the problem, highlighted the scale and scope of the phenomenon, documented the anatomy of a scam, identified common psychological traits of offenders and victims, and identified the obstacles and aids to helping online romance scams victims (Buchanan and Whitty, 2014; Whitty and Buchanan, 2012, 2016; Sorell and Whitty, 2019; Whitty, 2013a; Whitty 2018). Still, with the exception of a recent scoping review by Coluccia and colleagues (2020), scant attention has been given to documenting the current state of knowledge regarding ORF.

Coluccia et al.'s (2020) seminal scoping review presents quantitative and qualitative evidence on ORF victimization, focusing on epidemiological characteristics (e.g., sociodemographics), relationship dynamics (e.g., luring strategies, coping mechanisms), and the psychological characteristics of targets, victims, and fraudsters. The review employs a systematic approach to document current knowledge and gaps in understanding ORF. Specifically, the authors included 12 studies in their scoping review, drawing several core conclusions. First, they found that 63% of social media users and 3% of the general population reported having ever been victimized. Second, females and middle-aged individuals experience a relatively higher risk of victimization. Third, certain psychological traits, such as neuroticism, romantic idealization, sensation-seeking, impulsivity, and susceptibility to addiction heighten vulnerability to online romance scams.

Despite its original contribution, Coluccia et al.'s (2020) scoping review was limited in several respects. For example, they only searched three academic databases, which may increase the likelihood of missing relevant studies. Moreover, although their eligibility criteria included studies published in multiple languages (i.e., English, Italian, Spanish, and German), all ultimately selected studies were written in English. Lastly, Coluccia and colleagues (2020) used only online romance scams descriptors connected by the Boolean operator OR and searched them in only three electronic databases: PubMed, Scopus and Google Scholar. As a result, the search strategy they developed could not be comprehensive enough to be able to locate all relevant literature.

This current review extends Coluccia et al.'s study (2020) in several ways. First, we query a much larger number of databases, including grey literature sources, to reduce the

likelihood of missing relevant studies. Second, we used an expanded list of search terms and query the databases using both natural language and controlled vocabulary terms. Third, we incorporate studies written in Chinese in addition to English. In sum, this scoping review aims to update and extend prior work by collecting and summarizing additional available evidence, presenting a comprehensive picture of the current body of literature on ORF. The ultimate purpose is to serve decision-makers and identify opportunities for future knowledge generation.

Methods

This scoping review will collect and summarize the empirical literature on ORF. This review has several key objectives:

- Highlight the characteristics, tactics, and modus operandi of online romance scammers and their criminal schemes.
- Identify the main characteristics of ORF victims and the various risk factors for victimization.
- Summarize the outcomes, context, design, quality, and main findings of included studies; and
- Surface both practice and policy implications of academic research on ORF.

We use PRISMA Extension for Scoping Reviews (Tricco et al., 2018), Moher et al.'s (2009) recommendations for conducting scoping reviews, and Coluccia et al.'s (2020) scoping review to guide our methodology for the current review.

Inclusion and Exclusion Criteria

Studies were included if they a) examined any aspect of ORF, b) employed a social science research method, c) were preprinted or published in a peer-reviewed journal, or available from grey literature sources, d) were written in either Chinese or English, and e) reported either quantitative or qualitative findings. In addition, we applied no geographic or time period restrictions.

The following types of publications were excluded from this review: commentaries, general studies of online fraud that do not focus specifically on romance scams, studies investigating romance scams only in an offline setting, cost-benefit analyses, and papers examining the legal aspects of this crime.

Bibliographic Search Strategy

The initial bibliographic search was conducted from January 8-10, 2022, using the following 7 academic vendors: (1) EBSCO (Academic Search Complete, APA PsycINFO, Criminal Justice Abstracts, HeinOnline), (2) ProQuest (ASSIA, ProQuest Criminal Justice Database, Sociological Abstracts, Social Science Database, Dissertation & Theses A&I, Social Science Database) (3) Elsevier (Embase, ScienceDirect, Scopus), (4) IEEE, (5) JSTOR, (6) PubMed, and (7) Clarivate (Web of Science). The following 5 grey literature databases were also searched: Criminology Open (https://www.criminologyopen.com/), Evidence-based Cybersecurity Group (https://ebcs.gsu.edu/projects/), Google Scholar (https://scholar.google.com/), ScholarWorks (https://scholarworks.gsu.edu/). In addition, academic researchers in China primarily use the search aggregator *Zhi Wang* (https://i.cnki.net/#/) to access bibliographic databases in both China and foreign countries. Thus, *Zhi Wang* was the main search portal used to identify ORF studies written in Chinese.

Table 1. Search Results

Search Source	Number of Items	Duplicates removed before screening	Total
Academic Search Complete	39	13	26
APAPsyinfo	17	1	16
ASSIA	26	8	18
Criminal justice Abstract	20	16	4
Embase	5	0	5
HeinOnline	96	6	90
IEEE	6	0	6
ProQuest Criminal Justice Database	39	13	26
Pub Med	19	3	16
Science Direct	118	1	117
Sociology Abstract	163	6	157
Web of Science	62	11	51
Zhi Wang	82	13	69
Open Society Framework	0	0	0
ScholarWorks	0	0	0
Google Scholar	47	25	22
Social Sciences Research Network	6	0	6
Criminology Open	1	1	0
Dissertation & Theses A & I	4	0	4
Evidence Based Cybersecurity Group	1	1	0
Total	751	118	633

Our search strategy used Boolean logic to find studies with title, abstract, or keyword hits across all three of the following domains: online (e.g., internet, online), romance (e.g., dating, relationship), and fraud (e.g., victim, fraudster). We employed both natural and controlled vocabulary search terms, using wild cards where appropriate to capture word variants. Similar Chinese words were used to search *Zhi Wang*. See Table 2 for our complete English language search strategy. Bibliographic records were downloaded into EndNote X9 for management and review.

Table 2. Search Terms and Boolean Logic

Domain	Natural Vocabulary		Controlled Vocabulary
Online	Internet* OR Computer* OR Mass marketing * OR Fraud* OR Online deception* OR Online identity theft* OR "Catfishing" OR "Security" OR "Identity theft"	OR	"Internet crime" OR "Cybercrime" OR "Crime" OR "International crime" OR "Financial loss" OR "Marketing" OR "Computer security" OR "Internet security" OR "Computer-mediated communication" OR "Social media" OR "Network security" OR "Hyperpersonal internet use"
AND			
Romance	Love* OR Intimacy OR Dating* OR Online* OR Internet* OR Online dating fraud* OR Online romance scams* OR "Advance fee fraud" OR "Relationship"	OR	"Romantic love" OR "Dating services" OR "Dating" OR "Dating (social customs)" OR "Social dating" OR "Romance cybercrime" OR "Human relation" OR "Social network" OR "Personal relationship" OR "Romantic beliefs" OR "Love story"
AND			
3. Fraud	Victim* OR Target* OR Mark* OR Scammer* OR Fraudster* OR Social engineer* OR Deceiver* OR Con artist* OR Swindler* OR "Wine hustler"	OR	"Psychology" OR "Psychological abuse" OR "Coping" OR "Violence" OR "Emotions" OR "Vulnerability" OR "Susceptibility" OR "Impulsiveness" OR "Persuasive communication" OR "Social engineering" OR "Influence" OR "Error of Judgement" OR "Personality" OR "Cognition" OR "Persuasions" OR "Swindling" OR "Decision making" OR "Elaboration" OR "Manipulation" OR "Swindle" OR "Neutralization technique" OR "Rationalization" OR "Psychological capital" OR "Victimization fear"

Study Selection Procedure

We used a two-stage screening process to assess the eligibility of studies retrieved during the bibliographic search. In the initial stage, the first author reviewed the titles and abstracts of the retrieved studies, flagging potentially eligible studies for second-stage screening. During the second stage, the first author reviewed the full text of all of potentially eligible studies, with dual

screening performed by the second author for a random 20% subset of English-language studies. Per protocol, any discrepancies in the inclusion decision were resolved by consensus discussion.

Data Abstraction and Synthesis

Both quantitative and qualitative information from eligible studies was coded by the first author, with quality control provided by the second author. The following information was extracted into an Excel spreadsheet for subsequent analysis: (a) data collection year, (b) publication language, (c) publication type, (d) target country or countries in which the study was performed, (e) study objective, (f) research design, (g) target or reference population, (h) sample size, (i) unit of analysis, and (j) main findings. In addition to extracting structured codes, we thematically analyzed the qualitative content of each included study according to a modified "crime triangle" framework based on routine activity theory. Using this framework, we analyzed study context across three theoretical domains: offender, victim, and crime opportunity. The latter domain was modified to an online setting to focus on organizational structures and the stages of ORF.

The following thematic analysis process was conducted in three stages based on the target population and main finding. Based on the theoretical structure provided by the crime triangle theory (CTT) (Cressey, 1953), the primary author first read all eligible articles and categorized those studies into the three grand domains provided by the CTT. Following this stage, the primary author went over the main finding of each article and identified subcategories under the three domains. During this process, the primary author identified the main finding first and then reviewed the results section of each article to minimize any deviations. Study summaries were composed and written by the first author, which were then reviewed by the second author to obtain mutual agreement on the selected themes and findings. All themes

emerging from these studies were labeled and conceptualized following in-depth discussion and agreement between both authors. Once data analysis was complete, themes were checked again to ensure they were distinct with no duplication.

Results

Study Screening and Selection

The study screening and selections results are presented in the PRISMA graph in Figure 1. The initial literature search yielded 751 studies, of which 118 were duplicate records, leaving 633 potentially eligible studies. During the initial title and abstract review, 512 studies were excluded as ineligible. During the next-stage full-text screening of the remaining 121 potentially eligible studies, 20% (n = 24) were dual screened. We achieved 100% agreement between both screeners, similarly categorizing 15 of the 24 studies as eligible. The remaining studies, including 47 written in Chinese, were single screened by the first author.

Table 3. Summary of Included Studies in the Review (N=35)

Author/s	Year	Location	Method
Rege	2009	United States	Qualitative (content analysis)
Koon and Yoong	2013	Malaysia	Qualitative (case study analysis)
Rege	2013	United States	Qualitative (content analysis)
Whitty	2013a	United Kingdom	Mixed (content analysis and cross-sectional survey)
Whitty	2013b	United Kingdom	Qualitative (Semi-structured interviews)
Buchanan and Whitty	2014	United Kingdom	Survey based quantitative analysis
Garrett	2014	United States	Survey based quantitative analysis
Wu and Jian	2014	United Kingdom	Qualitative (interviews)
Huang et al	2015	United Kingdom	Qualitative
Kopp et al	2015	Australia	Qualitative (case study analysis)
Kopp et al	2016a	Australia	Qualitative (case study analysis)
Kopp et al	2016b	Australia	Qualitative (case study analysis)

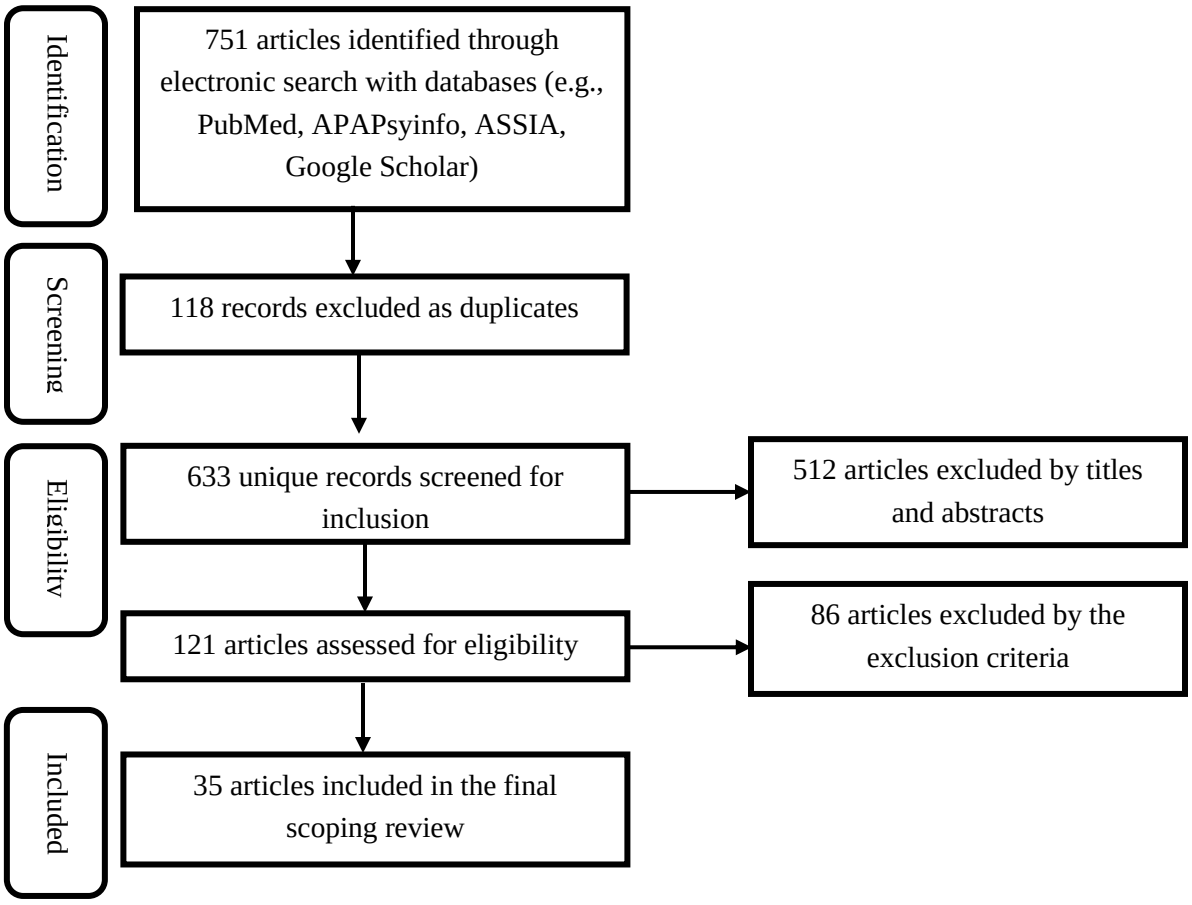
Table 3. Summary of Included Studies in the Review (N=35) (continued)

Whitty and Buchanan	2016	United Kingdom	Qualitative analysis
Archer	2017	United States	Qualitative (content thematic analysis)
Cross, Dragiewicz and Richard	2018	Australia	Qualitative (semi-structured interviews)
Edward et al	2018	United Kingdom	Quantitative
Saad et al	2018	Malaysia	Survey based quantitative analysis
Whitty	2018	United Kingdom	Survey based quantitative analysis
Qiu	2019	China	Qualitative (case study analysis)
Shaari et al	2019	Malaysia	Qualitative
Whitty	2019	United Kingdom	Survey based quantitative analysis
Anesa	2020	Italy	Qualitative (content thematic analysis)
Barnor et al	2020	Ghana	Qualitative (semi-structured interviews)
Dreijers and Rudzisa	2020	Latvia	Qualitative
Offei et al	2020	Ghana	Quantitative (cross-sectional survey)
Ye and Duan	2020	China	Mixed (experiment and case study analysis)
Wang and Pan	2020	China	Qualitative (case study analysis)
Carter	2021	United Kingdom	Qualitative (case-study approach)
Cross and Holt	2021	Australia	Mixed (quantitative analysis and content thematic analysis)
Cross & Layt	2021	Australia	Qualitative analysis
Offei	2021	Ghana	Survey based quantitative analysis
Wang et al	2021	United States	Mixed (experiment and qualitative analysis)
Cross and Lee	2022	Australia	Qualitative analysis (thematic)
Wang and Topalli	2022	United States	Qualitative analysis (thematic analysis)
Wang and Zhou	2022	United States	Qualitative (thematic analysis)

Overall, of the 121 studies flagged for retrieval (See table 3), we could not locate the full text for 5 reports through either library or direct author requests. Of the remaining 116 studies, we included 35 primary studies for online romance scams assessments (see below table 1). The

81 ineligible studies were excluded for the following reasons: scoping review (1), examined issues other than ORF (27), employed non-social science research method (15), no quantitative/qualitative results reported (11), commentaries, news, opinions (14), discussed only legal aspects (12), and discussed only economic aspects (1).

Figure 1. PRISMA Flow Diagram for Identifying Relevant Online Romance Scams



General Characteristics of Included Studies

Table 4 displays the characteristics of studies included in this scoping review. All studies were published between 2009 and 2022, with most (48.6%) published between 2016 and 2020. Almost three-quarters of eligible studies appeared in peer-reviewed journals, followed by conference proceedings and dissertations/theses. Notably, three studies included in this scoping

review were published in Chinese, which primarily use a qualitative approach to characterize online romance scams in China. Concerning the analytic approach, 65.7% of studies used a qualitative method, 22.9% used a quantitative method, and 11.4% used a mixed method approach. Concerning geographic location, most studies were conducted in the United Kingdom (28.6%), with sizable numbers also conducted in the United States (20%) and Australia (20%). Lastly, we included three studies each from Malaysia, Ghana and China, with one study each set in two other countries (Italy, Latvia).

From those statistics, we can observe some intriguing patterns. First, almost all studies are published after 2010, specifically a substantial increase from 2016 to 2020. This statistic is congruent with the increased societal attention on the ORF worldwide. For example, approaching the end of 2019, the Chinese government started to enforce a "tough on telecommunication crime" policy, aiming to increase control over domestic and cross-board cyber-fraud such as online romance scams (Huang and Paez, 2019). In the United Kingdom, Online Dating Association (ODA) was established to create a safer online dating environment for daters and the general public. Moreover, during that same year, seven major banks in the UK joined forces to refund money to ORF victims (Peachey, 2019). Second, most located studies were conducted in English-speaking countries. One of the speculations behind this phenomenon could be the lack of availability and accessibility of relevant datasets in different countries. However, it should be noted that this current review only looked at ORF literature in Chinese and English, thus it could be possible that other studies exist in different languages. Lastly, most studies in this subfield are qualitative, often based on interviews and victim testimonials. Nevertheless, ORF is still a new research field that remains ripe for further quantitative research in the future.

Table 4. General Characteristics of Included Study for Scoping Review (N=35)

Characteristic	Number	Percentage (%)
Publication year		
< 2010	1	2.9%
2010-2015	9	25.7%
2016-2020	17	48.6%
>2020	8	22.9%
Publication Type		
Conference proceeding	7	20.0%
Journal Article	26	74.3%
Thesis dissertation	2	5.7%
Language		
Chinese	3	8.6%
English	32	91.4%
Analytic Approach		
Qualitative	23	65.7%
Quantitative	8	22.9%
Mixed method	4	11.4%
Geography		
Australia	7	20.0%
China	3	8.6%
Ghana	3	8.6%
Italy	1	2.9%
Latvia	1	2.9%
Malaysia	3	8.6%
United Kingdom	10	28.6%
United States	7	20.0%

Thematic Analysis Process

The thematic analysis in this section draws upon the "crime triangle" perspective highlighting three main domains: (1) the modus operandi of ORF, (2) characteristics of offenders, and (3) characteristics of victims.

Stages and Organizational Structure of ORF

Overall, eight studies address aspects of ORF operations and organization. Four papers characterized ORF as occurring in distinct stages or phases (Whitty, 2013a and 2013b; Qiu, 2019; Wang & Zhou, 2022). We also identified another four studies that discuss ORF group

structure (Rege, 2009 & 2013; Qiu, 2019; Wang and Pan, 2020), focusing on the operational characteristics and skills of ORF criminal groups.

Stages of ORF. Table 5 indicates that four studies empirically describe ORF sequencing or stages of action. Whitty (2013a) proposed the first model, consisting of five stages, based on research with UK victims. Stage 1 involves the initial baiting of victims based on a false online dating profile. Stage 2 entails grooming victims with intimate communications. When the timing is right to exploit or "sting" the victim, stage 3 engages the victim with a crisis story. In stage 4, fraudsters manipulate victims into performing sex acts online, supporting extortion. Stage 5, the revelation, occurs when victims discover they have been defrauded and decide how to respond. Whitty's (2013b) follow-up work revised her original model. Stage 1 emphasizes victims' strong motivations to find ideal partners, which increases the targets' vulnerability to scams. Stage 2 involves fraudsters' presentation of the ideal profile, presenting a false narrative and attractive pictures to bait victims. After gaining a favorable first impression, fraudsters initiate stage 3, the grooming stage, which focuses on establishing sufficient trust with victims. Stage 4 is the sting process, in which fraudsters usually deploy two essential techniques to request money from victims: (i) the foot-in-the-door technique that starts with requesting small sums of money and (ii) the presentation of a personal financial crisis. During stage 5, Whitty further described that both financial and non-financial victims would experience the continuation of the scam. In essence, fraudsters deploy the foot-in-the-face technique on those victims who did not comply with the foot-in-door techniques. This new technique involves asking for an extreme favor and then reducing this to more reasonable requests (see also Cialdini, 1984). This process involves the presentation of a new crisis until the victims are ready to part with the money. Stage 6 involves sexual extortion and blackmail. Stage 7 engages in revictimization, where either (i) the

original scammer admits fault but claims to have fallen in love with the victim to continue the scam or (ii) new fraudsters emerge claiming to be law enforcement needing assistance to apprehend the original scammers.

Two more recent papers establish ORF stage models in the Chinese context. Qiu (2019) observes that the operation of ORF in China follows a scripted design in which fraudsters identify themselves as "real people" by fabricating personal backgrounds and stories to enhance their legitimacy. Qiu (2019) identified seven general stages fraudsters usually deploy to bilk their victims. Typically, fraudsters initiate stage 1 by identifying potential victims based on their online profiles. They often used web-crawling techniques to target victims who label themselves as "longing for love" or "seeking a partner/love." Stage 2 happens when fraudsters make initial contact, chatting with targets on dating apps before inviting them to more private messenger apps such as WeChat or QQ. Stage 3 initiates the grooming process, where fraudsters use pre-established scripts and pictures/videos to impress potential victims and establish trust. Once trust and affection are established, fraudsters move to stage 4, mentioning potential mutual investment opportunities. Stage 5, the harvesting stage, involves swindling larger amounts of money. Stage 6 involves laundering the illicit gains. Stage 7 is the revelation followed by a scammer exit or attempt at revictimization.

Following Qiu (2019), Wang and Zhou (2022) further explored the modus operandi of ORF offenders in China by developing a persuasive model using the ‘seven principles of persuasion’ proposed by Gardner (2006). Wang and Zhou (2022) observed that ORF in China followed a process of swindling like those used in Western countries. In brief, there are three main stages of persuasion—the hunting stage, nurturing/grooming stage, and harvesting stage. The authors observed that fraudsters search for ideal victims during the hunting stage. In the

nurturing/grooming stage, fraudsters use visceral factors, precisely resonance and sharing fabricated personal life stories with victims to increase intimacy and trust. In the harvesting stages, fraudsters appeal to visceral factors to convince victims to invest money in legitimate looking but fraudulent schemes. Moreover, they often employed the “redescription” technique in which other fraud group members pose as customer service behind the app/platform to further the charade by seeking payments and investments. Lastly, fraudsters will use real-world events to facilitate the persuasions or exits from the scam.

Stages models of ORF have been developed in Western and non-Western contexts. There are similarities between models developed from UK and Chinese samples. For example, the offenders are skilled at using romantic schemes to manipulate victims psychologically. Moreover, the anatomy of the ORF operation in China is much like the online romance scams in Western countries, involving initial searching, grooming/trust-building, and the sting. Despite these resemblances, ORF in China tends to employ fraudulent investment or gambling schemes rather than direct appeals for cash. Moreover, ORF in China uses more complicated strategies to present themselves as "real" people looking for a relationship or wanting to benefit the victim financially (Qiu, 2019). For example, scammers often instruct victims how to maneuver the fraudulent investment app and ply victims by fronting initial investment capital. Concerning the deployment of the crisis, as inferred from Qiu (2019) and Whitty (2013b), ORF in China would follow investment schemes (either stock, online gambling, or cryptocurrency) to engage victims to invest in the fraudulent app developed by scammers. In contrast, non-Chinese romance scammers mainly choose to fabricate urgent scenarios and ask for money directly from victims – the death of family, car accident, illness; or request them to pay an advanced fee – inheritance, package delivery, and recipient of a certificate.

Table 5. Stages of ORF (N=4)

Author/s	Year	Location	Method	Target Population	Key findings
Whitty	2013a	United Kingdom	Mixed (content analysis and cross-sectional survey)	(1) 200 posts online (2) 20 victims of online romance scams (3) One interview with Organized Crime Agency officer	Five stages of ORF operation identified: (1) ideal profile presentation (2) grooming (3) the sting (4) sexual extortion (5) scam revelation
Whitty	2013b	United Kingdom	Qualitative (Semi-structured interviews)	20 romance scams victims	The persuasive technique model is established: (1) motivated target to find the ideal partner (2) ideal profile presentation (3) grooming (4) the sting (5) scam continuation (6) sexual extortion, (7) revictimization
Qiu	2019	China	Qualitative (case study analysis)	One convicted ORF case	Seven stages of operation were identified for ORF in China (1) filtering potential victim profiles (2) initiate contact and privatize messaging, (3) grooming (4) highlight fraudulent investment opportunities (5) the harvesting (6) money laundering, (7) revelation
Wang and Zhou	2022	United States	Qualitative (thematic analysis)	(1) 40 publicly available victim testimonials in Chinese (2) Four victims' report obtained from Chinese law enforcement	A persuasive technique model is established for ORF in China: (1) hunting stage (2) nurturing/grooming stage (3) harvesting stage

Organizational Structure of ORF. Table 6 provides information on the four studies that explored the organizational structure of ORF. Two studies were conducted in the United States

(Rege, 2009, 2013) and two in China (Qiu, 2019; Wang and Pan, 2020). Rege (2013) mentioned that the operation of online romance scams requires scammers to be competent social engineers instead of advanced computer hackers. Equipped with their "scam culture," Rege (2009) noted that large criminal syndicates do not predominate; many ORF scams were committed by individuals working alone or in small groups. Two main similarities can be observed among small and large-scale criminal groups. First, fraudsters working in small or large-scale criminal networks would treat the scamming businesses like a job requiring them to work at least six-hour shifts (Rege, 2009). Second, Rege (2009) found that those individuals working in a cohort, despite the size of the group, do not have a networked structure. In other words, fraudsters have no head authority, operating instead in a loosely organized way (Rege, 2009). Moreover, the networked structure of these criminal groups would enable fraudsters to shield other group components from law enforcement surveillance (Rege, 2009). Despite the similarities, several differences prevail. Compared to large criminal groups, small-scale groups are less hierarchical and therefore operate with greater ease and speed. Such a mode of operation paves the way for a rather loosely structured network that is "transitory and goal-specific in nature" (Rege, 2009). In most cases, small-scale groups are less likely to be detected by law enforcement as they coalesce to commit certain crimes and disband upon task completion (Rege, 2009).

Table 6. Organizational Structure of ORF (N=4)

Author/s	Year	Location	Method	Target Population	Key findings
Rege	2009	United States	Qualitative (content analysis)	170 online documents relevant to online romance scams	(1) Offenders have a clear roles assignment for both individual, small group, and large-scale criminal networks (2) Fraudsters heavily rely on fabricating crisis and excuses to ask money from victims.

Table 6. Organizational Structure of ORF (N=4) (continued)

Rege	2013	United States	Qualitative (content analysis)	72 online documents relevant to online romance scams	(1) Scammers are patient in grooming their victims (2) Scammers require only basic computer skills and sufficient social skills (3) Scammers followed established routines and worked in six-hour shifts (4) Scam networks subscribed to a 'scam-culture'
Qiu	2019	China	Qualitative (case study analysis)	One convicted ORF case	(1) ORF offenders in China usually operate as a group (2) Four types of sub-groups existed under the head: resource-providing group, conversation group, IT group, and money-laundering group
Wang and Pan	2020	China	Qualitative (Case study analysis)	37 ORF criminal cases in China	There are three categories for ORF in China: investment, gambling, and money extortion

For fraud groups operating in China, Qiu (2019) found that ORF offenders usually operate within a group, with members operating in different cells and assuming specialized roles (see also Wang and Pan, 2020). Criminal syndicates, not individuals, typically undertake ORF in China. Across nearly all ORF cases, Wang and Pan (2020) observed that ORF syndicates operating in China typically engaged in three swindling schemes: investment, gambling, and money extortion. These schemes can be operated independently by group members depending on the perceived situation or the type of victims. On a few occasions, these three schemes are implemented simultaneously to enhance the legitimacy of the crisis and excuses. In addition, Qiu (2019) specifically identified a joint group operational structure across nearly all ORF syndicates in China. Typically, four cells operate under the group head: resource-providing group, conversation group, IT group, and money-laundering group (Qiu, 2019). In particular, resource-

providing group is exceptionally vital to the criminal syndicate as they provide necessary materials and supplies to the members, including pre-written scripts, fraudulent pictures/videos, social media accounts as well as daily essentials (i.e., food and housing for fraudsters). Conversation group, or the "host" group is to contact victims online and establish a romantic relationship with them before encouraging them to invest large amounts of money in an online investment platform. IT group is the one providing technical supports, mainly the maintenance of the websites or applications. This group of fraudsters would also be manipulating the numbers for the invested money on the fraudulent platforms. Last, the money laundering group will be responsible for laundering the swindled money (Qiu, 2019).

Based on current research, ORF operating in Western countries has a less well-defined group structure, whereas ORF in China is group-oriented and structured with clear divisions of labor. By operating as a business with a hierarchical structure, offenders work collaboratively to increase scam legitimacy and reduce potential victim wariness.

Online Romance Scammers

Tables 7 to 12 reported studies examining online romance scammers, primarily identifying the criminogenic etiology of their criminal careers, the strategies they use to swindle victims, and the techniques they use to avoid detection by law enforcement. This section first discusses the factors that draw individuals (offenders) in and out of ORF perpetration. We categorize strategies used to perpetrate ORF into four groups: presentation of false profiles, fabrication of love stories, deployment of neutralization techniques, and use of manipulative strategies. Lastly, we describe the self-protective mechanism fraudsters use to minimize enforcement risks and detection.

Why Do People Fall into and out of ORF. Exploring the causes of crime with active offenders can be difficult, specifically for those operating online. For those who were apprehended, researchers can have a challenging time interacting with these fraudsters in a face-to-face setting as most of them were sentenced to felonies (i.e., money laundering) and kept in federal prison. For those who were not arrested, such a circumstance adds another layer of challenge for researchers to locate offenders as they tend to scatter in different countries and continue their scamming businesses anonymously in cyberspace. Table 7 indicates that only two studies gained the opportunity to interview online romance scammers: the first was conducted in China (Wu and Jian, 2014) and the second in Ghana (Barnor et al., 2020). They investigated why individuals fall in and out of online romance scams offending. In particular, Wu and Jian's (2014) study emphasized the reasons for both offender desistance and persistence in the fraud business. They located the study subjects from a group of rural young fraudsters operating on China's southeast coast. Only six individuals were selected because they satisfied the selection criteria, that is, individuals who participated and later desisted from ORF perpetration. Barnor and colleagues' (2020) study stressed only the factors that have drawn individuals into committing online romance scams. They interviewed ten persistent fraudsters who operated in internet cafés and consented to participate in the study (Barnor et al., 2020). These two studies addressed at least one of three main research questions:

1. What factors drive individuals to become fraudsters?
2. What causes fraudsters to desist?
3. What motivates offenders to commit ORF rather than other forms of online fraud?

Research suggests that individual-level socioeconomic vulnerabilities such as financial strains and low educational attainment increase the propensity to initiate or join in fraud operations. Wu and Jian (2014) pointed out that the vast financial benefits of romance scams play the most significant role in incentivizing people to commit fraud. Moreover, they further concluded that the choice of personal fraudulent behavior is influenced by instrumental rationality (money as the goal, various defrauding strategies as the means), emotional factors (considerations over family members), and moral factors (the corrupt nature of romance scams and the risks of being apprehended). During the early stage of fraud, when the main incentive is to earn enough money to support themselves and their families, participants confessed that their instrumental rationalities usually prevailed over emotional and traditional boundaries. At later stages in the fraud, when enforcement risks become higher, emotional and moral factors weigh more heavily on the fraudster's decisions. Ultimately, this group of desisted offenders chose to change their careers (i.e., self-employed or business) to achieve harmony between the pursuit of money and the concern for family (Wu and Jian, 2014).

In Barnor and colleagues (2020) study, recruited fraudsters emphasized the two main reasons they chose romance scams over other types of online fraud: fewer constraints (i.e., space, time, and resources) and less risk of exposure. With those benefits, fraudsters can potentially swindle money more efficiently from a large group of victims. To maximize profits, some fraudsters choose to join together when there is a convergence between opportunity and ability. Specifically, opportunity is the prerequisite for a group-based fraud operation. Fraudsters in the study alluded that opportunity referred to the current weakness in national cybercrime legislation and the lack of technical knowledge and skills among law enforcement officers. With the presentation of an opportunity and the potential incentives, social and technical abilities further

solidify criminal group formation. In detail, social ability points to fraudsters' ability to function as a group and understand the duties of all group members. It also emphasizes fraudsters' abilities to maintain high-frequent interactions with victims. Fraudsters are also required to possess particular technical abilities (i.e., VPN, SOCK[2], RDP) before joining a group. These technical skills help them to stay in the 'shadows' while offering extra leverage of outpacing their victims at certain stages in the fraud (i.e., extortion or blackmail). With the interplay between these factors, fraudsters were drawn into the criminal group and stayed persistent throughout their criminal careers.

Despite ORF operating in cyberspace, individuals' propensity to join fraud networks depends mainly on the factors existing in the physical world. Both studies showed that fraudsters are often defined by vulnerable socioeconomic backgrounds. Aside from those individualized factors, operating romance scams in online space offers offenders maximized rewards at minimal risk compared to other forms of fraud. In addition, the convergence of opportunity and skill can facilitate the formation of criminal syndicates (Wu and Jian, 2014; Barnor et al., 2020). Furthermore, Wu and Jian (2014) emphasized that fraudsters' likelihood of persisting in or desisting from ORF is influenced by the relative weight they place on monetary versus ethical considerations. Lastly, perceived risks of detection and sanction influence individuals' choices to enter and remain in this illegal business.

[2] Socks (or "SOCKS") is a protocol that a proxy server can use to accept requests from client users in a company's network so that it can forward them across the Internet. Socks use sockets to represent and keep track of individual connections.
With the RDP, it is easy to access someone's computer in the US and use it. In other words, by using RDP, you will access the person's user ID and password and browse on the person's laptop without his/her knowledge.

Table 7. Factors Influencing Fraudsters' Choices (N=2)

Author/s	Year	Location	Method	Target Population	Key findings
Wu and Jian	2014	United Kingdom	Qualitative (interviews)	6 online romance scammers	(1) Individuals in poverty, unemployed, with a low level of education, or with low income are more likely to become fraudsters (2) Fraudsters' continuation and desistance from fraudulent behaviors is a process of seeking balance between monetary desires and traditional attachment towards family and society (3) The seriousness of sanctions and the risk of exposure can influence fraudsters' decisions between monetary reward, moral and emotional factors
Barnor et al	2020	Ghana	Qualitative (semi-structured interviews)	10 romance scams perpetrators who operated as a group and six independent cybercrimes perpetrators	(1) The interplay of various socioeconomic factors is a major driving force behind the commission of cybercrime (2) The lack of confidence in law enforcement grants cybercriminals the opportunity to commit crimes (3) Societal and technical abilities that individualized fraudster possess help to formulate a criminal syndicate.

Strategies to Perpetrate ORF. The following three sections focus on reviewing studies researching the three main steps of ORF: the presentation of profiles, the fabrication of love stories, and the deployment of manipulative techniques.

Presentation of Profiles. During the initial contact stage, fraudsters strategically formulate their fraudulent profiles on dating or social media sites. Table 8 presents six studies on

fraudsters' strategies to formulate fake online profiles (Koon and Yoong, 2013; Huang et al., 2015; Kopp et al., 2015 and 2016b; Edward et al., 2018; Cross and Holt, 2021).

Edward and colleagues (2018) observed that the source location of most ORF profiles originates in West Africa, Malaysia, and South Africa, with Nigeria the most significant single contributor. In addition, profiles that appear to have been created in the United States often share text or images with scam profiles created elsewhere (Edward et al., 2018). Concerning the content of the fabricated profiles, fraudsters project a positive self-image to cater to victims' preferences (Koon and Yoong, 2013). For example, male scammer profiles often use fantasy traits to attract female victims (Kopp et al., 2016b). In particular, fraudsters' formulations of specific profiles are often intertwined to fabricate appropriate love stories or crises. For example, two studies by Kopp and colleagues (2015, 2016b) found that romance scammers often build personal love stories into fraudulent profiles, appealing to higher emotional stability among victims.

Huang and colleagues (2015) and Cross and Holt (2021) observed that fraudsters can also use different profiles to pander to their own "businesses." Huang and colleagues (2015) found four types of scammers frequently operate on dating sites: "escort service advertisements," "dates for profit," "swindlers," and "matchmaking services." Fraudsters sending escort services use unsolicited ads to promote their fraudulent businesses to attract users on dating apps. Moreover, by meeting victims in person, fraudsters who use dates for profits will exploit in-person meetings by asking for expensive gifts, drinks, or meals from victims. By conducting these scams in collusion with the owner of a restaurant or bar, fraudsters can potentially gain profits from the initial contact. Instead of deceiving victims in real life, some fraudsters prefer to hide their identities and swindle money in cyberspace by creating initial trust and then asking victims to

send them money to help in some task (i.e., buy a plane ticket, support the operation of businesses). These types of fraudsters are called "swindlers." Lastly, romance scammers will also create fake profiles of attractive people, lure users into handing out contact information, and then contact them directly, posing as the matchmaking agency. After receiving the deposit, the fraudster may disappear. Cross and Holt (2021) additionally observed that fraudsters' fabrications of military profiles serve two distinct but deliberate strategies—establishing an initial connection with victims through military identity or continuing storylines into financial requests. In sum, online romance scammers present different self-narrations on their profiles/accounts, attracting different types of victims/customers.

Table 8. Presentation of Fraudsters' Profiles (N=6)

Author/s	Year	Location	Method	Target Population	Key findings
Koon and Yoong	2013	Malaysia	Qualitative (case study analysis)	21 email interactions between fraudsters and victims	(1) Scammers will project positive self-image (2) Scammers will tailor their online identity according to victims' preferences
Kopp et al	2015	Australia	Qualitative (case study analysis)	37 fraudulent profiles	(1) The fraudulent profile needs to be seen in relation to the personal love story of the victim (2) Scam techniques appeal to strong emotions when involving in romantic relationship
Kopp et al	2016b	Australia	Qualitative (case study analysis)	345 fraudulent profiles	(1) Personal love stories are built into fraudulent profiles of online romance scams (2) Male scammer profiles are more likely to use fantasy traits to attract victims

Table 8. Presentation of Fraudsters' Profiles (N=6) (continued)

Edward et al	2018	United Kingdom	Quantitative	5402 fraudulent profiles	(1) The origin of most online dating fraud profiles is in West African, Malaysian or South Africa, with Nigeria the largest single contributor (2) Profiles which appear to have been created from the United States can often share text or images with scam profiles being created from elsewhere
Huang et al	2015	United Kingdom	Qualitative	510503 scam accounts	Four types of scammers that are identified on site: (1) Escort service (2) Dates for profit (3) Swindlers (4) Matchmaking services
Cross and Holt	2021	Australia	Mixed (quantitative analysis and content thematic analysis)	375 online victim reports	The deployment of military narrative serves two general purposes: (1) Initiate the conversation (2) Further the storyline to support financial requests

Fabrication of Love Stories. Table 9 identifies four articles discussing a common strategy that fraudsters use in the initial stage of a scam to fabricate fraudulent love stories (Kopp et al., 2016a and 2016b; Archer, 2017; Anesa, 2020). In general, the purposes of such a strategy are to: (1) camouflage the real intentions by coinciding with the desires and dreams of victims, (2) facilitate the romantic relationship, (3) facilitate the request of funds, and (4) win victims' trust and maximize the emotional connections. In addition, we also observed that fraudsters also strategically deployed love stories in ways that pander to victims' gender and cultural backgrounds.

Specifically, Anesa (2020) observed that fraudsters frequently fabricated love stories to camouflage their real intentions during the grooming stage. The purpose of using these fictional stories is to coincide with the desires and dreams of victims (Anesa, 2020). Specifically, Kopp and colleagues (2016) identified that fraudsters use two parallel stories—relationship and funding narratives—to facilitate relationship development and the request for funds. Borrowing from the "five main groups of stories "proposed by Sternberg (1999),[3] this study further identified four groups of "relationship development" stories used frequently by fraudsters during the initial stage of a scam. These five groups incorporate object stories (recovery, religion, and house/home), asymmetry stories (finding solutions to legal problems to gain 'real' family properties and fraudsters giving instructions to victims on what to do), coordination stories (business-related issues), and narrative strategies (using established fantasy stories). The most frequently used stories are fantasy and recovery stories, followed by religion (Kopp et al., 2016b). Notably, victims' self-reports also identified that fraudsters frequently "speak about the relationship as being permanent" to gain victims' trust in the relationship (Archer, 2017).

Fraudsters often study information that potential victims share online and then use this information to strategically fabricate stories to maximize the emotional connection (Anesa, 2020). Kopp and colleagues (2016b) noticed that fraudsters use different love stories based on the gender of victims. For example, the fantasy story is frequently used by female scammers in combination with religion, recovery, and traveler stories. In particular, the fantasy story follows the classic scenario of a "beauty" in need of help, with the victim identified as one who can rescue the situation (with payments) (Kopp et al., 2016b). The purpose of "female" fraudsters

[3] Five main groups of stories: asymmetrical stories, object stories, coordination stories, narrative stories, and genre stories.

doing this is to show the vulnerability of a young female who needs help from the male victims (who are typically older) to deal with "crisis." Such an approach plays on themes of masculinity and engendering empathy to increase chances of getting the requested monetary assistance (Kopp et al., 2016b). Last, there are differences in the deployment of love stories according to the origins of the scam. African profiles appear to be more confident and demanding, whereas Russian profiles suggest a preference for softer and humbler presentations. Such differences may originate from the different cultural backgrounds and values held by scammers (Kopp et al., 2016b).

Table 9. Characteristics of the Fabricated Stories/Crisis (N=4)

Author/s	Year	Location	Method	Target Population	Key findings
Kopp et al	2016a	Australia	Qualitative (case study analysis)	17 online victim reports	(1) Identified two parallel stories deployed most often. (2) Among these two types of stories, five types of story categories are proposed.
Kopp et al	2016b	Australia	Qualitative (case study analysis)	345 fraudulent profiles	(1) The most frequently used stories are fantasy and recovery story followed by religion and history story (2) There are differences in terms of the deployment of love stories by genders (3) There are differences in term of the deployment of love stories according to the origins of scam
Anesa	2020	Italy	Qualitative (content thematic analysis)	26 online interactions between fraudsters and victims	(1) Frauds are camouflaged as love stories and various mechanisms are adopted to enhance involvement. (2) Fraudsters will study victims' preferences posted online or draw the hints from their shared photos or videos.

Table 9. Characteristics of the Fabricated Stories/Crisis (N=4) (continued)

Archer	2017	USA	Qualitative (content thematic analysis)	82online victim report	Three key themes were identified in the stories of the victims: (1) "Speaking about the relationship as being permanent" (2) "Tragic biographic narratives" (3) "Deadline" the scammer imposes deadlines on the victim to comply with

The Deployment of Manipulative Strategies. Following the use of fabricated profiles and love/romantic stories, Table 10 summarizes seven studies that identified fraudsters' psychologically manipulative strategies used during the commission of online romance scams (Whitty, 2013b; Cross, Dragiewicz and Richard, 2018; Shaari et al., 2019; Ye and Duan, 2020; Drejiers and Rudzisa, 2020; Carter, 2021; Wang and Topalli, 2022).

Whitty (2013) interviewed victims and identified seven persuasive techniques used by romance scammers. The techniques include using "person of authority," activating "norms," deploying "scarce deal/emergency/crisis," using "reciprocation," appealing to "commitment and consistency," emphasizing "love, liking, and similarity," and employing "visceral influences" (Whitty, 2013b). Her study further pointed out that these seven techniques often trigger victim motivational and cognitive errors, increasing susceptibility to scams (Whitty, 2013b). In furtherance of those observations, Wang and Topalli (2022) additionally revealed that fraudsters would also entice victims guilts and use specific fraud scenarios (i.e., time sensitive emergency funds, medical funds, business funds, package delivery scam, banking scam and inheritance scam) to swindle their victims. Further, Drejiers and Rudzisa (2020) revealed that fraudsters' conversations with victims have manipulative effects, mainly in their written letters. This study identified that fraudsters frequently use flattering language appealing to trust and romance,

engendering emotions of attachment, bonding, and altruism among victims (Drejier and Rudizisa. 2020).

Shaari and colleagues (2019) reported that scammers are polite and patient with victims during the grooming stage. The most frequent strategy fraudsters use to groom victims is deploying visceral influences by expressing love and commitment to the relationship (Cross, Dragiewicz and Richard, 2018; Ye and Duan, 2020; Carter, 2020). For example, fraudsters used intimate personal indicators/pet names (e.g., sweetheart, my love, husband/wife) to denote their commitment (Ye and Duan, 2020). As mentioned, using narrative love stories is another strategy fraudsters use to facilitate the development of romantic relationships with victims (Ye and Duan, 2020). Through this initial set-up, the fraudster presents himself as being powerful, authoritative, financially needy, romantically vulnerable, and desperate for help (Carter, 2020).

Following the grooming stage, Shaari and colleagues (2019) also found that fraudsters' attitude shifts from positive to negative during the money-asking stage, involving acts such as direct claims, statements, and requests. During this process, Cross, Dragiewicz and Richard (2018) identified that some manipulative psychological techniques are like those used by domestic violence offenders. These strategies include economic abuse, isolation, monopolization, degradation, psychological destabilization, and emotional or interpersonal withdrawal. Fraudsters also attempt to ensure complete manipulation and obedience by isolating victims from outside supports. By deploying such tactics, fraudsters seek to deprive victims of access to reality checks and make victims think they will be lonely forever without the fraudsters, and that any intervention from friends or family will create an obstacle (Carter, 2020).

Table 10. Manipulative Strategies Used by Fraudsters (N=7)

Author/s	Year	Location	Method	Target Population	Key findings
Whitty	2013b	London	Qualitative (Semi-structured interviews)	20 romance scams victims	(1) Fraudsters deploy 7 potential persuasive techniques to influence victims' rational judgements. (2) A scammers' persuasive technique model is established.
Cross, Dragiewicz and Richard	2018	Australia	Qualitative (semi-structured interviews)	25 romance scams victims	There are some similarities in terms of offending strategies deployed by DV offenders and romance scammers.
Shaari et al	2019	Malaysia	Qualitative	60 online interactions between fraudsters and victims	(1) Scammers will use some politeness strategies to establish relationship with victims before executing scamming activities. (2) Towards the end of scam, the entire politeness strategy basically shifts from positive to negative and this involves acts such as direct claims, statements, and requests
Ye and Duan	2020	China	Mixed (experiment and case study analysis)	(1) 1 ORF criminal case (2) 30 recruited general population	Fraudsters' use of personal indicators, narrative strategies and turn-taking strategies may facilitate the formation of romantic relationship with victims
Dreijers and Rudzisa	2020	Latvia	Qualitative	7 email interactions between fraudsters and victims	(1) There is a manipulative effect observed among scammers' interactions with victims (2) The interactions revealed similar lexical and macrostructural patterns common in online romance scams
Carter	2021	United Kingdom	Qualitative (case-study approach)	a conversation between the victim (Mandy) and offender	Through the set-up and drip feed, the use of visceral responses and isolating the victim, the fraudster can present himself as rich, powerful and authoritative, as well as financially needy and need helps.

Table 10. Manipulative Strategies Used by Fraudsters (N=7) (continued)

Wang and Topalli	2022	United States	Qualitative (thematic analysis)	52 Victim testimonials collected from five main websites	(1) Fraudsters are observed to use seven different social engineering techniques (2) Fraudsters are observed to use six different fraud scenarios

Fraudsters' Self-Protective Mechanisms. The last part of this section identified four studies addressing two self-protective mechanisms fraudsters commonly use when they face heightened risk of exposure (Wang et al., 2021; Rege, 2013; Offei et al., 2020; Barnor et al., 2020). The first mechanism is behavior modification, which was presented in Wang and colleagues' (2021) experimental study. As summarized in Table 11, the study used an innovative experimental approach to send warning messages to fraudsters directly pointing to the fraudulent behavior and the potential legal sanctions. To make the experimental results stand out, Wang and colleagues sent two additional types of messages to fraudsters, namely ambiguous (i.e., simply a "hi") and "promising" messages (i.e., willing to offer them money to visit the victim). This research demonstrated that romance scammers can indeed be restrictively deterred. Precisely, fraudsters who were sent a deterrence message, instead of a promising or ambiguous message, replied less often, used fewer words in their replies, and replied less frequently without denying wrongdoing (Wang et al., 2021).

Table 11. The Effects of the Sanction on Altering Fraudsters' Behaviors (N=1)

Author/s	Year	Location	Method	Target Population	Key findings
Wang et al	2021	USA	Mixed (experiment and qualitative analysis)	546 female romance scammers	• The results show that romance scammers can be restrictively deterred. • Romance scammers can be deterred in various ways, in terms of their change of behaviors.

The second mechanism is the use of neutralization techniques. Three studies presented in Table 12 examined this tactic. As indicated previously, the deployment of neutralization techniques is one of the self-protective mechanisms that fraudsters adopt when non-affiliated individuals inquire about their illegal operations. In order to release themselves from moral guilt, Rege (2013) found that three types of neutralization techniques are used frequently by a group of Nigerian scammers: "denial of a victim," "denial of injury," and "apply to higher authority" techniques (see also Brulliard, 2009; Dixon, 2005). Consistent with previous observations, Barnor and colleagues (2020) provide further empirical support for use of both "denial of injury" and "denial of a victim" neutralizations. To further explore empirical support for the prior observations, Offei (2020) surveyed a group of active romance scammers operating in an internet café. The quantitative evidence revealed that only "denial of a victim" is used to justify the intention to defraud victims. Additionally, fraudsters were observed to use "denial of risk" to reason that involvement in online romance scams is less risky than other predatory crimes (Offei, 2020).

Table 12. Neutralization Techniques Used by Offenders (N=3)

Author/s	Year	Location	Method	Target Population	Key findings
Rege	2013	USA	Qualitative	72 online documents relevant to online romance scams	Online scammers engaged in three main neutralization techniques to rationalize their activities before bilking their victims.
Barnor et al	2020	Ghana	Qualitative (semi-structured interviews)	4 romance scammers who operated as a group and six independent cybercrime perpetrators	• Fraudsters find justifications to make sense of their unlawful behaviors, specifically the use of "denial of injury" and "denial of a victim".
Offei et al	2020	Ghana	Quantitative (cross-sectional survey)	350 individuals with knowledge Or committed crimes	• Only denial of victims is used to justify • The findings about denial of risk is consistent

Online Romance Scams and its Victims

The previous section reviewed the studies focusing on the stages and organizational structure of ORF as well as the characteristics of online romance scammers. The following section provides additional review that emerged during the analysis process, seeking to address (1) the severe negative influences of ORF on victims, (2) vulnerable characteristics of victims (demographic, psychological, personality, and behavioral traits), (3) the potential self-protective approaches victims can use when chatting with strangers in cyberspace. Specifically, we have identified two studies revealing the negative impact of ORF on victims' overall physical and emotional well-being (Whitty and Buchanan, 2016; Ye and Duan, 2020). In addition, seven studies identify vulnerable risk factors for ORF victimization, including demographic, psychological, personality, and behavioral traits (Garrett, 2014; Buchanan and Whitty, 2014; Whitty, 2018; Whitty, 2019; Saad et al., 2018; Cross and Holt, 2021; Offei, 2021). Last, two studies proposed self-protective mechanism that victims can use when they interact with strangers in online space (Whitty, 2019; Cross and Holt, 2021; Cross and Layt, 2021).

Negative Influence of ORF. Table 13 presented three studies that stressed the vulnerability of victims and the pervasive negative effects of ORF victimization (Whitty and Buchanan, 2016; Ye and Duan, 2020; Cross and Lee, 2022). Victim-centered research on ORF suggests that victims have higher risk tolerance for investing in opportunities, maintaining new relationships, and engaging in new experiences (Ye and Duan, 2020). During the post-victimization stage, Whitty and Buchanan (2016) highlighted several ways victims negatively experience their victimization. First, victims can suffer from shame, embarrassment, and depression, feelings that can be exacerbated by lack of family and social support. Moreover, victims often experience negative personal and social changes due to financial and emotional

losses. Notably, despite these impacts, some individuals maintain trust in future relationships and continue to use online dating sites (Whitty and Buchanan, 2016).

Our review suggests that the consequences of ORF for victims can be devastating. Understanding potential vulnerabilities for victims falling into these "romantic" traps is therefore critical. This section reviews research focusing on the aspects of victims that result in their vulnerability and imprudence, including demographic, psychological, personality, and behavioral aspects of victims.

Table 13. Background of ORF Victimization (N= 3)

Author/s	Year	Location	Method	Target Population	Key findings
Whitty and Buchanan	2016	United Kingdom	Qualitative analysis	20 individuals are recruited from an introduction from law enforcement or participants in a survey study conducted by the author	8 key themes relating to the aftermath impact of online romance scams are identified
Ye and Duan	2020	China	Mixed (experiment and case study analysis)	1 *Sha Zhu Pan* criminal case and 30 general population	(1) When in a romantic relationship, victims are more likely to make decisions that are involved with higher risks. (2) When victims are making decisions to offer money to offenders, their decision-making process involves with three aspects: investment, maintaining relationship with offenders and attempting to try new things.

Table 13. Background of ORF Victimization (N= 3) (continued)

Cross and Lee	2022	Australia	Qualitative analysis (thematic)	3259 victimization reports from ACCC	(1) Fear of crime can be observed among those victims who reported their crimes (2) An interaction between the themes of affect, behaviors and cognition can be observed among victims with fear of crime mentality (3) Fear of crime can be evident across both online and offline context

Factors Influencing the Victimization Propensity: Demographic. Four studies presented in Table 14 identified the characteristics of online romance scams victims' age, gender, language, income, education, and marital status. It should be emphasized that current research on the demographic characteristics of ORF victims is not designed to be representative of the general or even victim population, but available studies indicate young to middle aged individuals are often the targets of online romance scams (Garret, 2014; Whitty, 2018; Saad et al., 2019; Cross and Holt, 2021). Moreover, females and English speakers are likely to be targeted (Garret, 2014; Cross and Holt, 2021). Garrett (2014) and Saad and colleagues (2018) found that individuals' propensity to be targeted by online romance scams is inversely related to income. In other words, individuals with little income or who work part-time are more likely to be defrauded by online romance scammers. Interestingly, people with higher education have a greater chance of being victimized (Whitty, 2018; Saad et al., 2018), which contradicts the belief that less educated individuals are more likely to fall victim to ORF (Whitty, 2018). It has been hypothesized that better-educated people are overconfident in detecting scams (Whitty, 2018).

Table 14. Demographic Characteristics of ORF Victimization (N= 4)

Author/s	Year	Location	Method	Target Population	Key findings
Garrett	2014	United States	Survey based quantitative analysis	300 internet users who visited the www.Russian-Dating-Scams.com between January 2009 to March 2014	(1) Individuals between age 30-39, 40-49 and 50-59 tend to be more likely to be victimized (2) Majority of victims are coming from English-speaking countries (3) Study participants who worked part time ("part time" and "employed with two jobs") show significantly higher victimization rates and higher mean loss amounts
Whitty	2018	United Kingdom	Survey based quantitative analysis	11780 general population recruited through online ''Qualtrics''	Individuals at higher risk of being scammed are female, middle-aged, having a high education level
Saad et al	2018	Malaysia	Survey based quantitative analysis	280 romance scams victims in Malaysia	(1) Between the ages of 25 and 45 years were likely to be the victims of cyber-love scams (2) The majority of the victims are educated with the majority having a diploma (3) Individuals with no income are also vulnerable to being the victims
Cross & Holt	2021	Australia	Mixed (quantitative analysis and content thematic analysis)	73 online victim report	There were multiple significant predictors identified for reporting a military narrative, including being female, being younger in age, being an English speaker

Factors Influencing the Victimization Propensity: Psychological. Table 15 shows three victim-centered studies that explore the psychological traits that may lead to higher likelihood of being victimized by ORF (Garrett, 2014; Buchanan and Whitty, 2014; Whitty, 2019). Specifically, these studies identify two psychological characteristics that increase the

likelihood of online romance scams victimization. First, from a psychological perspective, the studies suggest that a strong desire for a romantic partner increases victimization risk. This risk seems to increase for individuals with highly idealized romantic beliefs (Garret, 2014). For example, two studies found that individuals with highly idealized romantic beliefs are less diligent in detecting online romance scams (Buchanan and Whitty, 2014; Whitty, 2019). Second, having amenability to long-distance dating is associated with a higher likelihood of victimization (Garret, 2014). Such individuals appear to be more easily be convinced by fraudsters' various monetary requests.

Table 15. Psychological Characteristics of ORF Victimization (N = 3)

Author/s	Year	Location	Method	Target Population	Key findings
Garrett	2014	United States	Survey based quantitative analysis	300 internet users who visited the www.Russian-Dating-Scams.com between January 2009 to March 2014	(1) The higher number of respondents with an interest in finding a romantic partner positively correlates with the higher likelihood of victimization (2) Users with no interest in long-distance dating prior to the scam appear the least likely to go along with scammers requests for travel expenses, or to send large amounts of money for such expenditures
Buchanan and Whitty	2014	United Kingdom	Survey based quantitative analysis	• Study 1: 853 users of a European dating website • Study 2: 397 victims recruited from online support site	High scores on the romantic belief of idealization was associated with likelihood of being a romance scams victim

Table 15. Psychological Characteristics of ORF Victimization (N = 3) (continued)

Whitty	2019	United Kingdom	Survey based quantitative analysis	261 general population in UK	Those who scored high on romantic beliefs are less likely to spot online romance scams

Factors Influencing Victimization Propensity: Personality. As indicated in Table 16, Whitty and colleagues conducted three major studies (Buchanan and Whitty, 2014; Whitty, 2018, 2019) revealing personality characteristics of online romance scams victims. Notably, individuals at higher risk of being defrauded have higher scores on various personality traits, including urgency, sensation seeking, unkindness, trustworthiness, and addictive disposition (Whitty, 2018). Moreover, individuals who scored low on factors measuring consideration of future consequences, impulsivity, and openness to new experiences were less likely to be scammed by fraudsters (Buchanan and Whitty, 2014; Whitty, 2019). As most scam victims experience certain levels of distress, victims with high neuroticism and high loneliness tend to suffer from high levels of emotional distress compared to those who score low on these personality traits (Buchanan and Whitty, 2014).

Table 16. Personality Characteristics of ORF Victimization (N = 3)

Author/s	Year	Location	Method	Target Population	Key findings
Buchanan and Whitty	2014	United Kingdom	Survey based quantitative analysis	(1) Study 1: 853 users of a European dating website (2) Study 2: 397 victims recruited from online support site	(1) Level of emotional distress was associated with high neuroticism, and also with high loneliness (2) Victims who did not lose money are associated with low openness to experience
Whitty	2018	United Kingdom	Survey based quantitative analysis	11780 General population recruited through online ‘‘Qualtrics’’	Individuals at higher risk of being scammed are high on urgency and sensation seeking, less kind, trustworthy, and have an addictive disposition

Table 16. Personality Characteristics of ORF Victimization (N = 3) (continued)

Whitty	2019	United Kingdom	Survey based quantitative analysis	261 general population in UK	Those who scored low in consideration of future consequences and low impulsivity are less likely to spot online romance scams

Factors Influencing Victimization Propensity: Behavioral. As presented in Table 17, four victim-centered studies highlight three major behavioral characteristics of online romance victims: prior experiences, cybercrime awareness, and behavioral presentation during the scam. Garrett (2014) and Whitty (2019) found that individuals with no international dating experiences and who have not previously spotted romance scams are more susceptible to fraudulent narratives. Concerning the role of cyber awareness, potential victims are more likely to respond to money solicitations if they use the internet as the primary medium to search for romantic partners (Garrett, 2014). Moreover, Saad and colleagues (2018) also revealed that lack of computer skills and cybercrime awareness is associated with a higher probability of being scammed. Admittedly, most research suggests that scam victims' behaviors are provoked substantially by the psychological, behavioral, and emotional influences of offenders. As a result, observers note that victims should not be held unduly responsible for the outcomes of the fraudulent events (Sorrell and Whitty, 2019; Cross, 2015 and 2018). Based on observations from offender data, Offei (2021) explored the types of victims' responses facilitating offenders' rationalization of their offending behaviors. His study found that scam offenders rely heavily on victim precipitation to perpetuate their criminal activities: All the three dimensions of victim precipitation theory (facilitation, provocation, and openness) were used by these criminals as justification techniques for engaging in online romance scams.

Table 17. Behavioral Characteristics of ORF Victimization (N = 4)

Author/s	Year	Location	Method	Target Population	Key findings
Garrett	2014	United States	Survey based quantitative analysis	300 internet users who visited the www.Russian-Dating-Scams.com between January 2009 to March 2014	(1) Participants that use the (2) Internet in their search for a romantic partner were twice as likely to respond to money solicitation as those searching for a partner offline. (3) Participants who had no prior experience with international dating had high victimization rates and the highest mean loss amounts. (4) Prior IT training seems to have little effect on the likelihood of victimization or the mean loss amount, but users with no IT training have the highest victimization rate
Saad et al	2018	Malaysia	Survey based quantitative analysis	280 romance scams victims in Malaysia	Those who lack computer skills and less levels of cybercrime awareness are more likely to be a victims of online romance scams
Whitty	2019	United Kingdom	Survey based quantitative analysis	261 general population in UK	Those who had previously spotted a romance scam were more likely to accurately distinguish scams from genuine profiles
Offei	2021	Ghana	Survey based quantitative analysis	320 online romance scammers	(1) Victims' facilitation positively influences their relationship with the intention to commit internet romance scams (2) Victim's provocation positively influences their intention to commit internet romance scams. (3) Victim openness positively influences the relationship between the victim and the intention to commit internet romance scams

Victims' Self-Protection Behaviors. Lastly, three studies in Table 18 use empirical evidence to discuss how potential scam victims can avoid being swindled. Cross and Holt (2021) found that victims who lost their details and financial information are more likely to be targeted by military narrative offenders. Cross and Layt (2021) also found that victims can use internet searches such as reverse image searches to verify the legitimacy of the strangers' identities. Moreover, the information provided on fraud detection websites can help detect inauthentic profiles (Cross and Layt, 2021). Finally, Whitty (2019) found that individuals who spend more time assessing a profile's authenticity are more likely to detect a scam profile. In sum, individuals are less likely to be victimized if they 1) use the internet to search specific profiles for evidence of scamming, 2) take steps to protect their identity and financial information, and 3) are patient and rational when encountering an ideal profile on dating apps.

Table 18. Protection Behaviors of ORF Victimization (N = 3)

Author/s	Year	Location	Method	Target Population	Key findings
Cross & Holt	2021	Australia	Mixed (quantitative analysis and content thematic analysis)	375 online victim report	• Complainants who lost their personal details were also more likely to involve military narratives • Those who did not report abuse in their narrative, did not lose personal details, but lost their banking details were also more likely to report financial losses
Cross & Layt	2021	Australia	Qualitative analysis	2671 reports of romance scams lodged to the ACCC during July 1, 2018, to July 31, 2019	(1) Use of a reverse image search on the profile picture or other photo (2) The potential effectiveness of internet searching as a strategy to confirm or deny the legitimacy of a profile (3) The use of fraud websites

Table 18. Protection Behaviors of ORF Victimization (N = 3) (continued)

Whitty	2019	United Kingdom	Survey based quantitative analysis	261 general population in UK	Individuals use longer time in their responses to a profile have higher possibility of getting the correct fraudulent profiles.

General Discussion of Evidence

As an emerging phenomenon, online romance scams did not catch the attention of policymakers or researchers until it began to cause substantial harms to individuals and society. Since the seminal article by Rege (2009) noted the dynamic features of online romance scams operations, a number of scholars shifted their attention to this unique type of cyber-enabled crime, focusing on understanding the *modus operandi* of offenders and vulnerabilities of victims. As research on ORF is still emergent, scoping reviews are a valuable methodology for understanding the current theory and evidence in online romance scams literatures.

This scoping review increased current understandings of this phenomenon by reviewing current ORF literature analyzing the nature of the event itself, as well as the characteristics of fraudsters and victims. By following the PRISMA Extension for Scoping Reviews (Tricco et al., 2019), we identified 36 relevant articles for this review.

In comparison to the previous scoping review conducted by Coluccia and colleagues (2020), this review made several advancements in data collection and analysis. First, in addition to the three databases Coluccia and colleagues (2020) included in their review, we searched 9 additional databases (1 database is in Chinese), leading us to find additional ORF-related studies. Note that our 35 included studies contain the 12 studies from the earlier scoping review (Coluccia et al., 2021). Second, the current review expanded the search terms and fields used in the academic database searches. Third, the current review accommodates additional aspects of

online romance scams. The previous review focuses primarily on the epidemiological aspects, relational dynamics, and the psychological characteristics of victims and scammers. This current review expanded this purview to ORF stages and operations, fraudster decision-making, fraudster self-protective behaviors, and victim vulnerabilities.

We framed our analysis of the ORF literature using the "crime triangle" perspective, which focused our attention on (i) how scammers operate, (ii) the characteristic of these fraudsters, and (iii) the traits of victims.

In the first domain, we highlighted the stages and organizational structure of ORF across cultural contexts. In detail, four studies revealed that the general stages of ORF differ across Western and non-Western contexts. In both contexts, fraudster profiles seek to connect online with ideal victims, bait them by deploying various grooming techniques (e.g., using romantic schemes), and then exploit the victim before disappearing (Whitty, 2013a and 2013b; Qiu, 2009; Wang and Zhou, 2022). Despite these resemblances, differences prevail across contexts. ORF in non-Western settings, specifically China, tend to use more complicated "sting" techniques. For example, most scammers in China typically follow "money-making" schemes that promise considerable profits to lure victims onto a fraudulent investment platform (Qiu, 2009; Wang and Zhou, 2022). In comparison, fraudsters in Western settings tend to use urgent crises or advanced payment scenarios to solicit cash payments directly from victims (Whitty, 2013a and 2013b). As for the different organizational structures of ORF, four studies confirmed that ORF operating in Western countries have less defined group structure when comparing to the more centralized and business-alike group operations in China (Rege, 2009 and 2013, Qiu, 2019; Wang and Pan, 2020). Specifically, online romance scams syndicates in China typically divide themselves into

cells with different functions. Recruited fraudsters will be assigned to a cell based on their specialized skills (Qiu, 2019).

In the second domain, we also presented findings on why fraudsters fall in and out of ORF, strategies to perpetrate ORF, and fraudsters' self -protective mechanisms. Two studies found that individuals prone to be drawn into the criminal syndicate because they are more socioeconomically vulnerable (Wu and Jian, 2014) and think that participating in romance scams can give them quick cash with fewer constraints and less risk of exposure (Barnor et al., 2020). Moreover, individuals can persist in or desist from the scam when there is a change on the weight they place on monetary versus ethical considerations. Lastly, fraudsters can be deterred from continuing the fraud businesses due to external forces—seriousness of sanctions and risk of exposure (Wu and Jian, 2014).

Seventeen studies (not unique) summarized the characteristics of three main strategies that fraudsters deploy to perpetrate ORF: presentation of profiles, fabrication of love stories and deployment of manipulative strategies. Mainly, most fabricated profiles have certain features, for example, concentrating in certain regions (Edward et al., 2018), catering towards gender differences (Koon and Yoong, 2013), appealing to emotional stability among victims (Kopp et al., 2015 and 2016b) and catering towards different fraudulent online businesses (Huang et al., 2015; Cross and Holt, 2015). Moreover, researchers revealed some common traits existed within the fabricated love stories, that is to say the frequent deployment of two parallel stories (i.e., relationship and funding stories) (Kopp et al., 2016), the focuses of love stories based on personal shared information online (e.g., lifestyle, country origins and gender) (Anesa, 2020, Kopp et al., 2016a; Archer, 2017; Kopp et al., 2016b). In addition, fraudsters are also observed to deploy manipulative strategies, for example, deploying "scarce deal/emergency/crisis" (Whitty,

2013; Wang and Topalli, 2022) and “isolation” or “monopolization” (Cross and Richard, 2019). the use of flattering languages (Drejiers and Rudzisa, 2020), the establishment of reliable figure through romantic relationship (Ye and Duan, 2020; Nabid, 2021; Cater, 2020; Wang and Topalli, 2022), the presentation of contrasted attitudes (positive and negative) before and after the money-asking stage (Shaari et al., 2019).

Lastly, four studies identified two common self-protective mechanisms that fraudsters frequently employ when there are threats of being exposed. The first is the behavioral modification (Wang et al., 2021). And the second one is the use of neutralizations (Rege, 2013; Offei, 2020; Barnor et al., 2020).

In the third domain, studies revealed the negative influence of ORF on victims, major vulnerable factors leading to the victimization, and the potential self-protection behaviors among potential victims. In general, online romance scams can result in tremendous emotional, psychological and even physical traumas along with the financial loss (Whitty and Buchanan, 2016; Sorrell and Whitty, 2018; Ye & Duan, 2020). Pertaining to answer the question on what traits make an indiivudal more likely to fall into the scam, studies found that both demographic (Garrett, 2014; Whitty, 2018; Saad et al., 2018), psychological (Buchanan & Whitty, 2013; Whitty, 2019), personality (Buchanan & Whitty, 2014) and behavioral traits (Offei, 2021; Whitty, 2019) could influence the propensity of being victimized or revictimized in the future. Lastly, victims are also recommended using certain self-protection behaviors to victims or potential targets when talking to strangers online, such as learning to protect their personal or financial information and frequently doing reverse image checks. (Cross and Holt, 2021; Cross and Layt, 2021; Whitty, 2019).

Limitations

There are three major limitations of this scoping review. Methodologically, scoping reviews have a broad focus by definition (Peterson et al., 2017). Nevertheless, a scoping review remains appropriate for investigating the state-of-knowledge regarding online romance scams because the evidence remains emergent. Moreover, by following established guidelines for reporting scoping review results, we followed best methodological and reporting practices (Tricco et al., 2018).

In a typical scoping review, two reviewers will dually screen and code all studies. Due to personnel and time constraints, dual screening and coding was feasible for a subset of studies. Despite this drawback, coders achieved perfect match on studies that were dually screened.

The third limitation is the inclusion of online romance scams studies in Chinese. Potential selection and translation bias may be present, even with a first author whose native language is Chinese. Moreover, there could be other ORF literature in other languages. Future research should expand search protocols to additional languages.

Conclusions and Implications

Our review highlights three main research gaps concerning online romance scams: (1) homogenous content for most ORF offender and victim studies, (2) homogenous data collection and analytic methods for most ORF offender and victims' studies, and (3) an absence of ORF studies exploring criminal justice system responses. Taken together, these research gaps suggest that additional data outlets are needed to enable researchers to explore diverse perspectives concerning offending, victimization, and law enforcement. Recommendations for future research

are suggested below to increase communications between researchers and law enforcement and enhance theoretically driven ORF research.

First, collaborating with criminal justice agencies may allow researchers to obtain primary interview data from offenders who are, for instance, detained in state or federal prisons. Several previous studies have interviewed offenders of physical crimes locked in prison and generated meaningful outcomes on the patterns of criminal behaviors and implications for criminal justice practices (Fendrich et al., 1995; Cheah et al., 2020; Jeffries and Chuenurah, 2019; Liu et al., 2021). Although it should be admitted that talking to detained offenders may bias the responses to a certain extent compared to communicating directly with active offenders (e.g., Copes et al., 2015), such an approach is ideal to obtain direct ORF offender data as cybercriminals are hard to locate in anonymous space. As a result, through interviewing, researchers may be able to gain additional insights compared to those revealed through anonymous online sources.

Furthermore, collaborations with law enforcement can also enable researchers to obtain victimization data. Multiple studies done by Cross are suitable exemplifiers for such an approach. For example, Cross and Layt (2021) used the victim complaint data gathered from a federal Australian governmental agency to analyze victims' responses to bogus profiles and generate insights for how individuals can protect themselves from ORF. Thus, by establishing relationships with law enforcement and government agencies, researchers may be able to leverage new data for understanding ORF. For instance, in the United States the Internet Crime Complaint Center (IC3) collects data from victims' self-reports, which could be a fruitful data source for future academic research.

Establishing a connection with law enforcement can also facilitate research-practitioner collaborations into online romance scams. Whitty (2013a) used multiple sources to investigate the early anatomy of online romance offending, including interviews with law enforcement experts on cyber-fraud (Whitty, 2013a). As previously stated, there are no studies in online romance scams exploring the performance of law enforcement agencies in investigating online romance cases. Future researchers should learn from Whitty's 2013(a) study to collect responses from different law enforcement agencies concerning their performance in the investigation and prosecution of online romance scams offenders.

Lastly, future studies in ORF should be theoretically driven. To date, ORF studies have tended to rely on researchers' interpretation without support from existing criminological theories. Future research into ORF should use appropriate theoretical orientations, such as rational choice theory or routine activity theory, to explain offender and/or victim behaviors.

Theory-informed research will have stronger implications for developing policy and practices, including crime prevention and intervention efforts. Although online romance scammers strategically plan their operations (Whitty 2013a and 2013b), they are deterrable (Wang et al., 2021). As a result, a proactive approach to mitigating online romance scams should be deployed by online service providers and law enforcement actors. Dating platforms operators could develop algorithms to identify likely offenders and then send them automated deterrence messages, which can be stopped by passing a screening protocol. Such a proactive approach can also incorporate screening tools that assist in identifying at-risk victims. Admittedly, such a proposal may involve with the privacy or freedom of speech disputes, however private industry and law enforcement agencies can collaborate to come up with solutions to overcome such a concern.

At a societal level, although online romance scammers have caused substantial harm to both victims and government finance, ORF fraudsters tend to be burdened by poverty, unemployment, low education, and other social inequities (Wu and Jian, 2018; Barnor et al., 2020). Consequently, government agencies might consider developing specialized reentry programming for convicted fraudsters to prevent the return to crime and enhance reintegration.

Importantly, to avoid victim-blaming and the associated long-lasting negative effects (Buchanan and Whitty, 2014; Cross et al., 2018), the development of government-based victim assistance and support programs could prove beneficial (Cross et al., 2014). Victims are rarely made whole, even after successful prosecution and asset recovery. Effective counseling and self-protection programs may assist scam victims and prevent future revictimization.

In summary, this review provides a comprehensive review of online romance scams studies examining some offending and victimization characteristics. With increased amounts of empirical online romance scams studies, future review study should continue in current rigorous tradition, however overcoming existed limitations, to generate updated review studies using advanced methodologies (i.e., systematic review or meta-analysis) where possible. Moreover, based on the research and practical implications drawn from current review study, future scholars studying online romance scams should be theoretically driven and work collaboratively with law enforcement agencies and cybersecurity industries. Public serves and private industries should also establish join forces in creating multiple prevention and assistant programs in minimizing the occurrences and harms brought by online romance scams. Only together the efforts from academia, governmental agencies and industry leaders, can a safer online environment be created for daters.

Chapter III: What Money Can Do: Examining the Effects of Rewards on the Behavior of Online Romance Scammers

Abstract

In this study, we use a randomized experimental design to explore how fluctuations in potential rewards shape the behavior of persons committing online romance fraud (ORF). Our mixed-method analysis of 94 sequential email exchanges with active fraudsters first illustrates that their exchanges with potential victims are comprised of up to seven different conceptual domains. We then demonstrate that fraudsters' use of these various domains' changes in accordance with variations in the presented likelihood of receiving reward from victims. Our findings add to current understanding of ORF and have implications for interpersonal deception theory and rational choice.

Introduction

Romance scams—or swindling money from victims using false identities and sham romantic relationships has long been documented (Buse 2005; Vitola 2018). With the advent of the internet romance scammers began operating online, increasing their access to potential victims and thus the prevalence and harms of this crime (Rege 2009). In the United Kingdom, losses in 2020 from bank transfer romance scams reached approximately £18.3 million by November, a 20% increase from 2019 (UK Finance 2021). From 2016 to 2020 losses in the United Stated quadrupled, with losses in 2020 alone reaching $304 million (FTC 2021). Canadian authorities report similar figures, with reported losses in 2020 of more than $18.5 million (CBS News 2021). In China, victims reported financial losses of ¥3.88 billion, or almost $598 million (Sina News 2019). In addition to financial damages, victims of online romance scams also report negative social impacts (i.e., damage to intimate relationships) and emotional,

psychological, and physical harm (Cross, Smith, and Richards 2014; Cross 2016; Whitty and Buchanan 2016).

Despite these harms, criminologists have devoted limited attention online romance scams. The scant research that has examined it has been limited to studies drawing from victims' experiences. These have focused on identifying typologies of romance scammers, their motivations, and analyses of the financial and non-financial impacts on victims (e.g., Whitty and Buchanan 2012 and 2016; Buchanan and Whitty 2014; Sorell and Whitty 2019; Whitty 2015). Outside of criminology, in fields such as information and computer science, attention to online romance scams has been limited to developing tools and algorithms to identify and prevent romance scams schemes (e.g., Pan et al. 2010; Suarez-Tangil et al. 2019).

What is missing is consideration of the rationality of romance scammers drawing from data collected from them. Researchers have long argued that offenders make assessments of risk and reward (e.g., Bachman, Paternoster, and Ward 1992; Nagin and Paternoster 1993; Piquero and Tibbetts 1996) and that their decisions and attendant behavior are shaped by these assessments (e.g., Gibbs 1975; Jacobs 1996, 2010). Researchers have yet, however, to explore whether and how similar processes occur among romance scammers. Moreover, understanding of whether and how offenders' behavior is shaped by perceptions of reward is still in its infancy (see Piliavan, Thornton and Matsueda, 1986).

Additionally, while scholars have specified the processes of interpersonal deception (see, e.g., Buller and Burgoon 1996; White and Burgoon 2001, on "Interpersonal Deception Theory" [IDT]), criminologists have devoted only limited attention to exploring the role of these processes in ORF. Interpersonal deception is a reciprocal communicative process wherein interactants use strategic and non-strategic behaviors to elicit desired outcomes from one another

(Buller and Burgoon 1996). These deception processes occur in both face-to-face and computer-mediated interactions (e.g., Carlson et al. 2004; Giordano et al. 2007; Hancock et al. 2007). While a small body criminological research has highlighted that persons committing non-payment email fraud change the character of their emails—specifically the use or non-use of urgency cues—over the progression of the offense (see, e.g., Maimon et al., 2019 & 2020), criminologists have yet to explore how the deception strategies of romance scammers may similarly fluctuate in response to victims' behavior.

In the present study we address these gaps in empirical understanding of romance scams. We explore whether and how these fraudsters alter their exchanges with potential victims in response to varying promises of reward. To do so, we draw data from sequential email exchanges with 94 active romance scammers collected via a randomized experimental procedure and analyze these data using a mixed-method design. Our study advances prior understanding of romance scams by allowing us to make causal inferences regarding fraudsters' behavior using data collected from fraudsters themselves. In doing so, we add to understanding of ORF and contribute more broadly to theoretical understanding of the way reward functions in rational choice. Finally, we further specify the decision-making process of persons committing crimes involving interpersonal deception, such as romance scams, by integrating IDT within the rational choice framework.

Conceptual Background

Online romance scam is one type of online fraud— or instances wherein an individual uses the internet when responding to a "dishonest invitation, request, notification or offer by providing personal information or money [leading] to a financial or non-financial loss" (Cross and Richard 2014:1-2). ORF differs in that it occurs when an individual adopts a fake online

identity to gain a victim's affection and trust. They then use the illusion of a romantic or close relationship to manipulate and/or steal from the victim (FBI, n.d.). These relationships can be established via email or through a variety of websites and apps (e.g., Tinder, E-Harmony, Facebook, Instagram, Google Hangout, etc.) (FTC 2019).

Prior research has demonstrated that ORF typically consists of an interaction between fraudsters and victims occurring over time (Whitty 2015). Fraudsters use persuasive techniques throughout these interactions to develop relationships with victims and then convince them to hand over money. These techniques include fraudsters taking roles as authorities, stoking victims' adherence to social norms (e.g., helping others in need), and imbuing victims with feelings of urgency. They also indirectly influence victims through the visceral feelings stemming from their artificial relationships. Fraudsters will then adjust their techniques in response to victims' reactions to their initial and subsequent persuasive strategies (Whitty 2013). Through these techniques and others, romance scammers obtain financial rewards by having victims send them money directly, by having them make advance payments for promised outcomes or by drawing them into schemes wherein they unwittingly launder money by transferring funds or goods (Galdo, Tate, and Feldman 2018).

Rational Choice

In the rational choice framework, offenders are considered rational actors in that they base their crime-related decisions on assessments of risk and reward (Clarke and Cornish 1985). As perceived risks increase, they are less likely to pursue contemplated crimes (e.g., Nagin 1998; Paternoster 1987); as perceived rewards inflate, they are more likely to undertake them (e.g., Baumer and Guastafson, 2007; Goldstein 1985; Cressey 1953; Loughran et al. 2016).

Research using this framework demonstrates offenders' behavior is influenced by their perceptions of risk and reward. For instance, offenders will sometimes reduce how often or where and when they offend or alter their offending in other ways in response to risk (Gibbs 1975; Jacobs and Cherbonneau 2014). Likewise, offenders will undertake offense opportunities seen as more rewarding than others (e.g., Nagin and Paternoster 1993; Thomas, Loughran, and Hamilton 2020). Additionally, they may also take steps, such as careful target selection, to maximize the perceived rewards from an offense (e.g., Jacobs 2010). Research suggests these processes are influenced by the nature of interactions between perpetrators and victims. For instance, the initial stages of armed robbery are guided by an interplay between robbers' and victims' behavior. Sometimes robbers adopt a "normal appearance" when approaching victims by asking for the time of day or to buy drugs. If victims are duped by these ruses, robbers calmly approach them. However, if victims become suspicious, robbers either abandon the offense or violently rush them (Wright and Decker 1997: 98). Studies of illicit drug sellers and potential buyers show a similar interplay. Drug sellers may avoid selling to potential customers who behave suspiciously during transactions (e.g., Johnson and Natarajan 1995). Sellers may also overcharge or otherwise defraud customers who demonstrate less drug knowledge (i.e., going prices, appropriate terminology) to increase profits (e.g., Jacques, Allen, and Wright 2014).

As mentioned previously, victims' accounts describe how romance scammers will engage in different tactics over the course of the offense (Whitty 2013). Research also argues that fraudsters alter their behavior due to raises in their perceptions of risk (Wang et al., 2021). If viewed through the lens of rational choice, this research suggests that online romance scams consist of a reciprocal interaction between fraudster and victim. Moreover, in this interaction, fraudsters' perceptions of the risks of being identified as predatory by victims and others change

in response to the behavior of potential victims. As these perceptions of risk rise, fraudsters alter their behavior. Although it has been noted that romance scammers are motivated by reward (e.g., Buchanan and Whitty 2014), it is unclear whether they alter their tactics in response to fluctuations in it in the same way they do in response to risk. While the rational choice framework can help explain why romance scammers' decisions and behaviors change in response to reward, it offers little conceptual guidance for understanding the interactive processes occurring between them and victims that may influence these changes. To guide our exploration of these processes, we draw from the Criminal Event Perspective and Interpersonal Deception Theory (IDT).

The Criminal Event Perspective and Interpersonal Deception Theory

The criminal event perspective focuses attention on the microsocial level of illegal behaviors, stressing on the need to study the offenders, victims and the context of interest (i.e., environment) (Meier, Kennedy, and Sacco, 2001). The CEP indicates that victims and offenders converge within the same social context they share, and that is when crime happens (Anderson and Meier, 2004, see also Cohen & Felson 1979). For example, the way offenders or victims present themselves, the reciprocal influence of participants responses and the setting in which these interaction shape the interactive process (Meier, Kennedy and Sacco, 2001; see also, Maimon et al., 2019). When situated it in cyber context, Topalli and Nikolovska (2020) further expanded upon CEP, stressing on the fact that the convergence between cybercriminals, victims and the technological context can be conducive to a happening of a cybercrime incident. A number of prior research has deployed the CEP in explaining violent offenses (e.g., Deibert and Miethe, 2003; Pino, 2005; Chopin and Beauregard, 2020) and online fraud (e.g., Maimon et al., 2019 & 2020). However, this theoretical framework only provides a general framework for

developing future research, but not being cohesive and detailed enough to develop research hypotheses aiming to understand the interactive process of victims and offenders. To fill this theoretical lacuna, the Interpersonal Deception Theory is discussed in the following paragraph to provide useful and thorough information about the interaction between offenders and targets during the progression of a criminal event.

Stemming from communication studies, IDT explains interactions between persons intent on deception (i.e., "deceivers") and those they want to deceive (i.e., "receivers") (Buller and Burgoon 1996). IDT argues that a key feature of these interactive contexts is their dynamic nature. That is, deceivers and receivers are active participants and "adjust to one another's feedback" (206), thereby altering the progression of their interaction. When attempting to deceive others, deceivers may have instrumental (e.g., acquiring resources, etc.), relational (e.g., initiating or maintaining relationships, etc.), or identity (e.g., avoiding embarrassment, etc.) goals. Receivers may also be motivated by various goals, but it is assumed they are always trying to avoid deception. To achieve their respective goals, both parties use strategic and non-strategic behaviors. Strategic behaviors are intentional actions, whereas non-strategic behaviors are unintentional. Because these situations consist of reciprocal exchanges, the strategies used by a deceiver and a receiver will change over the course of the deception event. Moreover, they can be aimed at achieving multiple goals simultaneously (Buller and Burgoon 1996).

Interactions involving deception can be shaped by several factors. First, when people presume that other interactants are credible, they are less likely to assess the behavior of these others for signs of deceit and vice versa. The degree of credibility one lends to another can stem from a prior relationship (Buller and Burgoon 1996) or from a commonly held tendency to enter all interactions assuming others are trustworthy (e.g., Buller and Hunsaker 1995; Kalbfleisch

1992). Regardless of whether interactants enter an interaction with a pre-existing relationship or develop one over the course of it, as the relationship grows in strength—or at least the stronger it is perceived to be—the more likely receivers will fail to recognize or seek out signs of deception. Likewise, the more receivers attribute positive emotions to the relationship, the more likely they will trust deceivers (Buller and Burgoon 1996).

Criminologists have only recently begun to use IDT when examining criminal behavior and cybercrime more specifically. In a study of online non-payment fraud, Maimon and colleagues (2019) found that the deception strategies of the fraudsters engaged in this crime were contingent on the behavior of their targets. They found that the fraudsters were more likely to continue using similar strategies—here cues of urgency—when targets reacted without suspicion. In a separate study using the same sample, Maimon and colleagues (2020) found that these fraudsters were more likely to continue using politeness, sometimes in conjunction with cues of urgency, when targets were deemed suitable. This work highlights that the assertions of IDT regarding deceivers' use of strategic behaviors apply to online fraudsters. Questions remain, however, as to whether these assertions apply to persons committing online romance scams and, moreover, if they can explain the decision-making of these fraudsters from a rational choice perspective.

The Current Study

If considered together, the extant research described previously suggests that IDT can be used to explain the rationality of romance scammers. Romance scams can be conceptualized as an interpersonal deception event occurring between a fraudster and a victim. Over the course of these events potential victims will become more or less suspicious of fraudsters' motives in response to the ways in which fraudsters behave. As they become less suspicious, and thus more

likely to provide fraudsters with some type of financial returns, this raises fraudsters' perceptions of the potential rewards of the crime. Contrarily, as potential victims become more suspicious, this lowers fraudsters' perceived rewards. Fraudsters engage in behaviors, such as acting as authority figures or building relationships with potential victims, to attenuate victims' suspicions and thus raise the chances of reward. Thus, prior research suggests that as fraudsters' perceptions of reward fluctuate due to victims' behavior, they will alter their own behaviors in response.

In the current study, we examine these processes. More specifically, we explore whether and how online romance scammers alter their behavior in response to changes in the likelihood of reward. We suspect that upon receiving clear signs of rewarding cues from victims, this will increase fraudsters' perceptions of reward. In other words, this may increase their views that victims are ready to send rewards and comply with future financial requests. Accordingly, fraudsters may then modify their behavior as a means to increase the chances that victims will do so. We first conduct an exploratory qualitative analysis to identify the strategies used by these fraudsters over the course of their interactions with a "victim." We then test if fraudsters are more or less likely to use these various strategies given several degrees of potential reward operationalized as various email messages.

Data and Methods

Our study is informed by data collected from *stop-scammers.com*. *Stop-scammers.com* is a website where victims of romance scams report the individuals who have defrauded them—hereafter referred to as *fraudsters.* These reports include the fraudster's claimed age, gender, email address, phone number, social media information, and a brief description of each scam. The website only includes information for scammers who claim to be female. Each report undergoes a vetting process requiring supportive documentation before it is posted to the website

(see Wang et al., 2021 for a description). To collect data, we deployed a Python scraper to gather the email addresses of all the fraudsters reported to this site in 2020.[4] We did not scrape for demographic information.

After obtaining the email addresses, we employed an experimental design wherein we randomly assigned 500 of them into three groups. In early 2021 we sent email messages posing as a potential victim to the fraudsters in each group using a program developed in Python. Of these initial 500 emails, 100 were sent to inactive email addresses. Our final sample size (n = 94) consists of all the fraudsters who replied to this first email, with 33 in group 1, 31 in group 2 and 30 in group 3.

We followed the fraudsters' responses to our first email with a series of standardized email exchanges. The schedule and content of our messages are shown in table 19. These emails only differed by experimental group and did not differ due to the content or length of the fraudsters' replies. Email 2 (sent to all 3 groups) was intended to make the fraudsters aware that the victim possessed a gift card (i.e., a potential reward) and, moreover, that "he" could be potentially persuaded as to what to do with it. We then began varying the degrees of potential reward in email 3. For group 1, the degree of potential reward was slightly raised by asking for their opinion on what to do with the aforementioned gift card. For groups 2 and 3, we significantly raised the degree of reward presented to the fraudsters by indicating that the victim wanted to give them the gift card.

Table 19. Experimental Procedure

	Group 1: placebo control group	**Group 2: control group**	**Group 3: treatment group**

[4] Our full research design was approved by the Georgia State University Institutional Review Board (IRB).

Table 19. Experimental Procedure (continued)

Email 1	Hi. I'm John. I saw your profile on <INSERT NAME OF *FIRST* PLATFORM LISTED ON WEBPAGE>. I don't like using platforms to talk, so searched for an email. I'm quite the internet stalker! Are you the same person on that platform? Sorry if not. A little about me: I'm 28 and live in Chicago. I work for Delta so travel a lot, domestic and international, so like to meet people in new places. Hopefully the pandemic will be over soon, so things go back to normal! If you're single and ready to mingle, write me back!		
Email 2	I'm so excited! My birthday is coming up and my parents just gave me a $250 Amazon gift card!!!!!!! The only problem is I don't know what to spend it on!		
Email 3	I've been thinking hard about what to do with that Amazon money. I really need new cookware. What do you think?	I've been thinking hard about what to do with that Amazon money. I really need new cookware. But I'm a big believer in karma, so I'd like to give you some of it. What do you think?	
Email 4 + E-Card	I'm sending you an e-card with money for Amazon! Please confirm you get it. I don't know why, but they always go into my junk mail.		
	Send a hallmark e-card with: "Been thinking of you and so sending you this special message! I hope it makes you happy!"	Send nothing	Send an Amazon e-card with $1 with: "Been thinking of you and so sending you this special message! I hope it makes you happy!"

Email 4 consisted of two parts for each group. First, each group received a message. Then each group received a varying level of reward. For group 1 (NM), we did not alter the level of the reward presented in our message. We then sent them a hallmark e-card with a short message (i.e., no reward). For groups 2 and 3, we again raised the level of presented reward by promising to send them the gift card (PR). Next, we varied the level of treatment between the two groups. Group 2 received nothing (RN). Group 3 received a $1 and a short message (MR$1).

Analytical Plan and Measures

We employed qualitative-quantitative mixed method analytical approach in this study (see Maruna 2010). We first conducted an inductive qualitative analysis intended to distinguish the conceptual domains comprising the fraudsters' replies. We then quantitatively assessed whether these domains significantly differed over the course of our email exchanges with the fraudsters.

Qualitative Analysis

In our qualitative analysis, we organized the conceptual links between the domains and subdomains in our data using the qualitative software program NVivo. We first explored the data for patterns within and across the email exchanges with the fraudsters. We sorted similar statements and language into general domains (e.g., statements about personal identity) before distinguishing more precise similarities and differences within these domains (e.g., sharing personal information, sharing personal qualities). This analysis identified seven key emergent themes: *1) fraudster's personal identity, 2) victim's identity, 3) relationship with victim, 4) ask for, demand or accept money, 5) ask for personal information, 6) request to talk or chat,* and *7) interactional facilitators*. These themes inform our qualitative findings and were guided our quantitative analysis. Our qualitative analysis also revealed an eighth thematic category comprised of fraudsters' references to receiving the money or saying thanks for it. This domain was omitted from our analysis as it was only present in the fraudsters' responses to our fourth email, and we determined it had little theoretical relevance.

Quantitative Analysis

Our quantitative analysis examined the following variables derived from the qualitative analysis: *1) fraudster' personal identity, 2) victim's identity, 3) relationship with victim, 4) ask*

for, demand or accept money, 5) ask for personal information, 6) request to talk or chat, and *7) interactional facilitators*. Each variable received a number identifying which email it was present in (e.g., fraudster's identity 1 referred to the presence of the variable after email 1). Variables were coded 1 if present and 0 if not.

We examined the data using Fisher's Exact test for differences in the variables' presence between the emails. This test determines whether there is an association between two dichotomously measured categorical variables (e.g., sex, occupation) (Sage 2017:2) Fisher's Exact test is best suited for small samples (< 1,000 cases) because it does not rely on distributional assumptions. We chose Fisher's Exact test because the Chi-Square test should not be used when the smallest expected number of the sample size is less than 5 and the total sample size is less than 20 (Kim 2017; Cochran 1954). In our dataset, the smallest number of responses can be as low as 18 and 20 (group 1 and group 2 in email 4; group 2 in email 3).

Qualitative Findings

Our qualitative analysis revealed that the fraudsters' responses contained seven conceptually distinct domains. First, the fraudsters took subtle and overt steps to shape the presentation of their *personal identities*. They also crafted their responses such that they could alter the *victim's identity* or how the "victim" viewed his own identity or the *victim's identity*. Next, their responses suggested a *relationship* with the victim. Fourth, the fraudsters *asked for, demanded, or accepted money*. In the fifth and sixth domains, the fraudsters *asked for identifying information* from the victim or to *talk or chat* with him further via another platform. Finally, the fraudsters' responses also contained *interactional facilitators*, or innocuous text encouraging the victim to continue the exchange. It is important to note that the fraudsters' communications were multi-functional in that they often consisted of one or more of these domains acting in concert. In

what follows, we describe these domains and illustrate them with excerpts from the fraudsters' responses to our emails.

Personal Identity

All the fraudsters' presented themselves as persons who, at least ostensibly, were "real" persons and not out to victimize the "victim" in some way. They first did so by sharing personal information such as their names, ages, marital and familial statuses, where they lived, and in a few cases, photographs of "themselves." Mary's initial response exemplified this strategy. "I am Mary," she stated, "but you can call me Bae for short 30 years old single with no kids and never been married before…I was born and raised in the USA Texas (city in Houston)."[5] A few also shared their personal qualities. Angela noted that she was a "habitual early bird" and was "pretty at heart," while Janet "believe[d] in open communication, standing in our truth, being honest, and having integrity."

The fraudsters also presented their identities by emphasizing they were persons looking for relationships. Monica claimed she was "ready for a new love relationship." Kate wrote she wanted to "have a serious relationship with a serious man." They also others sometimes stated the qualities they desired in a relationship. Mary Lloyd claimed she was looking for "true love." Janet was more verbose:

> *I am looking for a man that will be able to listen to me, communicate his feelings to me, make me laugh, hold and comfort me in need, stand by my side, respect me, passionate lover in every way, support me in every way*

[5] Quotes from the fraudsters' responses are presented verbatim and, as such, contain uncorrected spelling and grammatical errors.

Many also presented themselves as persons interested in our "victim." Linda stated, "I really wanna know you more better dear." Others asked more general questions such as "how has been your day?" (Sara). Once money was introduced into the exchanges, some of the fraudsters framed themselves as interested in "helping" spend the money. Linder said, "Scratch the amazon gifts card with the full receipt and send it here to my email address and I will help you with it.".

Finally, the fraudsters identified as "non-scammers" by distancing themselves from persons committing romance scams or, in their words, "scammers." Elizabeth did so by stressing wariness that our "victim" was out to defraud her. "If you are a scammer or if you are here for my nudes," she said, "don't try talking to me anymore because I heated and detest these two things." Daniela echoed this, "If you are a real person not imposter (African Nigerians) or scammers (soldiers, conman, fraudster) then we can mingle." She continued, "I'm not an online scammer after any man's money."

Throughout these different and often overlapping forms of communication, the fraudsters presented themselves as "real" people. If viewed through an interactionist lens, in doing so they shaped how our "victim" would view them throughout the interaction (see Goffman 1957). By painting a picture of themselves as "real" people looking for a relationship or wanting to help our "victim," they also symbolically distanced themselves from how they did not want our "victim" to see them: as potential fraudsters. If viewed through the perspective of IDT, doing so could also contribute to our "victim" seeing them as more credible by increasing the amount of knowledge he had of them (Buller and Burgoon 1996).

Victim's Identity

Each of the fraudsters also took subtle steps to alter how our "victim" saw himself. They did so in two primary ways. In the first, they used flattering language. Bella stated she had "a

feeling that you are an honest person and courageous." Following the introduction of money, Linda (group 3) stated, "I guess you're a responsible man lol." With such flattery, the fraudsters may have been attempting to encourage the "victim" to see himself as attractive or as possessing other desirable traits. The high emotional response initiated by this can then override the victim's ability to objectively assess the risks of sharing information or otherwise continuing to interact with a fraudster (Cialdini 1984; Lea et.al 2009).

The second way the fraudsters focused on the "victim's" identity was by giving him decisive power. Their statements were worded such that they could be interpreted by the "victim" to mean that the direction of their interaction was up to his discretion. For example, when asking for identifying information—a tactic we describe shortly—the fraudsters would do so without using imperative statements. They would instead request this information with terms such as "can" or "maybe." Most would simply ask "can you send me some pics of you?" (Rachael). Some, like Stantel, were less imperative. "I guess we can share pictures," she wrote, "if you don't mine then or what do you think about that…"

The fraudsters wrote similarly when discussing money. Rather than directing the "victim" to send them money they would instruct him to spend it as he saw fit. "Well you can use it to buy things for you," Lailatul wrote. Some "suggested" he send them the money:

> *Whatever pleases you it's your money and you can do whatever you want with it okay or Perhaps you can cash it out and buy your cookware and also buy another card with the rest of the money and send to me as a sign of your real love to me (Elizabeth)*

Although subtle, linguistic choices such as these are important because their use in communication can indicate to a recipient that he or she has the decisive power to carry out or follow through with a suggested action. This can then alter how the recipient sees his or her own

identity in relation to that of the person or persons with whom they are interacting (see Weinstein and Deutschberger 1963 on 'altercasting'). The sense of power or status it can lend may cause a recipient to see the other interactant as less threatening (Kemper and Collins 1990; Scherer 1984). In the situational context of romance scams, this may cause potential victims to discount the level of risk or threat they would otherwise attribute to potential fraudsters during their interaction. If, in the terms of rational choice, this resulted in a potential victim's perceptions of risk being lowered, the victim may be more likely to continue facilitating the offense—here by continuing to interact with the fraudster—rather than cutting it short.

Relationship

The fraudsters also used language aimed at shaping the "victim's" perception of their "relationship." For some, this involved statements hinting at a potential future relationship. Janet stated, "Am gonna be happy to meet you in person very soon and see how things go from there…we can be the perfect match." Lailatul echoed this, commenting, "I will love to chat you more and know more about each other and see where it will lead us to." Others indicated a preexisting relationship with the "victim." For instance, referencing the "victim's" birthday, Sara wrote, "we make food for you and your friends…I'll come over and celebrate that together." While Elizabeth wrote, "know that baby I am always here for you."

The fraudsters also did so by peppering their exchanges with terms of endearment or "pet names." These included "dear," "honey," "babe," "my love," and "baby." The use of these terms may at first seem like meaningless filler. It is important to note, however, that the use of "pet names" are keyways that individuals suggest affection or social closeness with others (see Drake 1957; Ezebube et al. 2020). Hence, fraudsters' use of pet names could be interpreted by victims as indicative of the presence of a relationship.

In suggesting a future or current relationship, fraudsters may shape how potential victims define their interaction or situation with fraudsters. That is, if a potential victim begins to view his or her relationship with a fraudster as being meaningful or possibly developing into this, he or she may interact differently with the fraudster. As Buller and Burgoon (1996) argue, trust flows from intimacy. Therefore, while a potential victim may be wary and distrustful of a fraudster viewed as a stranger, he or she may act contrarily with a fraudster viewed relationally closer. And this, in turn, may make it easier for a fraudster to defraud the victim in some way.

Ask for, Demand, or Accept Money

The fraudsters also attempted to persuade the "victim" to take several types of action throughout the exchanges. Key among these was to send them money. For many, this involved orders to provide them with the previously mentioned gift card. They would make statements such as "Send the card to my DM" (Jeana) or "Send me the picture of your card" (Brenda). Others were less commanding and used the softer language previously discussed. They gave the "victim" power to decide whether to send them money. Some justified these imperative or passive statements with their financial needs. Aminatu wrote, "I think I will need one of it to update my phone to be able to chat here on email whenever we want." Stella was "very happy to use it for some stuffs." And Sara stated, "get me 50 out of the Amazon gift card so I could be a gas [gas tank emoji] and drive down to you." Finally, after being told they would receive the "e-card with money for Amazon," (email 4PR), many of the fraudsters' passively accepted the money. It was common for them to simply state "Okay" (Angelina). Some of them added to this with comments that they were "waiting" (Mary) or with questions like "how are you sending it?" (Aminatu).

Identifying Information

At some point each of the fraudsters also encouraged the "victim" to send them identifying information. As noted previously, for many this involved demands or requests for photographs of "him." Others wanted more information, such as his age, profession, marital status, familial status, phone number, and place of residence. Sometimes they outright requested this information. Naya wrote, "Where are you from and what is your profession?" As with their requests for photos the fraudsters embedded these requests in comments seemingly directed at shaping their identities, the "victim's" identity, or their relationship. For instance, Lailatul responded to email 2 like this: "Well you can use it to buy things for you…What is your name?"

Such information may be important to fraudsters because it could be used to steal the identities of victims and then defraud them. But it could also be used to further fraud in a more indirect way. The fraudsters could take such information and use it to liken their presented identities to those of their potential victims. Doing so can increase victims' feelings of connection with a fraudster. Such emotions can then "viscerally influence" (Loewenstein 1996) victims' decision-making such that they are less able to effectively weigh potential risks (see also, Whitty 2013). This, in turn, may then facilitate a fraudster's ability to defraud the victim.

Request to Talk or Chat

A third action the fraudsters encouraged the "victim" to take was to talk or chat with them via a separate platform, such as WhatsApp or Google Hangouts, or to do so by text message or phone call. They did so with statements or questions such as, "Can we chat on Google Hangouts now?" (Grace) and "Do you do Hangout or send me your text number" (Cassandra). Sometimes they further attempted to persuade the "victim" to do so with the

pretense that it would facilitate his abilities to “chat better” (Annabelle, Rita) or “talk better” (Kate, Joyce) and “take time to know each other better” (Stella).

Interactional Facilitators

Finally, throughout their communications all the fraudsters made statements or posed questions urging the “victim” to continue corresponding with them or to respond faster. Most would ask questions such as “How are you doing today?” (Mary) or “Hello John are you here with me now?” (Grace). Following the promise of sending them money (email 4PR) or of their receipt of one dollar (email 4MR$1), they would also pose questions such as “Am waiting. Let me give it try. You there?” (Lizzy) and “Why only 1 dollar?” (Ashley). While on their face these comments and questions may seem innocuous or even genuine, given that the fraudsters used them following the lack of timely response to their emails it is likely that they were intended to make the “victim” aware they were awaiting a response.

Quantitative Analysis

To examine group differences regarding the use of the different domains, we used two-sided Fisher’s Exact Test analysis. Results are presented in table 4, 5 and 6 and 7.

Personal Identity

Table 20 presents the three significant results on the use of *personal identity* across the four emails. First, there is a marginally significant difference between the fraudsters’ use of this domain between email 1 and email 2 ($p<.010$). They are also more likely to use it in email 2 than in email 3 to group 1 ($p<0.05$). Lastly, fraudsters are significantly more likely to present their personal identities more so after email 4(PR) when they are promised a reward than when they receive nothing (email 4RN) ($p<0.05$).

Table 20. Personal Identity

	Email2=0	Email2=1	Fisher's Exact *P* value	Email 3 G1=0	Email 3 G1=1	Fisher's Exact *P* value	Email4 RN=0	Email4 RN=1	Fisher's Exact *P* value
	N=61 (0.65)	N=11 (0.12)		N=58 (0.76)	N=1 (0.013)		N=60 (0.95)	N=0 (0)	
Email1 (0/1)	N=14 (0.15)	N=9 (0.10)	0.065 †						
Email2 (0/1)				N=14 (0.18)	N=3 (0.04)	0.33*			
Email4 (PR) (0/1)							N=2 (0.032)	N=1 (0.016)	0.048*

Note: numbers in the bracket stands for the probability
PR: stands for fraudsters in email 4 who were promised to receive money from the "victim"
RN: stands for fraudsters in email 4 who were promised to receive money from the victim but receive nothing
MR$1: stands for fraudsters in email 4 who were promised to receive money from the victim and receive $1 from the victim
NM: stands for fraudsters in email 4 who received only a hallmark of the e-gift card
†p ⩽ 0.10, *p ⩽ 0.05, **p ⩽ 0.01

Victim Identity

In table 21, we observe two significant results regarding fraudsters' use of *victim identity* across the four emails. This domain is significantly more present following email 3 (to groups 2 and 3) than after email 4 (MR$1) ($p<0.01$). It is also more present when fraudsters are promised the reward (email 4PR) than after they receive $1 (email 4MR$1) ($p<0.01$).

Table 21. Victim's Identity

	Email4 MR$1=0	Email4 MR$1=1	Fisher's Exact *P* value	Email4 MR$1=0	Email4 MR$1=1	Fisher's Exact *P* value
	N=55 (0.87)	N=0 (0)		N=61 (0.97)	N=0 (0)	
Email3 G2&G3 (0/1)	N=7 (0.11)	N=1 (0.016)	0.01**			
Email4(PR) (0/1)				N=1 (0.016)	N=1 (0.016)	0.009**

Table 21. Victim's Identity (continued)

Note: numbers in the bracket stands for the probability
PR: stands for fraudsters in email 4 who were promised to receive money from the "victim"
RN: stands for fraudsters in email 4 who were promised to receive money from the victim but receive nothing
MR$1: stands for fraudsters in email 4 who were promised to receive money from the victim and receive $1 from the victim
NM: stands for fraudsters in email 4 who received only a hallmark of the e-gift card
†p ≤ 0.10, *p ≤ 0.05, **p ≤ 0.01

Relationship with Victim

Table 22 shows three significant differences in the *relationship with the victim* domain across fraudsters' responses to our four emails. First, fraudsters are significantly more likely to use this strategy after email 3 (to groups 2 and 3) than after they are promised the reward in email 4PR ($p<0.05$). There is also a marginally significant difference between the presence of this domain in email 3 (to groups 2 and 3) than in email 4(RN) (when fraudsters are promised reward but receive nothing) ($p<0.10$). Lastly, a marginally significant relationship exists between fraudsters' use of this domain in email 4PR than after receiving $1 (email 4MR$1) ($p<0.10$).

Table 22. Relationship with the Victim

	Email 4 PR=0	Email 4 PR=1	Fisher's Exact *P* value	Email 4 RN=0	Email 4 RN=1	Fisher's Exact *P* value	Email4 MR&1=1	Email4 MR&1=0	Fisher's Exact *P* value
	N=55 (0.87)	N=2 (0.03)		N=57 (0.90)	N=0 (0)		N=59 (0.94)	N=0 (0)	
Email3 G2&G3 (0/1)	N=4 (0.06)	N=2 (0.03)	0.042 *	N=5 (0.08)	N=1 (0.16)	0.095†			
Email4 (PR) (0/1)							N=3 (0.05)	N=1 (0.16)	0.063†

Table 22. Relationship with the Victim (continued)

Note: numbers in the bracket stands for the probability PR: stands for fraudsters in email 4 who were promised to receive money from the "victim" RN: stands for fraudsters in email 4 who were promised to receive money from the victim but receive nothing MR$1: stands for fraudsters in email 4 who were promised to receive money from the victim and receive $1 from the victim NM: stands for fraudsters in email 4 who received only a hallmark of the e-gift card †p ≤ 0.10, *p ≤ 0.05, **p ≤ 0.01

Ask for, Demand, or Accept Money

In this domain, there are eight significant results on fraudsters' use of the ask for, demand, or accept money (ADAM) domain across the different emails. First, fraudsters are significantly more likely to use ADAM after email 2 than after email 4(PR) ($p<0.05$). Second, fraudsters in groups 2 and 3 are significantly more likely to use this strategy after email 3 than fraudsters in group 1 after the same email ($p\leq 0.001$). Third, fraudsters in group 1 are significantly more likely to use ADAM after email 3 than after email 4(NM) ($p<0.001$). Fourth, fraudsters in group 2 and 3 following email 4 (PR) are significantly more likely to refer to ADAM than those in group 1 subsequent to email 3. Fifth, sixth, and seventh, fraudsters in groups 2 and 3 are significantly more likely to rely on ADAM as a strategy after email 3 than after email 4(NM) ($p<0.01$), email 4 (RN) ($p<0.01$), and email 4(PR) ($p \leq 0.001$). Eighth, fraudsters' responses to email 4(PR) are more likely to include ADAM than those to email 4(RN). It is important to note that these latter two relationships are marginally significant ($p<0.10$).

Request to Talk or Chat

Table 23 reveals three significant results on fraudsters' use of the *requests to talk or chat* domain across the different emails. The fraudsters in group 1 are more likely to use this strategy than those in group 2 and 3 after email 3 ($p\leq 0.10$). Furthermore, fraudsters are significantly

more likely to *request to talk or chat* following email 4(PR) than after receiving a $1 (email 4MR$1) ($p<0.05$) or after receiving nothing (email 4RN) ($p<0.05$).

Table 23. Request to Chat on Private Platform

	Email3 G2&3=0	Email3 G2&3=1	*P* value	Email4 MR$1=0	Email4 MR$1=1	*P* value	Email4 RN=0	Email4 RN=1	*P* value
	N=37 (0.49)	N=0 (0)		N=60 (0.95)	N=0 (0)		N=60 (0.95)	N=0 (0)	
Email1 (0/1)	N=35 (0.46)	N=4 (0.05)	0.01†						
Email4 (PR) (0/1)				N=2 (0.032)	N=1 (0.016)	0.048*	N=2 0.032	N=1 0.016	0.048†

Note: numbers in the bracket stands for the probability
PR: stands for fraudsters in email 4 who were promised to receive money from the "victim"
RN: stands for fraudsters in email 4 who were promised to receive money from the victim but receive nothing
MR$1: stands for fraudsters in email 4 who were promised to receive money from the victim and receive $1 from the victim
NM: stands for fraudsters in email 4 who received only a hallmark of the e-gift card
†p ⩽ 0.10, *p ⩽ 0.05, **p ⩽ 0.01

Interactional Facilitators

Table 24 presents two significant results on the *interactional facilitators* domain across fraudsters' responses to the four emails. First, fraudsters are significantly more likely to use *interactional facilitators* following email 2 than after email 4NM ($p<0.05$). In addition, fraudsters are also significantly more likely to use this strategy when there is a promise of reward (email 4PR) than when they receive nothing (email 4RN).

Table 24. Interactional Facilitators

	Email4 NM=0	Email4 NM=1	Fisher's Exact *P* value	Email4 RN=0	Email4 RN=1	Fisher's Exact *P* value
	N=52 (0.83)	N=2 (0.03)		N=58 (0.92)	N=1 (0.016)	
Email2 (0/1)	N=6 (0.10)	N=3 (0.05)	0.018*			

Table 24. Interactional Facilitators (continued)

Email4(PR) (0/1)		N=2 (0.03)	N=2 (0.03)	0.009*
Note: numbers in the bracket stands for the probability PR: stands for fraudsters in email 4 who were promised to receive money from the "victim" RN: stands for fraudsters in email 4 who were promised to receive money from the victim but receive nothing MR$1: stands for fraudsters in email 4 who were promised to receive money from the victim and receive $1 from the victim NM: stands for fraudsters in email 4 who received only a hallmark of the e-gift card †p ⩽ 0.10, *p ⩽ 0.05, **p ⩽ 0.01				

Asking Identifying Information

No significant results are observed for the asking identifying information domain across different emails.

Summary of Results

Put simply, fraudsters are more likely to present their personal identities after the introduction of a potential victim than when reward is introduced to the interaction. They are also more likely to do so after reward is introduced than when it is indicated that the victim is amenable to persuasion. Finally, they are more likely to use this strategy following the promise of a reward than after they received nothing.

Concerning manipulating victims' identity, fraudsters are more likely to attempt to do so after the victim wants to give them a reward than after they receive $1. Likewise, they are also more likely to do so after they are promised the reward than after they receive $1. Furthermore, fraudsters are more likely to refer to their relationship with the victim it is suggested the victim wants to give out reward than after they are promised the reward but receive nothing. Similarly, fraudsters are more likely to use this strategy when there is a promise of reward than when they receive $1.

In addition, fraudsters are more likely to use ADAM when they are made aware of the presence of a potential reward than after they are promised one. Likewise, they are more likely to include this domain in their responses when victims indicate their intentions to give fraudsters money than when asked their opinion on what to do with money, when they only receive images of the reward, after they are promised the reward, or after they receive nothing. Moreover, fraudsters are more likely to use this strategy after they are asked their opinion on what to do with money than after they receive an image of the reward or after they are told they are receiving money. Lastly, fraudsters that are promised reward are more likely to use ADAM after they are told they are receiving it than after they receive nothing.

Again, when the victim initiates the first interaction, fraudsters are more likely to request to talk or chat than when the victim has the intention to give out reward. Fraudsters are also more likely to request to talk or chat in email 4 when there is a promise of reward than after they receive $1 or receive nothing.

Lastly, fraudsters are more likely to use interactional facilitators after the money is first introduced in the conversation than after receiving only a hallmark image of a gift card. They are more likely to do so if they are promised a reward than if they receive nothing.

Discussion

The aim of this article was to examine if and how romance scammers alter their behavior in response to changes in the chances of receiving rewards from potential victims. Broadly speaking, our analysis reveals that romance scammers do indeed alter the shape of their interactions with victims due to fluctuations in potential reward. Our qualitative thematic analysis suggests that romance scammers' communications with potential victims are multifaceted and can simultaneously include up to seven types of deception strategies:

presentations of their personal identities; manipulations of victims' identities; manipulations of their "relationships" with victims; the asking for, demanding, or accepting of money; requesting identifying information from victims; requesting to talk or chat with victims on other platforms; and attempts to encourage victims to continue interacting with them.

Our quantitative analysis shows that online romance scammers change the degree to which they use certain strategies in response to fluctuations in the level of presented reward. For some strategies, such as *personal identity* and *relationship with victim*, as reward increases, fraudsters are less likely to use them. For others, such as *asking for, demanding, or accepting money*, at times fraudsters use them less when reward is increased and at others, they use them less when it is decreased. Finally, for all strategies, save *asking identifying information*, the fraudsters are more likely to use them when the potential of reward is highest (i.e., after being promised the reward) than after receiving either a hallmark image, nothing, or $1.

Our findings are important for several reasons. First, they add to current understanding of online romance scams. As noted previously, prior work on this offense, drawing primarily from victims' accounts, has highlighted its prevalence (Whitty and Buchanan 2012), impacts on victims (Buchanan and Whitty 2014; Whitty and Buchanan 2016), stages (Whitty 2015), and the techniques used by fraudsters (Whitty 2013). To our knowledge, our study is the first to examine online romance scams through analysis of data collected from fraudsters themselves. Moreover, it is the first to use an experimental design to determine whether and how fraudsters respond to changes in the presentation of rewards. Our findings that fraudsters alter their behavior—by changing the number of words they use and the degree to which they use deceptive strategies—in response to that of their victims adds to this body of research by demonstrating that they, like

persons involved in other types of offenses (see, e.g., Cornish and Clarke 2014), are rational actors. That is, online romance scammers guide their decisions by weighing risks and rewards.

These findings also add to the rational choice perspective more broadly by further explicating the role of reward in decision-making. Piliavan and colleagues (1986) noted some time ago that studies of rational choice to that point had largely failed to include measures of reward. Since that time, however, researchers have addressed this shortcoming and have begun to examine the role of reward in rational choice. For instance, we now know that the impact of rewards on decision-making varies across and within individuals over time (McCarthy 2002; Paternoster and Pogarsky 2009). Researchers have also argued that the presence of co-offenders can influence one's perceptions of reward (McGloin and Thomas 2016), that expectations of reward influence whether one will continue an offense (Pezzin 1995), and that perceptions of reward might be the most important element driving decision-making (Matsueda et al. 2006). And, as mentioned previously, offenders will also take steps to increase the chances of receiving a reward (e.g., Wright and Decker 1997). Our study contributes to this body of literature by suggesting that offenders—here romance scammers—will alter their behavior in response to changes in the likelihood of receiving a reward that occur over the course of an offense as a means to further increase the chances they will receive this reward. Thus, like assessments of risk, the weighing of reward is a dynamic process consisting of an interplay between offenders' perceptions of reward and their behavior.

Our study also furthers understanding of rational choice as it occurs among offenders involved in interpersonal crimes by demonstrating how CEP and IDT can be situated within this perspective. The findings reported in this chapter emphasize the relevance of the criminal event perspective in understanding the behavioral changes of fraudsters in online romance scams, and

expand the current body of literature in CEP focusing specifically on the context of violent crime and online fraud in general (e.g., Pino, 2005; Maimon et al., 2019 & 2020). Moreover, recall that IDT proposes that interpersonal deception situations consist of reciprocal interaction between a deceiver and a receiver wherein each party uses strategic behaviors to achieve their desired ends (i.e., deceiving and avoiding deception, respectively) (Buller and Burgoon 1996). Our analysis demonstrates that as potential romance scams victims indicate less or more certainty of reward (i.e., the presence of money to give, the willingness to give it) to fraudsters, fraudsters respond by using different tactics intended to encourage victims to provide the reward. In the terms of rational choice, this indicates that the fraudsters are acting on the basis of their assessments of potential rewards. The propositions of IDT then explain that the fraudsters base these assessments on the behavior of the potential victims and, moreover, that the changing of these assessments (as indicated by the changes in the fraudsters' behaviors) over the course of the offense is due to reciprocal interaction with the victims. Thus, not only is offender decision-making dynamic, as originally proposed by Clarke and Cornish (1985), but in some crimes this dynamic process consists of a reciprocal interplay between offender and victim.

Prior research on online romance scams has noted that a key strategy used by romance scammers is to manipulate their victims' perceptions of a relationship with them (Whitty 2013). We find that the fraudsters in our sample are no different. Throughout their interactions with our "victim," many of them took measures to give the impression of a relationship with "him." Recall that Buller and Burgoon (1996) argue that receivers may have a more difficult time detecting deception from others with whom they have relationships. They argue this stems from "positivity and truth biases" associated with familiar relationships that cause receivers to "overlook, discount, or misinterpret evidence of deceit" (p. 215). We thus argue that IDT

provides one explanation for why online romance scammers rely on manipulating victims' perspectives of their relationship as a key strategy. Beyond this, however, we also contend that this strategy can also be explained using notions from rational choice and prospect theory, a decision-making theory stemming from behavioral economics.

Limitations

Although our research design allows us to state whether the behaviors of romance scammers can be influenced by the change of reward, as with all research it has several limitations. First, we recognize that it is possible that two or more of the email addresses in our sample may be controlled by the same individual. If this is the case, it may call the validity of our study into question. Second, despite the steps we took to confirm the authenticity of the reports on *stop-scammers.com*, some of the email addresses that we messaged may have been inappropriately listed on the website, which may also contaminate the validity of our findings. However, if non-fraudsters were included in our sample, this would deflate, rather than inflate, the findings presented. Third, our validity may be similarly contaminated if the romance scammers we contacted viewed our initial emails as suspicious or unusual and, as a result, did not respond as they typically would when conducting an email fraud. Hence, it is possible in some cases we were unable to observe natural responses from fraudsters. Fourth, the generalizability of our results is unknown. Our results may only apply to the fraudsters sampled in the study and thus may not apply to fraudsters who use male personas, those running other types of romance scams (e.g., crypto-romance scams), or those operating on different websites or apps. It is possible other types of romance scammers employ different strategies to manipulate victims or may respond to changes in rewards differently. Nevertheless, despite these limitations, our study makes strides in further specifying some of the factors—here financial reward—that shape online romance scammers' behavior. In doing so, it contributes to understanding rational

choice as it relates to online romance scams and to the role of reward in this theoretical framework more broadly.

Chapter IV: Neutralizations, Altercasting and Online Romance Scams

Abstract

In the present study we draw from data collected from 87 online romance fraudsters to explore whether and how offenders may suggest neutralizations to victims as a means to facilitate their crimes. Through thematic analysis of a series of emails exchanged with each fraudster we find that they encourage victims to neutralize their misgivings about sending them money in four overlapping ways. First, fraudsters appeal to vicarious necessity or implore victims to consider the fraudsters' needs. They also appeal to an intimate relationship or suggest victims view their relationship as intimate in nature. Third, they use more straightforward altercasting strategy, for example the admitting of religious, in which they encourage victims to consider their own religious identities. Fourth, they also deny victims' powerlessness by allowing themselves to hold more power during the interaction. Finally, fraudsters also use strategies to altercast the context of interests containing deceptive cues into the one with potential rewards and opportunities. Our study contributes to understanding of neutralizations by explicating how neutralizations can be used by offenders as tools to assist their offending. It also adds to knowledge of the relationship between neutralizations and altercasting. In addition, we expand prior work illustrating the grooming process of online romance fraud and other crimes. We discuss implications for victim-blaming as it occurs among online romance fraud victims.

Introduction

Neutralizations are among the most studied theoretical concepts in criminology (Maruna & Copes 2005). Initially observed among juvenile delinquents (Sykes & Matza, 1957), researchers have since explored neutralizations as they are used by juveniles and adults involved with a range of actions, criminal and otherwise (e.g., Agnew 1994; Bohner et al. 1998; Copes

2003; Burkey & Bensel 2015; Holt & Copes 2010). The lion's share of this work examines how individuals use neutralizations to assuage actual or anticipated guilt stemming from actions they see as immoral or deviant and to thereby maintain positive self-identities (e.g., Benson 1985; Byer et al., 1999; Fritsche 2002; Minor 1981; Stadler & Benson 2012). A smaller body of work also highlights that individuals use neutralizations and other aligning actions, such as disclaimers and accounts (see Hewitt & Stokes 1975; Scott & Lyman 1968), to alter the ways others view them, or their social identities (e.g., Topalli 2005; Fritsche 2002; Jacobs & Copes 2015). For example, this can be seen from scholars' assessment of white-collar criminals (e.g., Chibnall and Saunders, 1977) and military officers' justifications in their sexual exploitation against women (e.g., Copley, 2014). In doing so, they manipulate the ways interactants would otherwise treat them (Sitkin & Bies, 1993).

Victims also use neutralizations to make sense of their victimization experiences (e.g., Agnew 1985). Through neutralizations, victims alter the ways they view their victimization and their roles in these experiences (e.g., Ahmed et al. 2001; Maruna & Copes 2005). This facilitates their abilities to maintain dignified self-identities and avoid shame and guilt (Agnew 1985). In some cases, such neutralizations also alter how victims perceive the persons that have harmed them and thereby facilitate victims' continued involvement or relationships with these victimizers (e.g., Ferraro & Johnson 1983; Weiss 2009; Higginson 1999).

Research on police interviewing has demonstrated that police officers also rely on neutralizations when attempting to elicit confessions from suspects. In short, officers using the Reid technique will introduce possible neutralizations for suspects' actions while interviewing them. Officers do so with the intent these suspects will then identify officers as likeminded persons who also consider the introduced neutralization as an acceptable justification for the

crimes, they are suspected of committing and, because of this, see their criminal actions as justified (e.g., Copes et al. 2007; Leo 1996). Put differently, officers will "give" neutralizations to interviewees in order to encourage them to take actions—here, confessing crimes—they otherwise would not.

Scholars in interactional sociology also emphasized on the fact that when expectations from an actor can be effectively transmitted through subtle, unconscious, sometimes nonverbal processes to another interactant, such a communication process is likely to involve "altercasting" – in other words, through labeling person into the role implied by the identity attribution (Weinstein & Deutschberger 1963; Felson 1978; Board, 1976). During the process of altercasting, one way the enforcers can use to control the directions of events is to offer accounts to recipients, which can altercast certain favorable identities that ultimately facilitating the event (Goffman, 1959; Blumstein et al. 1974; Scott and Lyman 1968). In doing so, by presenting the story-like constructions of events, including plot, story and attributions (Harvey et al., 1990a; Orbuch et al., 1993), enforcers can cause recipients to reconsider how they should view themselves during the interaction and the lines of action they can take (Felson 1978).

Thus, extant research illustrates that victims use neutralizations to manage their identities and that individuals may offer neutralizations to other interactants as a way to manipulate their actions. What has yet to be examined is whether and how potential offenders may provide neutralizations to potential victims as a means to manipulate their (victims) behavior such that it facilitates their (victims) own victimization. In the present study, we address this lacuna in the literature by examining the neutralizations a group of 87 active online romance fraudsters incorporate into their interactions with a victim both before and after they are presented with potential rewards. In doing so, we discuss how the prodding or nudging neutralizations help

facilitate online romance fraud by altering the way potential victims see themselves, and thus the actions they may take, when interacting with potential fraudsters.

Our study first contributes to understanding of how neutralizations can be used by offenders as tools to facilitate their offending. Additionally, the observations of our study further complement the current understanding of victims' use of neutralizations under the influence of offenders' persuasive techniques in cyberspace. Finally, it adds to the understanding of the stages of online romance fraud, specifically with respects to specify the inner-working process of identity-altercast among victims during the grooming process.

Neutralizations and Accounts

Sykes and Matza (1957) posited the concept of neutralizations as a way to explain how juvenile delinquents paradoxically violate norms, they hold yet seem to exhibit little or no guilt afternoon. In short, they argue that delinquents assuage anticipated or actual guilt by using neutralization techniques to maintain a strong bond with society and preserve their images as law-binding citizens (Sykes & Matza, 1957; see also, Topalli, 2005). Through engaging in those self-talks and justifications (Topalli, 2005), offenders attempt to "draft" in a mental state that allows them to change their views of the act, the identities of victims and condemner, and offenders' own identities so that prevent them from feeling guilt.

The original neutralizations initially proposed five ways delinquents do to neutralize their guilts. These techniques are (1) denial of responsibility, which is when the delinquent argues that the cause of his or her behavior is the result of force beyond one's control (2) the denial of injury, which is the claim that denies the existence of injury (3) the denial of the victim, which states as when the victim was the offender and deserved the punishment (4) condemnation of the condemners, which states as the deviant behavior is justified because of the corrupted external

environment (5) appeal to higher loyalties or the idea that crime has to be committed based on one's moral obligations to a party or associated necessities. As the theory has evolved, researchers have conceptualized new forms of neutralizations techniques, including but not limited to the metaphor of the ledger (Klockars, 1974), defense of necessity (Minor, 1981), denial of the necessity of law (Coleman, 1994), denial of criminal intent (Benson, 19865), justification by comparison (Cromwell & Thurman, 2003) and denial of humanity (Alvarez, 1997).

With neutralizations, offenders can strategically change their views when following immoral actions. Sykes and Matz (1965) stated that delinquents maintain strong bonds with society and want to be perceived as "good" (see also, Topalli, 2006). In other words, offenders' use of neutralizations can account for their deviant behaviors to influence others who situate in similar cultural contexts to see and treat these actions and offenders. For example, this can be observed among corporate/white-collar offenders (e.g., Goldstraw-White, 2011; Gottschalk, 2017; Klenowski, 2012; Breeze, 2012). Despite the end, delinquents use neutralization to interpret their criminal behaviors to minimize the possibility of contaminating their self-concepts or social standings (e.g., Scott and Lyman, 1968). In the same token, Scott and Lyman (1968) first introduced the concept of "accounts" that further, the application of neutralization in the way that gains insight into "the human experience [in order to] arrive at… culturally embedded normative explanations" (see also, Orbuch, 1997: 455). In brief, accounts can be understood through impression management (Goffman, 1959), in which they are socially approved vocabularies serving as explanatory mechanisms for deviant behaviors (Pogrebin et al., 2006). Such a process of social construction involves offenders' accounts to manage any societal stigma against their actions and to align their actions with personal and cultural expectations of

appropriate actions (see also, Klenowski et al., 2011). Accounts and neutralizations are similar types of aligning actions to neutralize. The employment of accounts focuses more on persuading others' perceptions of the individuals' deviant behaviors.

Research on neutralizations has moved far beyond the role of this technique in crime but rather how, and to what end neutralizations are used by crime victims. In other word, victims who have close relationships with abusers (i.e., gender-based violence) are observed to use neutralizations to justify offenders' identity as criminals and protect themselves from involvement in victimizations. The deployment of neutralizations generally represents preserving victims' dignity and avoiding shame & fear, and other adverse reactions (e.g., Agnew, 1985; Ahmed et al., 2001; Maruna & Copes, 2005). Specifically, Agnew (1985) argued that victims' deployment of neutralizations and accounts are not motivated to neutralize the harmful nature of their victimizations but rather to define their painful experiences as an "ambiguous reality" to maintain their psychological health (see Eriksen and Pierce, 1968). For example, Ferraro and Johnson (1983) extended Sykes and Matza's concepts (1957) by assigning interview responses from a group of battered women into the following six categories: appeal to the salvation ethic, denial of the victimizer, denial of injury, denial of victimization, denial of options, and appeal to higher loyalties. In this study, female victims consistently expressed that the primary purpose is to maintain relationships or marriages with abusers (Ferraro & Johnson, 1983). Further, Tomita (2000) discussed how the neutralizations proposed by Sykes and Matz (1957) could similarly be applied to elderly abuse victims who suffered from abusive relationships with someone closer to them. Higginson (1999) likewise found among the interviews with teenage mothers who suffered from statutory rape that this group of victims deployed several accounts in explaining or rationalizing their victimizations (e.g., why they prefer to date older males). Last, Weiss (2009)

found among a group of sexually assaulted victims that, they tend to use neutralizations to negotiate offenders' identities as noncriminal and minimize the seriousness of the offense. Commonly deployed techniques are denying offender responsibility, denying injury, and denying themselves as victims. Weiss (2011) utilized 792 victim narratives and established a theoretical framework for elucidating victims' non-reporting behaviors to the police. Specifically, this study listed five main accounts used by victims to rationalize their non-reporting behaviors: denying criminal intent, denying serious injury, denying victim innocence, and rejecting victim identity. Weiss (2011) emphasized that victims' perception of their crime as reasons for non-reporting tends to be overshadowed by the victim-offender close relationship and that preserving the relationship and protecting offenders are more critical for victims than reporting to an authority.

Most importantly, law enforcement personnel also attempt to develop an interrogation technique by offering justification or rationalizations to offenders in order to obtain confessions. This technique is known as REID Technique of Interviewing and Interrogation, which uses similar linguistic techniques that discover among offenders (Copes et al., 2007). Through establishing initial trusts with offenders by asking non-threatening questions, the interrogators who are taught this technique will gradually move to a stage where moral excuses are provided to justify for offenders' behaviors. These approaches can allow potential offenders to sense the amount of sympathy from the interrogators thus having higher possibility of sharing the event details with the interrogators and other officers (e.g., Senese, 2005; Copes et al., 2007). In general, REID technique can demonstrate a unique way of using neutralizations in changing offenders' behaviors (Copes et al., 2007)

Based on this prior literature, the part that has not been explored and studied is whether and how offenders committing interpersonal crimes in cyberspace may attempt to offer or give

neutralizations to victims in the hopes that they will "learn" them or take them on. In the present study, we examine this lacuna by exploring the ways a group of online romance scammers may do so to actively altercast victims' identities and the situation into favorable ones that facilitate the crime commission process. The observations from this study add to the current understanding of offenders' use of neutralizations and accounts during the commission of the crime. We also make suggestions for how these altercasting strategies contribute to less "victim-blaming" in interpersonal violent crimes despite their seemly "willingness" to "facilitate" the crime.

Altercasting

Interactional sociologists have observed multiple ways that actors attempt to control or guide the behaviors of other participants (e.g., Stets and Burke, 1996; Fiske, 1993; Peeters et al., 2005; Goffman, 1959). Drawn from Goffman (1959), Weinstein and Deutschberger (1963) proposed the idea of "altercasting", which is through "project an identity, to be assumed by other(s) with whom one is in interaction and is congruent with one's own goal" (p 454). In other words, a successful altercasting event can involve an actor (typically the enforcer) "casting" another into a particular identity, which is preferred or chosen by this individual (typically the recipient) (McCall & Simmons, 1978; Weinstein & Deutschberger, 1963). Altercasting, deems as a fundamental but critical component of the interactional relationship, exerts a form of control on an interpersonal relationship by demonstrating how individuals can work on others' self-representation (see also, Guadalupe-Diaz and Anthony, 2017; Weinstein & Deutschberger, 1963). Demonstrated in empirical literature, altercasting can be positive (Bernstein, 2016; Spitzer & Volk, 1971) and negative (Beckhouse et al., 1975; Beckman, 1985). For instance, using positive altercasting can allow a "difficulty" patient to be persuaded to adopt the "good patient" role and comply with nurse instructions (Spitzer and Volk, 1971). Such an approach can let those

"difficult" patients feel good about themselves and thus are more likely to behave in a way that is matched the imposed social role (Spitzer & Volk, 1971; Bernstein, 2016). In contrast, Beckman (1985) found that negative altercasting can lead to a certain amount of resistance from individuals to take on specific roles, specifically when it is congruent with the desired self-identity. For example, when individuals saw themselves as leaders but were altercasted into the follower identity, they were less likely to respond with leadership fashion (Beckhouse et al., 1973).

As mentioned, interactants can deploy different accounts to altercast other's identities into the favorable ones that facilitate the events. Likewise, individuals can potentially frame and construct their identities, roles, and responsibilities based on current issues, situations, and feedback from others (Lokatt et al., 2019). This strategy, which is named "self-casting" or "ego-casting" (Weinstein and Deutschberger, 1963), is similar to what Scott and Lyman (1968) demonstrated when actors understand what acceptable social behaviors should be based on the possessed culture and knowledge. "Self-casting" is initially used among health professions (e.g., Lokatt et al., 2019; Järvinen & Kessing, 2021). For instance, healthcare professionals will describe themselves as "must be professional and responsive" all the time when on duty because that is the expectation from the patients, and they serve the "best interests of the patients" (Järvinen and Kessing, 2021). Moreover, nurses can view their identities as less essential and dominant when they constantly receive negative accounts from physicians demonstrating how incapable they are of taking responsibility (Lokatt et al., 2019). Similarly, delinquents, such as drug dealers, can also self-cast their identities from criminals to "forgiving persons" who would respond to their customers' accounts by owing money and allowing more time for them to pay for the drugs (Dickinson, 2017). In sum, self-cast can be seen as a way in which the leading actor

casts himself/herself a particular identity based on the feedback (i.e., accounts) he/she received from other individuals during the interactional process.

The above research demonstrates that accounts can be used to not only altercast other' identities but also one's own identity. What remains understudied is whether offenders, specifically those operated in cyberspace, offer neutralizations and accounts to victims as a way to altercast their identities into favorable facilitating their own victimizations. The outcomes of our study fill this lacuna by exploring whether and how this happens among online romance fraudsters and their victims.

Online Romance Scams

Online romance scams refer to instances where individuals—herein referred to as "fraudsters"—financially defraud victims "through what the victim perceives to be a genuine relationship" (Cross et al., 2018: 2). It is distinct from fraud more generally in that the crime is initiated and carried out via various online dating websites and other service providers (e.g., social media platforms) (Ross & Smith 2011 [in Kopp et al., 2015]; Whitty 2013b). The key characteristic of online romance scams distinguishing it from other types of online fraud is that those committing it use the illusion of romantic relationships to steal from victims (Cross et al., 2018; Budd & Anderson 2011 [in Kopp et al., 2016]).

Whitty (2013b) argues online romance scams consists of several sequential stages (see also Budd & Anderson 2011; Kopp et al. 2016; Cross et al., 2018). In the first two, individuals seeking relationships somehow come into contact with fraudsters who then present themselves as "ideal partners." It is important to note that in these stages victims not only consider themselves—or their self-identities—as potential romantic partners but may also be wary and distrustful of those with whom they are interacting. After presenting themselves as ideal partners,

fraudsters “groom” potential victims “until they are ready to give money” (Whitty 2013b: 678). In the following stages, fraudsters persuade victims to send them money using a variety of techniques. For instance, they may ask for small amounts of money to test victims’ willingness to send it, or they may present false urgent crises (e.g., medical emergencies) and ask for large sums of money (Whitty, 2013a & 2013b). Regardless of what strategy fraudsters use, its success hinges on whether fraudsters have effectively groomed the victim (Cross et al., 2018).

The limited research on online romance scams suggests the grooming of its potential victims is comprised of three interrelated processes. First, fraudsters attempt to shape the way they are identified by potential victims such that are seen as potential romantic partners and not as threats (Whitty 2013b). This can entail sharing false information about who they are, where they live, and their interests (e.g., Koon & Young 2013; Whitty 2013a). For example, fraudsters may pretend to serve in the military or to hold positions of authority (Cross and Holt 2021). Second, they take steps to ensure potential victims view their interaction as a romantic relationship and not as predatory in nature (Cross & Lee 2022; Whitty 2013b; Whitty 2013a). To do so, they may declare love for the victim, contact them frequently, send photographs, and make claims for hopes of a “committed, permanent relationship” (Carter 2021; Kopp et al. 2016; Whitty 2013a). Finally, they groom the way potential victims identify themselves (Carter 2021).

For instance, the fraudster will groom the victim to believe that they are the ideal romantic partner who is destined to meet with the fabricated figure made up by the fraudster (Whitty and Buchanan, 2016; Whitty, 2018). Moreover, the victim may potentially view themselves as the potential “supporter” who should obey the social norm and provide necessary assistance to those in need (Wang and Topalli, 2022). For example, the fraudster may simultaneously leverage social norm and use visceral emotional trigger to ask money from the

victim under the pretense of "repaying them more" as soon as the crisis is resolved (see Whitty 2013b; Wang and Topalli, 2022). In sum, each play important roles in successful grooming, for as previously noted the ways interactants identify others, identify the situation, and identify themselves all shape the character of the interaction.

The scant research on the grooming process in online romance scams has focused primarily on the first two processes. Some of this research, however, has helped elucidate how fraudsters attempt to shape the identities of victims. To do so, fraudsters engage in different social engineering techniques to attribute to a certain level of cognitive dissonance which lead victims to ignore the red flags and choose to believe in those statements that are supposed to exist in a consonant relationship, such as the contingent expressions of love (Cross, Dragiewicz and Richard, 2018; Whitty, 2013b), norm activations (Whitty, 2013b). Lea and colleagues (2009) additionally brought up the fact that fraudsters can also deploy the "altercasting" strategy to groom their victims act from the complementary roles. In doing so, victims can fulfill certain social responsibilities that are assigned to this role (Lea et al., 2009a). In intimate partner violence (IPV) literature, Guadalupe-Diaz demonstrated that the abuser in IPV will try to cast the victim (specifically among transgender populations) in another role that makes victims amenable to control. The victim will typically go along with this role because they feel they need the abuser in some way. By doing so, the abuser of IPV will further control victims' behaviors and thoughts (Guadalupe-Diaz, 2019; see also, Rogers, 2021).

Based on these prior studies, it should be noted that there are no studies in online romance scams or cybercrime in general that have explored offenders' use of altercasting onto their victims. Criminologists have only recently started to explore offenders' use of neutralization techniques in digital piracy (Higgins et al., 2008; Moore & McMullan, 2009;

Morris & Higgins, 2009; Marcum et al., 2011), in drug selling on the Dark-Web (Martins et al., 2020) and in online romance scams (Offei et al., 2020; Barnor et al., 2020). However, questions remain as to how and what neutralizations fraudsters would deploy when facing the non-offenders' victims and if these can subsequently be answered in the context of online romance scams. Herein, in the present study, we add to this research by exploring this process among active online romance scammers. More specifically, we explicate the grooming process in online romance scams by exploring how fraudsters may use neutralizations as a means to altercast victims into identities favorable for victimization. In doing so, we contribute to the overall understanding of the grooming process, add additional substance to the understanding of neutralizations and specifying the important role of neutralizations in grooming process among online romance scammers.

Data and Method

The data informing the current study were collected from *stop-scammers.com*. This website offers a platform where victims of romance scams report the individuals/fraudsters who have defrauded them. These reports include fraudsters' age, gender, email address, phone number, social media information, and a brief description of each scam. It should be noted that this website only includes information about these fraudsters who claimed themselves to be female. As done by prior research using the same source (Wang et al., 2021), each report on this website undergoes a vetting process requiring supportive documents before they can be publicly available. For this research, I will only collect email addresses from fraudsters to establish online connections with them. I developed a Python scraper to gather the email addresses of all "female" fraudsters reported to this site in 2022. I selected 2022 because it was the most recent

year of complete available data at the time of data collection. No demographic information will be scraped during the process.

The initial scraping allows me to collect 607 unique email addresses. Of these initial emails, 135 were sent to inactive email addresses, which reduced the final sample size to 472. Following this, this study employed an experimental design wherein I randomly assigned 472 of them into three groups, with group 1 (control group) having 145, group 2 (treatment 1) having 156, and group 3 (treatment 2) having 171. In early 2022, I sent email messages posing as potential victims to the fraudsters in each group using an automated program developed in Python.

After the fraudsters responded to the first non-threatening email, I began a series of standardized email exchanges with them (see Table 25). The email messages are shown in table 1. Following email 1, wherein I introduced the potential victims to the fraudsters, I then began sending probing questions that naturally elicited their neutralization techniques from them. Email 2 was intended to make fraudsters aware that victims possessed the money and allowed them to imagine where they would use it if they had it. Email 3 is a follow-up to email 2, which aims to reconfirm with fraudsters and obtain any responses concerning the rationales/reasons why their neutralizations are justified. Following email 4, I subsequently sent the control group nothing, treatment group 1 for $1, and treatment group 2 for $10. It should be noted that I chose such a distinct amount to observe more differentiated responses in email 5. Last, in email 5 I again raised the similar probing question as email 2 and expected to observe different behavioral exhibitions.

After sending out all messages, I received 22 responses from group 1, 32 from group 2, and 33 from group 3. Notably, these fraudsters corresponded with us from email 1 to email 5.

Data were analyzed using NVivo as an organizational tool as I collected all responses. I first explored the data for patterns within and across emails exchanged with the fraudsters. Then I sorted similar statements and languages into general domains, which were then further classified by separating them into more specific subdomains. The second author and I revisited our codes for domain and subdomains based on fraudsters' use of neutralizations, the content of these neutralizations, their justifications, and the change in the use of neutralization. Throughout the analysis, themes would be modified or discarded. The final results comprised the prominent themes across all fraudsters, which will be reported in the following sections.

Table 25. Experiment Procedure

<table>
<tr><td></td><td>Group 1: Control group</td><td>Group 2: 1-dollars</td><td>Group 3: 10-dollars</td></tr>
<tr><td>Email 1</td><td colspan="3">Hi love. This is Michael/Jessica. We have talked before. Do you remember me? How are you?</td></tr>
<tr><td>Email 2</td><td colspan="3">I'm so excited! My birthday is coming up and my parents just sent me a $250 gift card on Cash App!!! I do not know how to spend it! If you have it, what would you use it for?</td></tr>
<tr><td>Email 3</td><td colspan="3">But I was thinking about spending it on buying new cookware, do you think what you need is more important than mine?</td></tr>
<tr><td rowspan="2">Email 4 &money</td><td colspan="3">That sounds fun. I'm sending you the money as a gift card. Check your inbox now, and confirmed if you get it</td></tr>
<tr><td>Shortly after sending Message 4, send nothing</td><td>Shortly after sending Message 4, I sent 1 dollar.</td><td>Shortly after sending Message 4, I sent ten dollars.</td></tr>
<tr><td>Email 5</td><td colspan="3">Hi, I think you should receive your money now! What will you or did you use this money on? I am very curious.</td></tr>
</table>

The Initial Observations

The initial idea in this study is to observe if there are any response differences between fraudsters in three groups after the delivery of potential reward. Intriguing enough, fraudsters

across three groups exhibit the following three behaviors that disable the ability of observing any differences. Firstly, specifically among fraudsters in group 2 and group 3, majority of them use exactly the same strategies (neutralizations or altercasting strategy) to justify the need of more rewards from the victim. Second, some fraudsters claimed that they did not receive any money from us across three groups, however the money had indicated being received. Such a situation hints to us that fraudsters may not want to further engage with us because the incentive is too small. Thirdly, some fraudsters, especially those in group 3 disappeared after receiving the money from us, which incapacitate us from further generating analysis assessing any differences concerning responses. With these in mind, rather than abandon the experimental results or view rewards as the one that can differentiate fraudsters' use of neutralizations, we decided to view it as the incentive that can entice fraudsters' active engagement with the designed conversation. As a result, we collected all responses fraudsters made to email 2 and 5 and used thematic approach to generate a detailed analysis on their uses of neutralizations and accounts when prompting with the potential rewards.

Finding

Our analysis of our email exchanges revealed that fraudsters engage both neutralizations and altercasting strategy in the deception of victims. Results are presented below. Importantly, the first two domains, *vicarious necessity,* and *intimate relationship,* are an intertwining of neutralization and altercasting, meaning that fraudsters actively use neutralizations to impose a rather subtly altercasting strategy in changing victims' identities. The rest of three themes (*admitting of being religious and denial of powerless* and *the use of visceral triggers*) are straightforward altercasting strategy. They describe the processes in which fraudsters impose

other favorable identities onto victims or altercast the situation into the rewarding ones to facilitate the crime commission process.

Vicarious Necessity

Similar to the defense of necessity, fraudsters in our sample would also justify their money-asking behaviors as necessary, however, in a way that altercates their intentions of needing money from victims and make them think that sending money to fraudsters is reasonable because victims are helping someone in urgent need. We name this "vicarious necessity, " conceptually similar to the defense of necessity. The most common neutralization offered by the fraudsters was that they framed themselves as urgently needing financial help and victims as persons who could provide it. They did so in three keyways.

First, the fraudsters made comments indicating they would use money from victims to pay off essential bills such as groceries, house rent, and utility bills. For example, Lauren's response is representative of many others. "Huh, I have some bills to pay; if not, I will not get anywhere to stay," she continues to add in the responses, "I will use it to pay my bills, I promise, because I have to find some amount to pay for my bills hun!!". In this demonstration, we can see that Lauren not only provided the reason for requesting money but also fabricated a critical situation--"nowhere to stay" and used several emphasizing but intimate words – "promise" and "hun!!". Such a way to construct the excuses can also be seen in Angela, who noted that her "house rent" will be due very soon, and she still has "no money" to pay for it. Likewise, Alison also stressed on the fact that the money she can obtain from the victim will certainly be used for paying bills, specifically the rent. She stated so by stressing: “I wished to get more than 250$ to add it to my bills so that my landlord will not push me out of the house, So hun I know you are the only man of my life who can help me out of this pain so please help me ...?”

Alternatively, others said they would use the money for emergent medication needs. For example, Morgan ensured to the victim that if she got the money, she would use it for her own medications because she was “not feeling well with my menses”. A similar statement is also used by Morgan, who claimed that "well, that is some of my meds, I do not have enough money to pay for it, and I am very sick now… you could tell I need this to survive… you should know that $100 bucks can safe [save] a life down here when I get my meds”.

A third way the fraudsters appealed to the necessity was by using excuses of preserving their (i.e., offenders) mental and emotional well-being. The fraudsters made comments indicating the help they needed from victims would potentially ameliorate their emotional and mental health. For example, Jonna claimed that she would use the money to "update the PC" because "it is worrying" her for a long time. Annabelle wrote similarly, stating she was looking forward to using the money to "hold a big party" because she had not enjoyed herself for a long time due to the pandemic and was getting "depressed”. A few offenders even stated their depressed or unpleasant mental status if cannot meet with victims and start a new life with them.

In other circumstances, fraudsters also demonstrated that they would use the money to survive in dire situations. Nancy, for example, described herself as a refugee placing in United Nations camp in Senegal and need the financial assistance from the victims in order to “leave this place and regain the normal life out of this camp”. She also showed her extreme sincere meeting and starting a new life with the victim once the victim “accept her background and herself”. Similarly, for the purpose of leaving a dangerous country, Yulia expressed her fear for the bombs in Ukraine and excused to the victim that she cannot wait to leave this country and “life is more important”.

Last, for others, the deployment of vicarious necessity is also used by fraudsters to help or benefit their (offenders) family members. For example, Maris stated, “please i really need you to help me and my daughter.” Daniella said, "get my granny some health stuff. She is in bad condition". Other fraudsters in the sample seek to use other less frequently used excuses, such as using the money for kids to celebrate birthdays. Ann, for example, stated, "I will give it to my girls for her for (my) birthday gifts."

By incorporating different urgency cues, personal emotions, and legitimate figures of a family member, fraudsters further enhanced the effects of the "vicarious necessity" strategy on the victim. Specifically, fraudsters are intended to manipulate victims' morality to think that the money requests are the unavoidable level of help needed to avoid dire consequences (e.g., having no place to stay and worsened health conditions). Moreover, by deploying the vicarious necessity techniques, fraudsters intend to cast victims into a "caregiver" role and make them think that they are the only person who can help the fraudsters. Caregivers are frequently viewed as necessary in assisting another person's social or health needs (Sabo and Chin, 2021). Thus, casting such an essential identity can cognitively reshape victims' perspective about their roles in this "romantic" relationship, which can potentially enhance the amount of responsibilities victim sense that they are obligated to. Casting such an identity onto victims can also, on the other hand, facilitate fraudsters' money-asking behaviors under the rationale that caregivers are responsible for their physical and emotional health. As a result, this alter-casting can cognitively normalize victims' impressions by making them think they are helping someone stuck in financially and emotionally devasted circumstances. This way, victims would be amendable to do things fraudsters want. At the same time, fraudsters can bolster their credibility in potential victims' eyes while reducing victims' motivations to process scam content objectively.

Previously, Minor (1981) identified the defense of necessity as a technique that offenders frequently used to reduce the feeling of guilty by referring to an illegal action as necessary. For example, white-collar criminals claim that illegal businesses are established to meet the competitive business climate (Chibnall & Saunders, 1977). Moreover, the defense of necessity is also deployed frequently among military officers who would justify their actions for sexually exploiting women as necessary to prevent men from inadvertently breaking the law due to the lack of such facilities (Copley, 2014). In our study, fraudsters' deployment of vicarious necessity is conceptually similar to what Minor (1981) proposed, as offenders both use the excuse of necessity to justify the crime. However, the difference still prevails for the specific approach. That said, instead of using necessity as an excuse to rationalize the consequence of behavior after the commission of the crime, the fraudsters in our sample take advantage of using urgent personal crisis, personal emotion, and family members to actively altercast victim's original identity into the identity of a "caregiver". The purpose is to engage victims into rationalizing that giving money to the fraudster can be justified because firstly serious consequences (i.e., break-up or issue with surviving) may result if not offered help during the conversation, and secondly, the "partner" is reliable and trustworthy. In sum, Minor's necessity strategy emphasizes engaging necessity excuses, usually after the commission of the crime. In contrast, our observations of necessity stress more on how fraudsters attempt to appeal to necessity influences on altercasting victims' identity and make them neutralize sending money to the "partner."

Intimate Relationship

A second way that is used by fraudsters in the sample is to use the intimate relationship to neutralize victims’ reluctance to depart with their money. To do so, the fraudsters would firstly allude to the existing relationship or the potential bright future they have with the victim. For

example, Nancy said, “I cannot wait to spend life with you together after I get out from this camp. I can image our beautiful life together”. Similarly, Mimi said wrote, “you are the person I will spend the rest of my life with…I am very very happy to have you as my darling husband.” Alicia also expressed her emotion in a similar way, “I promise to love you more and more with every passing day and be there by your side till my last breath…i'm convinced that the future has a special place for us.” Other fraudsters also use indirect approach to address the intimate relationship, such as the use of pet names (i.e., “hun”, “baby” and “sweetheart”).

A number of the fraudsters rationalize their money-asking behaviors by promising to use the money on something good (i.e., gifts) that can be beneficial to the victim, for example, buying a present. Specifically, Ella stated that "she" would use the money to "hook up" with the victim, and the rest would be returned to the victim. Similarly, Lucy also mentioned that the money would be used to celebrate the victim's birthday, and the rest would be used to enhance their relationship ("will be spent on talking to you"). Others tend to be more pronounced, emphasizing that they would use the money to buy "presents" (Rachael and Lilly) for victims.

Moreover, fraudsters also allude to their intimate relationship with offenders by asking for monetary assistance from victims to support them (i.e., offenders) to travel internationally to visit victims. For example, Catrina and Joy said they would use the money to "buy a flight" and visit the victim. In particular, Natalie asked the victim to send her money to get an "international passport" to enable her to first "transfer all her money" to the victim's account and second "allow her to come over to" the victim's country. In such instances, it could be possible that the fraudsters realized that simply using recreational excuses (i.e., taking flights) is not very convincing; however, such an excuse will likely result in more money from the victims. As a result, they add emotional cues on top of recreational excuses to justify why they need this large

amount of money from victims. During the persuasion, a few offenders even stated their depressed or unpleasant mental status if they could not meet with victims and start a new life with them.

Last, the fraudsters also neutralize the reluctance from the victim by altercasting their identities into favorable ones that facilitate the money-asking behavior. Olga, for example, described a small thing happened during the time she was in Orphanage however left her unforgettable memory. She had a really "good relationship with the teacher of [her] group in kindergarten" and became friend with her daughter, Irina. During that period of time, Olga demonstrated herself being "very lonely" especially in holiday, however her friend Irina "brought the doll she received for Christmas to her (Olga)", She described the doll as "the most valuable gift I have had in my entire life" because this act of her showed Olga "if I really love someone, then I should be ready to give him the most valuable thing I have! Because there is nothing more valuable than giving joy to a loved one!" Likewise, Maris also engages in active altercasting behavior by altercast the identity of the victim into a trustworthy and reliable one. She did so by expressing that,

> *I don't have any experiences in business, am a military woman, you are the one to direct me in any business that can benefit us in future, So anyone you chose that can benefit us very well, then we can go through it, okay.*

By hinting at the fact that they will start a new life with someone that is trustworthy to help her in difficult situations, both Maris and Olga subtly allude to the fact that if the victim wants to have an intimate relationship, then it is normal that the victim should help or give the fraudsters things that can help in dire environments. This also demonstrates a third way the fraudsters

suggested the victim neutralize sending them money: by reshaping their understanding of their degree of control over the direction of the interaction.

Intriguing enough, our sample of fraudsters allude to the intimate relationship as attempts to altercast victims' identities into a "romantic partner." Typically, under such a persuasive attack, vulnerable victims fantasize about having a beautiful life with this fabricated figure and deem that they are responsible for financially supporting the fraudster (either buying gifts or traveling to visit). In such a way, fraudsters reconstruct victims' thoughts that the money they gave to the fraudsters will ultimately benefit themselves (i.e., victims receiving gifts from offenders). Therefore, to facilitate the meet-up process, victims will ultimately send the asked amounts to offenders. Indeed, it is unknown whether fraudsters would use the money to buy presents for the victim; nevertheless, they attempted to use this strategy to enhance further the impression that there is nothing to lose during such a process. Victims can certainly get what they want from fraudsters which is a secured romantic relationship. Such an approach can further enhance their relationships with the victims and shade their true intentions of defrauding additional money.

Previous literature on online romance scams has identified that fraudsters would appeal to intimate relationships to win victims' trust and their "euphoric feeling of love." It lays a solid ground for obtaining the ultimate purpose of using these emotions to exploit victims financially. Moreover, Whitty (2013) also pointed out that fraudsters would appeal to the intimate relationship when they sense rejections from victims to send money. There was often the threat of withdrawing the intimate relationship if the victims did not pay what the offenders asked (Whitty, 2013a). Based on these prior observations, our findings denote that fraudster may altercast victims' identities from "being harmed" to "being benefited" through this relationship,

for example, by asking money from victims under the pretense of buying gifts for them to celebrate the birthday. Such a way of manipulation is very similar to the one used in domestic violence. Offenders would appeal to the intimate relationship by shielding their ultimate purpose of engaging in emotional exploitations without victims' realizations. Some domestic violence victims may even deny being harmed in a relationship and justify that there is no actual violence involved and all their partners want to do is to protect the 'relationship.'

Unlike the deployment of vicarious necessity, fraudsters using intimate relationships seek excuses rather closely associated with the victims themselves and this relationship. In contrast, the engagement of vicarious necessity appeals more so to fraudsters' own physical and health conditions. Moreover, the alercasted identities are also different. Using vicarious necessity appeals to victims' potential "caregiver" roles; however, the employment of intimate relationships rather altercast victims' identities into "romantic partner" roles.

The use of straightforward altercasting strategy

As fraudsters deploy neutralizations to subtly altercast victims' identities in previous two themes, they are also observed to use straightforward altercasting strategy to altercast victims' identities from the swindled one to different other types that may facilitate victims' own victimizations. The first type of the altercasted identity is being religious. The second type is being powerful and dominant in the conversation. In addition, these observations also lead to another finding in which fraudsters engage in the process of altercasting in changing the situation from deceptive to the one containing potential reward that ultimately attract victims to fall into different baits.

Admitting of Religious. The first keyway the fraudsters suggested to the victim was through using linguistic cues to altercast victims' identities into being religious. Specifically,

they found to use religious cues in their conversation with victims to either wish “him” (the victim) for the upcoming “birthday” or promise to come to visit “him” (the victim). For example, following the correspondence in the first email, Lucy, for example, wished the victim by saying "God will guide you and give you long life." Although "she" did not explicitly ask for money in this sentence, however later in this email, she continued to say that "card if I have one, I will use it to wish you….and the rest I will use it to be chatting with you on till it got finished my love". Likewise, Nancy also referred to the "sake of Allah" when she asked for monetary assistance from the victim and promised under the name of "Allah" that she would come over to the victim's country after using the money to obtain the passport. Fraudsters like Mimi would also engage in religious cues by referring to the fact that it is “the god” that allows them as destined couple meeting in online chat room. She did so by stating,

> *Regardless of the situation, thank and worship the Almighty God for giving us the grace to see the light of today and the opportunity to know each other. As for me, I'm safe, thank you for the compliment you gave me, my spirit still says that you are the person i will spend the rest of my life with, or a good friend forever.*

Using religious cues to altercast victims’ identities into being religious (even if they do not have one) is a subtle form of ‘emotional/moral blackmail’. In other word, fraudsters intend to compel victims to act in certain way (i.e., help others despite reasons) just like those who are committed religious personnel. As the result, when victims position themselves into this kind of identity, victims will find it more appropriate to justify their behaviors to help and trust others—specifically those offenders who demonstrated a “long history” of belief in this religion/belief. The elements of religion and faith can help develop a sense of trust and a feeling of responsibility among the victim/recipient.

Multiple previous studies have revealed that the use of religious cues or symbols can be a powerful marketing strategy in businesses (Mottner, 2007; Rinallo et al., 2019; Shah et al., 2019). Importantly, Abu-Alhaija and colleagues (2018) found the significant impact of using religion on product packaging in shaping customers' positive views towards the products and increased their intentions to purchase products. In online romance scams literature, for example, Kopp and colleagues (2021) pointed out that fraudsters are frequently observed to appeal to religious sensibility to develop emotional appeal among swindled victims. Advancing these previous observations, our findings further revealed the mechanism of fraudsters' use of religious cues among victims, that is to enhance the level of trustworthiness and responsibilities of victims through altercasting their identities into religious ones. Through this approach, victims would sense more obligations in helping and trusting others especially for their partners, thus they justify their money-giving behaviors as a way to fulfill their ideal images that fraudsters frame them in.

Denial of Powerlessness. Fraudsters in our sample are also observed to use two different approaches to enable victims' decisive power to decide the usage of the money. The first one can be summarized as letting victims to decide the place to spend the money. For example, Lena writes "if you have this money, go get yourself some good clothes and take yourself out for fun okay mumu, but it is up to you". Or Jessica said, "I do not know is your money then you have choice to spend your own thing". Alicia followed the trend, stating, "It's your choice to decide." Petty was equally succinct, stating, "it is up to you."

Others is more subtle in letting the victim to know it is his choice to whether send money to the fraudster. In these scenarios, some fraudsters attempt to put themselves on their feet while also touch on the fact that they wish victims can share the money with them if victims really

want to do it. For example, Carrie states that “if you want to share, I am fine with it”. Sarah was also one of these. "Yes, do you want to spend it with me?" She wrote, "I would be very happy if you do." Caroline was more straightforward, however, still using an inquisitory but imperative tone, "Do you want to give the money to me now? I will be happy if you do" Among them, it can be observed that fraudsters frequently used the word “want to”, “could” and “if”. The use of these words can unconsciously allow victims to neutralize that whether sending money to the fraudster is more of his own will.

Instead of simply justifying their behaviors by denying the victims’ existences, fraudsters in our sample strategically advance their techniques by giving victims the decisive powers to decide where they want to spend the money. Specifically, the deployment of such a technique is observed to use frequently among fraudsters after the victim inquiry how they will use the Amazon money if they have it. We speculated that such an approach could help fraudsters in altercasting victims’ identity from the “swindled one” to the “controlled one”, with the ultimate aim to deny the swindling events to lower down the victims’ guardians, leading to the final financial exploitations.

Majority previous ORF and non-ORF literature have pointed out that offenders would actively exploit victims’ different types of vulnerabilities for the purpose of gaining dominant control over the course of criminal incidents, for example child sex trafficking (e.g., Sigmon, 2008; Reid and Jones, 2011; Winters et al., 2022), domestic violence (e.g., Stark, 2012; Duron et al., 2021) and online romance scams (e.g., Rege, 2009; Whitty, 2013a & 2013b; Whitty, 2018; Wang and Topalli, 2022). In contrast to these prior observations, a study conducted by Wang and Zhou (2022) revealed that Chinese fraudsters would temporarily step down from the dominant side and offer victims certain amount of controls over the potential “investment” opportunity by

providing free initial investment fund or technical assistances/resources. In furtherance of prior observations, the finding in current study additionally divulged that fraudsters would also use linguistic cues along with emotional components to deceive victims that they have control over the money through altercasting their identities from the submissive to the dominant one. By doing this, fraudsters intend to deceive victims in the way that denying the swindling, minimizing the suspicions, shifting victims' attentions to the established "romantic" relationship (or the wonderful future) and the trusted personality of the non-existed "partner".

The Use of Visceral Triggers

The last finding from our observations indicates that fraudsters are actively engage in different kind of visceral triggers with the purpose of getting rewarded. Previous sections have identified four main altercasting strategies that fraudsters engage in changing victims' identities into the favorable ones that facilitate their own victimizations. These fabricated identities would include: 1). caregivers, 2). intimate partner, 3) the powerful being, 4) the religious being. It should be noted that the deployment of visceral triggers is conceptually different from these four altercasting strategies. For example, fraudsters' engagement in vicarious necessity is to neutralize victims' potential misgivings or suspicions by altercasting them into roles as caregivers; and the use of intimate relationships is to neutralize victims' misgivings by altercasting them into roles as intimate partners. In contrast, the employment of visceral triggers is to neutralize victims' misgivings by redefining the situation into the favorable one in which they (e.g., victims) will potentially be rewarded with either tangible or nontangible benefits. As offered in Office of Fair Trading (2009) research, the use of visceral triggers or appeals can involve with eliciting basic human needs such as money, sympathy, love, pain and sorrow. In this section, we have identified three different visceral triggers that are actively deployed by

fraudsters, which are sympathy, money and love, with the goal of creating delusions of getting rewarded among victims (Lea et al., 2009b).

The involvement of sympathy trigger typically concerns with the deployment of vicarious necessity. Fraudsters would oftentimes use the excuses of helping with paying off essential bills, preserving mental & emotional well-beings and assisting family members. These excuses oftentimes were used in couple with emotional or romantic connotations, such as different pet names “hun” or “sweetheart”. For example, Lauren said “Huh, I have some bills to pay; if not, I will not get anywhere to stay”. Or Jonna stated she would use the money to “update her PC” and it will worry her if “it is not fixed”. Or Daniella rushed that, "get my granny some health stuff. She is in bad condition, please sweetheart". By using urgency cues that are pertinent to the well-being of the “partner” and “her” family members, fraudsters seek to engage victims into sympathizing with “her” (the offender) impoverished circumstances and the situations faced by the family members which need immediate financial assistances. The coupled emotional connotations can frequently make victims to think that if they offer financial assistances to their “partners” online, then it is highly likely that “she” (the offender) will say express more love to them and the romantic relationship can be established or further enhanced. As a result, victims can potentially be “motivated” to give out money to the fraudster under the rational that they can be rewarded with enhanced romantic relationship with higher possibility of meeting up with the “partner” in the near future.

Other fraudsters in the sample seek to use actual monetary driven visceral triggers by directly promising the victim that they will be rewarded financially if they are willing to make the initial investment. For example, Millan affirmed to the victim that she would use the money to "open a supermarket and profit in 3-5 years". Millan assured that she would "share some of it

(profit)" with the victim. Intriguing enough, this fraudster uses reward-oriented visceral triggers to convince and assure victims that they will get their initial capital back if they are willing to make the investment upfront. This visceral trigger is the way that the fraudster used to altercast victims by allowing them to see themselves as persons who might get something that is actually tangible from this relationship. Such an observation is consistent with what Lea and colleagues (2009b) described as the importance of "visceral triggers" as an essential technique to persuade victims to respond to scams, as these direct them to focus on the positive outcomes of engaging in specific actions.

Last, some of the fraudsters also appeal to emotional(love)-related visceral triggers by hinting at the intimate relationship to push victims into identities where they think they are going to get either gift, money or a meet-up with the fraudster in the near future. For example, Lucy demonstrated that she would use the money that the victim sent to her to “buy birthday gift and ship it” to the victim’s house. Natalie, who also asked the victim to send money to her under the pretense that she will use the money to “get an international passport”, then use the obtained “passport” to transfer all her money to the bank account of the “victim” before travelling to see the “victim”. Different from the use of vicarious necessity, the appeal to the intimate relationship appears to be more direct and contextualized in engaging victims’ expectations towards the potential gifts, the meet-up and the money from the fraudster. By casting victims into a “romantic partner” identity, the fraudster’s use of emotional-related visceral triggers can easily facilitate victims in sending money to the fraudster through neutralizing their misgivings as they (victims) can ultimately obtain benefits/rewards from the “partner” either tangible or intangible or both.

Discussion

This article aimed to explore the role of offenders' neutralizations plays in how victims' rationalizations construct their views towards the scamming incident and how such a process may facilitate the victimization process. Through neutralizations, instead of directly asking for money from the victim, online romance scammers advance their techniques by attempting to altercast victims' identities from the ones containing harmful components (i.e., being swindled) to those favorable ones that accelerate the swindling process. Specifically, casting victims into those identities can potentially "assist" in formulating rationales for sending money to fraudsters and neutralizing the misgivings concerning any deceptive cues that fraudsters pose. In doing so, online romance scammers are observed to frequently appeal to vicarious necessity (i.e., pay off bills, maintain emotional & mental health and help with family members) to fabricate sympathy-generating situations that require immediate assistance from victims (i.e., "the caregivers) or dire consequences will be resulted. Fraudsters' neutralization deployment also involves fabricating excuses under the pretenses of alluding to an intimate relationship. By asking for money to enhance the relationship (i.e., asking to buy gifts for victims or travel to see victims), fraudsters create an illusion that engages victims to justify delivering money to fraudsters as a means to maintain their long-term relationships. Fraudsters are also observed to use straightforward altercasting strategies by impose favorable identities, in this case being religious and dominant onto victims. Casting those new identities to victims can unconsciously compel victims to act in a certain way that falls within fraudsters' expectations. The last altercasting strategy observed in this study is when fraudsters manipulate different visceral triggers (i.e., sympathy, money, and love) is to altercast the situation into the advantageous one that signals to the victim the potential rewarding opportunities.

These findings are essential first because they added to the understanding of the grooming process more generally by specifying how neutralizations can be offered to victims to altercast them into favorable identities. Ward (1995) argued that offenders' use of grooming techniques could be referred to as cognitive deconstruction, which involves processing at a lower, more concrete level, i.e., muscular movements and rewards of behavior, rather than social action. Resultantly, the individual has much more focus on feelings of pleasure and less awareness of the consequences of his/her behaviors (e.g., Ward, 1995; Whitty, 2013a & 2013b). Hence, it is critical to study how offenders create and maintain these grooming techniques/processes, what are these specific grooming techniques say about how they wish to be viewed by their victims, and how these techniques can influence victims' responses/behaviors. Previous literature has identified that sex offenders would use different grooming techniques to make their victims see themselves or the events in a different/positive way which "facilitates" the process of victimization. (See Ward et al., 1995). Some common techniques that have been identified are the use of bribes (gifts) (Campbell, 2009; Joleby et al., 2021), the use of friendship/romantic relationships (O'Connell, 2003; Whittle et al., 2015), the use of self-promotion and the use of intimidating adult figures (e.g., Bennell et al., 2001; Shakeshaft, 2003 & 2004; Campbell, 2009). The results of our analysis, drawing from extant grooming literature, builds on the finding of previous research suggesting that offenders in online space deploy more linguistic-driven grooming technique, referring to the neutralizations by highlighting the fact that, among those online romance scamsters, the use of neutralization is the key mechanism that can shape how victims view positively towards the scamming incident thus facilitate the victimization process.

The findings from the present study join those from previous research in suggesting that the dynamic representations of fraudsters' grooming techniques (see, e.g., Whitty, 2013; Kloess et al., 2014; Heffernan & Ward, 2015; Fortin et al., 2018). Here we add to this line of research by demonstrating that the characterizations of offenders' grooming techniques can also be represented through strategically altercasting victims' identities into favorable ones that facilitate the exploitation process. These "favorable" identities can cast victims into a specific position where they are "expected" to act in specific ways to fulfill the ideal images of these figures. For example, using vicarious necessity cues can altercast victims into the figure of "caregivers," which they (victims) felt responsible for providing financial assistance to satisfy offenders' immediate needs. In addition, these findings added to those from previous research by arguing that neutralizations used by offenders can additionally play a key role in enforcing the visceral triggers in altercasting situation into the one that benefits the victim tangibly or intangibly.

The results of our analysis also have implications for understanding how our observations add to neutralization theory by illustrating offenders' use neutralizations to facilitate their crimes. Numerous scholars have argued how neutralizations are used by offenders committing both crimes in physical and online space, for example, shoplifters (Cromwell & Thurman, 2003), auto-thieves (Copes, 2003), honor crimes (van Baak et al., 2018), serial murder (James & Gossett, 2018) and digital piracy (Marcum et al., 2011; Morris & Higgins, 2009). In addition to these previous findings indicating that offenders use neutralizations to justify their criminal behaviors after the crime, we advance this literature by demonstrating that offenders (i.e., fraudsters) also attempt to use neutralizations to altercast victims' identities during the swindling process. In addition, our finding suggests a second way that fraudsters use neutralizations—to

deploy it with visceral triggers, which deceive victims about the potential rewarded opportunities if they send money to assist fraudsters upfront.

Specifically, these deployed neutralizations (e.g., *vicarious necessity, intimate relationship*) reduced victims' perceptions of threats/deceptions posed by fraudsters by subtly or straightforward altercasting their identities into "caregivers," "lovers," "dominant one," and "religious ones." Specifically, concerning for the altercasting the victim identity into the "dominant one", Prior research has demonstrated that online romance scammers and offenders committing other types of interpersonal crimes take measures to gain a dominant role in the interaction, for example among child sex trafficking (e.g., Sigmon, 2008; Reid and Jones, 2011; Winters et al., 2022), domestic violence (e.g., Stark, 2012; Duron et al., 2021) and online romance scams (e.g., Rege, 2009; Whitty, 2013; Whitty, 2018; Wang and Topalli, 2022). In contrast to these prior observations, a study conducted by Wang and Zhou (2022) revealed that Chinese fraudsters would temporarily step down from the dominant side and offer victims certain amount of controls over the potential "investment" opportunity by providing free initial investment fund or technical assistances/resources. In furtherance of prior observations, the finding in current study additionally divulged that fraudsters would also use linguistic cues along with emotional components to deceive victims that they have control over the money through altercasting their identities from the deceived role to the dominant role. In this way, fraudsters attempt to mobilize victims' agencies to boost their confidences in trusting these fabricated figures and this "romantic" relationship. Such a strategy is to foreshadow the later financial exploitation.

In sum, these altercasted identities similarly "assisted" victims in neutralizing/justifying their misgivings by unconsciously accepting certain expectations projected from these identities.

By reducing the number of suspicions and deceptions involved with the fraudulent conversation, the fraudsters position themselves as persons (i.e., an impoverished figure or a partner) who need certain assistance from the victims in order to allow them to continue this relationship and meet up in the future, or persons who are trustworthy and have no intention to deceive victims (i.e., a submissive or religious figure). In doing so, the fraudsters took control of the swindling process by taking an active role in altering their roles during the conversation from the fraudsters to someone worthy to be trusted and assisted. And such behavioral alterations, in return, influenced fraudsters' use of different visceral triggers in making victims believe that sending money to them in advance can exchange for larger rewards in either tangible (i.e., monetary reward) or nontangible form (i.e., enhanced romantic relationship or meet-up).

Previous research on online romance scams proposed that this type of crime consists of several sequential stages (Whitty, 2013; Whitty, 2013a). The initial stage focuses on the initial baiting victims, followed by grooming victims with intimacy. In these two stages, fraudsters attempt to increase the interactions and enhance the trusted relationship with victims to present themselves as the "ideal partner" (Whitty, 2013a& 2013b). Subsequently, fraudsters would exploit the number of trusts established in the previous two stages and use pretenses to swindle money from victims' pockets (see also Cross et al., 2018). Several previous research has explicitly analyzed the grooming process in online romance scams, as this technique is an essential component that allows fraudsters to shape their identities from threats to "ideal partners" (Cross & Holt, 2021; Koon & Young, 2013; Whitty, 2015), allow victims to view the whole interactions as romantic rather than threats (Cross & Lee, 2022; Whitty, 2013b; Whitty, 2015), and change the way the victim identity themselves (Wang and Dickinson, preprint). Such a grooming technique is similarly abused by offenders committing sexual offenses and domestic

violence crimes (e.g., Ward et al., 1997; Ward, 2000; Hazama & Katsuta, 2019; Cross et al., 2018). Nevertheless, there is still a lack of knowledge on how offenders use grooming techniques, specifically how they use neutralizations to altercast or groom their victims into favorable identities that are amenable to sending them money.

The findings from the present study join that previous research in suggesting that fraudsters' use of neutralizations plays a vital role in developing the grooming technique in the way that altercasts victims' identities and situations. Here we add to this research by demonstrating that fraudsters in cyberspace also actively groom victims in a way that replaces the initial identities that were prone to be victimized to the identities that can be benefited from this relationship. Hudson (2005) previously pointed out that victims of sex offenses can go through stages of cognitive distortion and deviant sexual fantasies to support the overall abuse planning to groom both victims and the environments (see also Whitty, 2013a). Similar to this group of victims that are sexually abused in the physical world, romance offenders operated in cyberspace are also deploying a similar technique in using different neutralized excuses to lure victims into a certain type of cognitive distortion making them think that they are the identities, that fraudsters altercast them in. Similarly, altercasting victims' identities into favorable ones can facilitate the formation of cognitive dissonance by allowing victims to extract certain beliefs and opinions from the new identity to reach consonance or forget the uncomfortable aspects. For example, when the identity of a "romantic partner" is casted, victims are more likely to envision themselves as someone who should be responsible and help resolve their partners' hardships rather than questioning or doubting them. Under such a circumstance, victims tend to persuade themselves to ignore the red flags and deploy different excuses to send money to fraudsters.

Limitations

Although the results reveal essential factors in how fraudsters implement their neutralizations and accounts, the current study should also consider pointing out limitations in this work that should be the focus of future research. First, the current sample consists of only female fraudsters but no male fraudsters. Therefore, the generalizability of the observations is still being determined. In the initial stage, the researcher sent messages to male and female fraudsters; however, the response rate could have been higher (approximately only 6% of male fraudsters chose to converse with the researcher throughout these five emails). The researcher speculated that male fraudsters could be more suspicious and cautious than female fraudsters. Due to such a circumstance, the researchers decided to exclude male fraudsters from the sample. No meaningful results can be generated if the response rate for males and females is largely contrasted. Future similar experimental research should address such an aspect. Potential approaches could be giving male fraudsters additional time to respond or using different probes to get an increased rate of responses from them (i.e., sending out messages using another tone or attaching a fictional female image with the message). In addition, future research should also observe responses from those fraudsters running other types of romance scams (e.g., crypto-romance scams) or those operating on different websites or apps. Other types of romance scammers may employ different strategies to manipulate victims or use different neutralization or accounts differently.

Second, the validity of current findings may be contaminated if the romance scammers the researcher contacted viewed the correspondence as suspicious or unusual and, as a result, did not respond as they typically would in a typical fraudulent conversation or respond with unauthentic answers. It could be possible that some fraudsters may realize that the researcher is

not the actual victim but instead can be those affiliated with research groups or law enforcement agencies. As a result, some of them may play with us by intentionally giving us incorrect responses, which may lead to the impossibility of observing natural responses from fraudsters. Future studies can design the probing questions logically and naturally to minimize suspicions. Moreover, researchers can explore the type of websites or applications that have higher chances of encountering fraudsters. Researchers can then create a fictional profile and wait for the fraudsters to initiate conversations with them.

Nevertheless, despite these limitations, this current study further attempts to specify the neutralizations and accounts used by the fraudsters in the sample. Moreover, this study also reveals that using neutralizations and altercasting serves to impose favorable identities on victims, ultimately facilitating the perpetration of the scam. In doing so, it contributes to understanding romance scams, the grooming techniques used by fraudsters, and the application of neutralization theories to cybercrime. The following section will discuss the main policy implication that can be seen from current research outcomes.

Policy Implications

Previous studies have demonstrated a pervasive victim-blaming discourse among victims of fraud (Cross, 2015; Cross, 2016 & 2018), specifically among those experienced online romance scams (Sorrell and Whitty, 2019; Cross, 2015). The sufferers are constantly described to be “greedy”, “lonely or have nothing to do in their lives” or simply being questioned “how could you so stupid”, “how you could give money to someone you never met”. These individuals typically throw out those narrations under the stance that “I would never fall into these scams, and it would never happen to me”. Such a victim-blame discourse is specifically common among elder online romance scams victims (Cross, 2016; Sorrell and Whitty, 2019). As the result of

those blames, victims of online romance scams are found to have harder times recovering psychologically from the scam (i.e., have difficult time in trusting others or continuing a normal relationship). In some extreme cases, victims would live under amounted stress leading to the potential suicidal behaviors (Sorrell and Whitty, 2019).

Prior empirical research conducted by Sorrell and Whitty (2019) has pointed out the existence of victims' blame discourse among online romance scams sufferers. Moreover, in multiple of her works, Dr. Cassandra Cross used an interview approach and found that victim blame pervades online romance scams and fraud in general (2016, 2016 & 2018). However, to date, no prior research has assessed from the perspective neutralizations to analyze fraudsters' use of manipulative linguistic cues in changing victims' perceptions of themselves and the overall situations in the scam. Our finding is the first to support the fact that victims do not choose to trust those fraudsters of their free will or send money to fraudsters voluntarily. However, rather they are doing so under the influence of fraudsters' neutralizations in altercasting the identities into favorable ones. In other words, victims are deceived in a way that assumes themselves having an actual romantic relationship with their ideal partners. All the responses and behaviors are the consequences of love, belief, and trust toward loved ones. We believe that such outcomes implicate the necessity of minimizing victims' blame endemic and increasing the offer of victim therapy and assistance programs to reduce the psychological harm brought by online romance scams (see also Cross, 2014 & Cross et al., 2016). For example, governmental and non-governmental agencies should increase the publicization of awareness and education programs for the public. The purpose is to raise awareness, so everyone understands the internal operation of an online romance scams, its influences on victims, and the support that victims deserve from their families and friends. Moreover, law enforcement agencies or staffs

also need specific professional training to know how to deal with victims of online romance scams and how to handle relevant cases appropriately. Lastly, appropriate support services with trained professional support should be established to allow victims to access them whenever needed.

Chapter V: Discussion and Conclusion

Abstract

In this dissertation, I used four different theories to guide the study of fraudsters' behaviors in online romance scam. Specifically, in an attempt to generate a more accurate understanding of the rationality of romance fraudsters, I composed three papers to firstly point out the current main gaps in online romance scam study and then use experimental approach to collect responses from active romance fraudsters to argue that they are rational decision makers. The research suggested that fraudsters change their strategic behaviors in manipulating victims when there are presentation and fluctuations of rewards. In this chapter, it aims to provide an overall summary of prior observations, implications, and limitations. The chapter first starts with a comprehensive review of the seriousness of online romance fraud and prior relevant studies. Following, a summary of research outcomes in each chapter following the sequence is provided. Theoretical and policy implications drawn from each chapter are further refined and demonstrated in detail in the subsequent two sections. Lastly, the chapter ends with a proposal for future research based on current observations of limitations in each chapter. A general conclusion brings forth the end of this dissertation.

Discussion

With the fast advancement of information and communication technologies, the wide spread of the usage of internet has on the one hand, brought an endless supply of knowledge and entertainment, but on the other hand, posed one of the greatest threats to people's assets and the national security interests of US and other countries around the globe (Department of Homeland Security, 2022). In US alone, cybercrime costs approximately $6.9 billion in 2021 (IC3, 2022). It is estimated that the inflicted damages caused by cybercrime are predicted to reach around $10.5

trillion annually by 2025 (Morgan, 2020). Among all the cybercrime types, the top first three cybercrimes (e.g., BEC. Investment and Confidence Fraud/Romance) causing the most victim loss, as documented in 2021, are the types of crimes against individuals or organizations (IC3, 2022). Due to the lack of effective mitigation strategies (Maimon & Louderback, 2019), the statistics for cybercrime specifically those against persons exhibit an upward trend each year, and cybercriminals continue to evolve their social engineering techniques to deceive vulnerable individuals in online space. As a result, to assist in proposing evidence-based policies that protect internet users, it is necessary to understand the rationality and behavioral patterns of those cyber-enabled offenders in the ecosystem (e.g., Maimon & Louderback, 2019).

Previous research demonstrated that online romance scammers are rational decision-makers. Specifically, several authors (e.g., Whitty et al., 2013a and 2013b; Wang and Topalli, 2022) showed that romance fraudsters follow specific predesigned scripts and operations. In addition, a small fraction of research observed that online romance scammers, when facing a restrictive deterrence message, are likely to modify their behaviors to reduce the risk of exposure (Wang et al., 2021). Scholars further confirmed that romance scammers would strategically deploy neutralization techniques to justify their legitimate behaviors to avoid blame from the public and their inner selves (Offei et al., 2020; Barnor et al., 2020). Thus, it is reasonable to view the behaviors of online romance scammers in the same way as those offenders (i.e., robbers and drug dealers) (e.g., Jacobs et al., 2000; Jacobs, 2010) who carried out their illegitimate behaviors in physical space. However, very limited research has been able to use experiential evidence to support for such an assumption (Barnor et al., 2020; Offei et al., 2020; Wang et al., 2021).

As a result, the subsequent two papers choose experimental approach through obtaining the IRB approval and developing a standard protocol to establish communications with fraudsters. By sending them probed messages and rewards, both papers seek to understand the main strategies used by fraudsters and their strategic change of those behaviors when facing the variations of potential rewards from the victim. In specific, the results of the second paper indicated that romance scammers' communications with potential victims are multifaceted and can simultaneously include up to seven types of deception strategies. These seven strategies are: 1) *fraudster's personal identity*, 2) *victim's identity,* 3) *relationship with victim*, 4) *ask for, demand or accept money*, 5) *ask for personal information,* 6) *request to talk or chat,* and 7) *interactional facilitators.* Moreover, the quantitative assessment outcomes revealed that online romance scammers change the degree to which they use specific strategies in response to fluctuations in the level of presented reward. In sum, as previous research measures that fraudsters can be restrictively deterred by warning messages, this paper additional provides empirical evidence to the rational choice theory confirming that fraudsters' behaviors can similarly be modified with the presentation of reward.

Following, the third paper similarly used experimental approach to extract emails used by active romance scammers in a different year. Conceptually similar to the prior techniques brought up by Sykes & Matz (1957) and other neutralization scholars (e.g., Klockars, 1974; Minor, 1981; Alvarez, 1997), findings from this paper revealed that online romance scammers engage in using vicarious necessity and appeal to intimate relationship to make the persuasions. In furtherance of previous observations, this study additionally revealed that the use of neutralizations and accounts can potentially play a role in altercasting victims' identities into favorable ones that allow fraudsters to control the direction of the scamming incident. In

addition, fraudsters are also revealed to manipulate different visceral triggers to altercast the scamming situations into the favorable ones that further compel victims to depart with their monies.

In sum, online romance scams are currently understudied by scholars. Majority ORF studies are concentrated on conceptually similar areas of research using homogenous data collection or analytical strategies. Specifically, the area of understanding fraudsters' mindsets (i.e., rationality), which could provide supports for crime reduction policies and initiatives, is severely under-explored. Thus, the observations from chapter two and three serve for gaping the void by initiating proactive conversations with active online romance scammers. Findings largely support the fact that online romance scammers are rational would alter their behaviors strategically when facing the potential rewards. Specifically, the adoption of strategic behaviors is further observed to involve the employment of variety of neutralizations and accounts.

Theoretical Implications

The results discussed directly above, have a main theoretical implication—that is to encourage more scholarly research to apply appropriate theoretical constructs to explain the etiologies of a criminal behavior. Inherently, due to the nature of the occurrence of cybercrime (i.e., cross-jurisdictional, involves with massive financial loss and technical components), scholars in this field propose that an interdisciplinary perspective should be adopted to understand a cybercrime incident from varies perspectives (e.g., Howell, 2021; Holt, 2022). Thus, two empirical studies in this dissertation draws from rational choice theory, interpersonal deception and neutralization, which originates in the criminology and communication respectively, to provide theoretical support for explanation the rationality of online romance scammers when facing the reward. The findings from both studies bear substantive contributions

to criminological, communicational and cyber-criminological literature, specifically in online romance scams.

Rational choice theory (RAT) considers offenders are rational actors who always make assessments of potential risks and reward (Clarke and Cornish, 1985). Previous research has been able to use RAT to make sense of offenders' mentality in physical crimes concerning their use of different strategies to perpetrate crimes (e.g., the target selection) (e.g., Jacobs, 2010), the propensity of avoiding risks (e.g., Gibbs, 1975; Jacobs and Cherbonneau, 2014) and the tendency of increasing the frequency of offenses when there are facilitative opportunities (e.g., Nagin and Paternoster, 1993; Thomas et al., 2020). When explained the occurrence of cybercrime from the lens of rational choice theory, evidence-based scholars are able to (1) observe offenders' risk avoidance behaviors among online romance scammers (Wang et al., 2021), (2) reveal the reasons behind the offending and victimizations (e.g., greater or lesser TRDM) (e.g., Paternoster and Pogarsky, 2009; Louderback and Antonaccio, 2017), offenders' target selections (e.g., lack of suitable and capable guardianship) (e.g., Maimon and Louderback, 2019), victims' likelihood of being victimized in cyberspace (e.g., their online activities and visibilities) (e.g., Leukfeldt and Yar, 2016; Reyns, 2017), (3) propose the cybercrime prevention strategies based on situational crime model (e.g., target hardening) (e.g., Holtfreter and Meyers, 2015; Butler et al., 2022). Absent in criminological literature, however, is the ability to use empirical evidence to demonstrate offenders' rationality (e.g., Wang et al., 2021). Although Wang and colleagues (2021) have demonstrated that offenders can be restrictively deterred when facing potential sanctions, however it is yet unknown whether offenders will exhibit contrasted behaviors as there are potential rewards, specifically among online romance scammers.

In light of the observations in prior studies within the scope of rational choice theory, this research promotes theoretical development in the field of cyber-criminology by (1) using firsthand dataset through proactively holding live conversations with online romance scammers; (2) operationalizing the concept of reward through sending the actual electronic gift cards to offenders; (3) providing empirical support for the fact that romance scammers will alter their behaviors in response to changes in the likelihood of receiving a reward that occur over the course of an offense as a means to further increase the chances they will receive this reward; (4) expanding the scope of RAT by demonstrating that online romance scammers, similar to physical crime offenders, also exhibit the reward-maximization behaviours when there are opportunities.

The above implications also hint at future research considering the role of bounded rationality in an online romance scam. RAT assumes that decisions are characterized by 'bounded' or 'limited' rationality. In other words, criminal decision-making does not always ideally rely on assessing costs and rewards but rather as a consequence of the conditions under which such decisions are made (e.g., Campitelli and Gobet, 2010; Willison & Backhouse, 2005). With the associated risks and uncertainty in offending, criminals may make decisions that will be good enough rather than the best possible decision, specifically when they have insufficient knowledge of all the potential costs and benefits (i.e., the risks, efforts, and rewards) (e.g., Willison & Backhouse, 2005; Copes & Vieraities, 2009; Jacobs & Wright, 2010). When considering such an aspect, especially with the interplay of the internet in criminal behaviors, online offenders often lack sufficient knowledge about guardianships, the identity of the victims, victims authenticate reactions, and more. In this case, fraudsters' decisions may depend on, for example, preparation, target selection, etc. Therefore, these groups of offenders are likely to

engage in different thought decision-making processes than those operating in an offline setting. One central research question that can facilitate future online romance scam research in rational choice theory is to explore which rational choice processes are unique to an online scam. By addressing this central research question and those extended ones, the application of rational choice theory can be further assessed and expanded using an empirical dataset collected from online fraudsters.

The findings reported in the second paper additionally promote the relevance of the criminal event perspective in understanding the dynamics of fraudsters' behaviors in the online romance scams. They further expand the body of criminological literature using CEP in violent offenses and online fraud in general (Pino, 2005; Chopin & Beauregard, 2020; Maimon et al., 2019& 2020). The findings specifically demonstrate fraudsters' change of their self-presentation strategies (i.e., manipulation of personal and victim identities) to increase the chances of getting the potential reward or more incentives. Such an observation echoes the main offender element in the CEP, which presents that offenders can change how they present themselves to obtain illegitimate goals.

Furthermore, findings from this research also promote the theoretical development in the communication literature by demonstrating that fraudsters actively deploy the interpersonal deceptive strategies to manipulate their victims. Prior studies using IDT investigate the dynamic interactions between persons intent on deception and those they want to deceive in an offline setting (Buller and Burgoon, 1996). Scholars observe that such a dynamic exchange between deceivers and receivers involves with both strategic and non-strategic behaviors, which can be shaped by several factors (e.g., Burgoon and Buller, 2015; White and Burgoon, 2011; Buller and Hunsaker 1995; Kalbfleisch 1992). Empirical studies have only recently been initiated when

examining the application of IDT in computer-meditated communication. Specifically, scholars such as Carlson and colleagues (2004), Pak and Zhou (2014), Maimon and colleagues (2018 and 2020) and Wang and Topalli (2022) emphasized on the fact that computer-meditated communications can help to transfer both verbal & non-verbal social cues and explored the interactive exchanges between deceivers and receivers in online space. Nevertheless, scant studies collect data on active online offenders (Maimon et al., 2019) and examined the reciprocal communications between deceivers and receivers (e.g., Pak and Zhou, 2014). This current study, by operationalizing the certainty of a reward, expands the current understanding of IDT to the scope of online romance scams and reveal that (1) fraudsters would use different strategies to maximize the reward (i.e., the manipulation of personal identity, the use of interactional facilitators and more), (2) fraudsters will respond differently by using different tactics based on the certainty of reward with the intention to encourage the victim to provide the actual reward. Stated differently, the outcomes of the second study used the first-hand experimental data and confirmed the initial assumption from Buller and Burgoon (1996) that the behaviors of deceivers and receivers can influence each other reciprocally relying largely on strategic behaviors. Thus, future communication and criminology scholars can explore if such reciprocal communication can be additionally observed from another groups of cybercriminals.

Another aspect of offenders' rationality can be seen from their uses of neutralizations in justifying the illegitimate behaviours. Brought up by Sykes and Matz (1959), neutralization theory, consist of five main techniques, is used by offenders to facilitate their offending processes by "lessening the effectiveness of internal and external social controls," (see also Dickinson and Jacques, 2009). In other words, offenders acknowledge their actions are in violation of societal norms, yet still engage in them, because their behaviors are temporarily

justified and the morality that governed the actions are neutralized (e.g., Vasquez and Vieraitis, 2016; see also, van Baak et al., 2022). Past research has found associations between neutralizations and different offending outcomes, ranging from drug, property, and violent offenses (e.g., Maruna and Copes, 2005; Peretti-Watel et al., 2004; Shields & Whitehall, 1994; Vandiver et al., 2012; Piquero et al., 2005; Siebert and Steward, 2019). Neutralizations have also been extensively explored among cybercriminals, for example digital piracy (Higgins et al., 2008; Holt and Copes, 2010), sexting (Renfrow & Rollo, 2014), cyberbullying (Vysotsky & McCarthy, 2017), cyberstalking (van Baak et al., 2022) and computer hacking (Chua and Holt, 2016; Morris, 2011). In sum, prior neutralization literatures are focused on (1) the relevance of those neutralization techniques in predicting the offending outcomes, (2) the specific technique that offenders prefer (e.g., Chua and Holt (2016) found that hackers tend to use denial of responsibility & injury, but not appeal to higher loyalties), (3) external causes for using/learning neutralizations (i.e., situations or peers), (4) use of neutralizations among interrogation practices. What has been absent from the literature, specifically those studying cybercriminals, is to understand the inner mechanism of deploying neutralizations during the commission of crime by using first-hand experimental dataset obtained from active cybercriminals.

With attempt to address the above limitation, study three intends to explore whether online romance scammers would neutralizations and if they do, how do those neutralizations work. The unique findings presented in this study, which serve as a logical extension of neutralization, find variations in offenders' use of neutralization, and further identify that offenders' use of neutralization and accounts serve for altercasting victims' identities and the situations in the way that facilitate the crime commission process. Stated differently, the outcomes from this study not only expand the scope of neutralizations to online romance scams,

but also point out that neutralization can similarly use during the crime and understand the inner workings of neutralization and grooming among romance scammers.

In sum, the theoretical frameworks proposed and deployed in this dissertation, along with the findings observed from a series of analysis, emphasizes the value of using interdisciplinary approaches in studying the rationality of online fraudsters. Indeed, scholars have long applied those models and theories in criminological and communicational literature for studying individuals' behaviors in deviant and non-deviant online and offline environments (e.g., Cornish and Clarke, 2017; Ngo and Paternoster, 2011; Perkins and Howell, 2021; Maimon, Santos and Park, 2019; Bossler and Berenblum, 2019; Barnor et al., 2020). Nevertheless, this research is the first to integrate psychological, communicational, and situational explanations in the study of a unique cybercrime (i.e., online romance scam), as well as to prove the rationality of fraudsters' behaviors in cyberspace. Importantly, while this research is conducted on female fraudsters reported by victims, I believe its theoretical arguments could also be applied to study romance fraudsters operating on other platforms and in other cultural contexts. I will further elaborate on the possible avenues for future research in discussing future research ideas and directions.

Policy Implications

This dissertation highlights two key implications for improving evidence-based cybersecurity initiatives. If online romance scammers and potential victims are rational actors, this research suggests that incidents of online romance fraud can be thwarted through targeted online deterrent and educational messaging. First, since offenders are found to rationally change their behaviors when facing sanctions and rewards, one of the ways that OSP can do is to use word matching algorithm or similar approach in which certain words or string of words (i.e., "money", "bank", "send me money", "crisis") can trigger specific warning mechanism. When

the system is triggered, the platform can either automatically remove fraudsters' profile or flag their profiles before transferring to relevant personals to manually check and make decisions. In the sametime, a warning banner can simultaneously appear on victims' screens, alerting them the stranger they chat online could be potential romance scammers and please do not send money or share any personal information. By using similar algorithm, and if with sufficient and advanced technical resources, OSP can cooperate with law enforcement and send those fraudsters warning messages to nudge their subsequent behaviors once the fraud system is triggered by certain words. In the same token, previous research by Maimon and colleagues (2019& 2020) demonstrates fraudsters' use of specific urgency cues when deceiving their victims. Resultantly, it could be possible that online romance fraudsters may also engage specific urgency cues when holding conversations with victims. Moreover, researchers also found that the actual IP address and time zone that fraudsters situate are different from the ones they claim to be victims (e.g., Edwards et al., 2018; Suarez-Tangil et al., 2019). Thus, future algorithms embedded in various online platforms (e.g., social media, dating apps) that serve for alerting the conversation should be more rigorous and comprehensive in identifying fraud actions from different perspectives, for example, different cues, date of time, and IP address. Nevertheless, organizations and OSP should be cautious about the potential concerns posed by surveillance and privacy. It is recommended that they should initiate steps in determining whether privacy is protected in artificial intelligence deployments. Most importantly, those organizations can address the potential risks and concerns more obliquely through identifying specific algorithmic discrimination in the contract with users.

The second main take-away from this dissertation that can implicate a potential policy is that majority so called "voluntary" behaviors from victims are not from their conscious

willingness, but rather are influenced by fraudsters' discourses. As the result, there needs to be a dismantling of victim-blaming attitudes and a supportive environment is needed for the healing process of online romance scams victims. A number of prior studies have indicated that similar to gender-based violence in physical space (e.g., sexual assault, domestic violence), offenders tend to use similar grooming/social engineering techniques to manipulate their victims and the aftermath of these incidents typically involve with substantial psychological/emotional trauma. Findings from the current studies have supported this notion and further indicate the type of grooming and neutralization techniques fraudsters would use to maximize the potential benefits from vulnerable victims. Up to date, a few victim-assistance programs has been developed for gender-based violent crimes, for example domestic violence. However, current initiatives in aiding the recovery of online romance victims are established mostly by non-governmental agencies (e.g., The Coalition, The ACFE Insights, Romancescamsurvivors.org). A similar proposal of victim assistance programs should also be initiated by governmental agencies. Except offering free or low-cost counseling therapeutic services carried out by trained personnel to online romance scams victims, other aspects should also be simultaneously improved. For example, in terms of the incidental reports, there needs to have a formalized agency training towards online romance scams and its harm. The purpose is to have law enforcement officers trained to comprehend the stress & hardships that online romance scams victims experience and provide appropriate reporting services to victim that aim not to humiliate and re-victimize individuals (see also, Button et al., 2009b). Moreover, there potentially can open multiple channels for reporting online romance scams incidents, for example through counseling services or medical practitioners, which can be more comfortable reporting approaches for victims (e.g., Cross, 2018). In terms of the financial aspect, despite having the bank to try to trace back the

defrauded money, government should provide temporary financial assistance with restitution and compensations to victims (specifically those elders) who are possibly experiencing bankruptcy.

Social organizations (e.g., non-profit, law enforcement, or service providers) should also provide appropriate training to potential victims of an online romance scam and their close family members. Previous studies and the current three papers in this dissertation provide a detailed understanding of who is more likely to be tricked by online romance fraudsters and the modus operandi of those offenders (e.g., Whitty, 2013a and 2015; Wang et al., 2021; Wang & Topalli, 2022). The observations drawn from these studies can help in the development of effective education and prevention programs (e.g., government online safety websites and safety alerts on dating sites) in order to raise awareness among users about the potential scamming incidents that may happen throughout the conversation they hold with strangers online (e.g., Whitty, 2019). Moreover, as Cross and colleagues (2018) and Carter (2020) study pointed out, despite using different manipulative psychological strategies to influence victims' willingness to give out money, fraudsters also attempt to use visceral responses to generate fear and isolation among victims that deprive their accesses to outside resources of supports. Drawn from this observation, society should also endeavor to create specific awareness programs for the general public about the potential signs (e.g., depression, unwilling to share) they should watch out for when having someone in a household stay online or with their phones for quite a long time. By developing training programs for potential victims and their close relatives, online romance scam can be prevented before it becomes unmanageable.

Limitations and Future Research

Although the current work provides insights into online romance scammers and offers in-depth analysis of offenders' rationality, notable limitations exist. To better demonstrate them in a

structured and inclusive approach, limitations will be discussed in two main points: (1) issues with selected methodology and (2) issue with the sample.

The first limitation concerns the selected methodology, and such a limitation can be observed across three different papers. The scoping review methodology used in chapter 2, as described by majority scholars, can pose potential issues with less defined research, comprehensiveness of selected studies, and requiring exhaustive resources (i.e., manual search). In this current study, as the main research aim is to understand all current existed literature in online romance scams in social science spectrum, this less defined or limited research aims and questions can lead researchers to manually look into almost every social science database that may contain relevant studies, especially those composed with foreign languages. Moreover, potential limitation is also presented when there does not appear to have an exhaustive examination of all included study. Although two researchers are presented, however due to limited time resources, the second author is only able be review the 20% of English-language studies that are randomly assigned by the first author. Despite those drawbacks, scoping review approach is the only synthesis approach that fits the best to the limited numbers (< 50) of online romance scams literature. In addition, similar to systematic review and meta-analysis, Tricco and colleagues (2018) have established checklists for conducting rigorous scoping review under the PRISMA extension. In sum, although presenting potential limitations, this approach is scientific and most appropriate for synthesizing the current literature for the identified cybercrime.

The experimental methodology used in the rest two studies also present several issues. The most problematic issue is with the controlled environment. Unlike the system trespassing experiment conducted by Maimon and colleagues (2014), it is almost impossible to use one set of honeypot to attract all romance scammers to one space (i.e., computer interface) and observe

their changes of behaviors. Therefore, controlled environment is unobtainable in current two experiments. Such an issue can pose two main issue: one is with the temporal order of fraudsters' responses, or in other word whether they respond to the probing questions instantly or have certain delayed periods; second is that there is no way to tell whether fraudsters realized that they were not chatting with an actual victims but honeypot-driven questions. The prior issue is not likely to tamper the results of both studies as duration of time is not counted as an independent variable for assessment. Admittedly, the latter one can potentially contaminate results; however, it could be overcome by initiating similar experiments in a controlled setting by recruiting fraudsters from state or federal prisons (will be discussed in later section). Another issue is that it could be the case that the "dosage" of the treatment (i.e., the amount of money) is simply not enough to receive significant behavioral changes by subjects. Specifically, offering amazon gift cards with greater amounts or sending money directly to their bank accounts or money apps (i.e., PayPal or Cash App) can produce different results. Related to this, using different probing questions with varied tones (i.e., determinant or uncertain) may also result in different behavioral changes.

The second limitation concerns with the issues of our sample. In the scoping review paper, incorporating empirical studies written in Chinese analyzing online romance scams can certainly boost the comprehensiveness of the search, however it can pose additional constraints. For example, as the primary author is the only one proficient in Chinese, thus when selecting, interpretating and summarizing Chinese studies, there might present the issues with objectivity. In the following two experimental studies, despite the fact that the research design allows researchers to understand the inner operations of online romance scammers, however there are several backfalls concerning with the sample used in both studies. First, it could be possible that

two or more email address may be controlled or supervised by the same individual. If that is the case, it could be possible that some fraudsters are simply playing around with us, rather than seeing us as the real victims. And such a potential consequence may threaten the validity of our study. Second, although the authenticity and legitimacy of the reports on *stop-scammers.com* have been assured by the admins and confirmed by the initial pilot studies, some of the email addresses that received email messages from us may still have been inappropriately listed on the website, which can contaminate the validity of the findings. Whereas, if this happens, the incorporation of non-fraudster sample would only deflate, rather than inflate, the findings presented. Third, researchers are unable to observe if fraudsters may be suspicious in receiving the first email from us because there are no evidences that we had conversations before. Therefore, if it is the case, these experimental studies are unlikely to observe the natural responses from fraudsters when they conduct actual email fraud against victims. Fourth, as we only extracted email addresses belonging to "female fraudsters" on only stop-scammers.com, such a selection procedure may present the issue with generalizability as only female personas are chosen. Our results may only apply to certain groups of fraudsters who claim them to be female but not those who claim them to be male. Similarly, fraudsters who operated on other platforms (i.e., dating apps or social media platform) or using other approaches (i.e., use investment platforms and cryptocurrency) to deceive their victims may deploy operational strategies than those observed in current sample.

Admittedly, the extant of these limitations may bring up issues with validity concerning the methodology and sample in these three paper, nevertheless, both papers made attempts to address current gaps in online romance scams literature and the bulk of these limitation can, and should be addressed in the future studies. Firstly, the limitation with the scoping review

methodology can be remedied by using either systematic review or meta-analysis to carry out similar review studies, however under the premise that there can be more quantitative or experimental studies in online romance scams. The fact is that there indeed has an increased attention from scholars to the problem of online romance scams. Relevant studies have appeared to indicate a trend which initially focus on being narratives/descriptive to explore more opportunities to discover valuable datasets (i.e., Topalli and Wang, 2022; Wang and Zhou, 2022; Cross and Lee, 2022; Cross and Layt, 2022). Thus, it certainly should be anticipated that future online romance scams review studies may overcome the current limitations presented by scoping review and use more synthesized approaches to demonstrate enhanced understandings towards this complex cybercrime. Secondly, the limitations with experimental approach can be addressed by (1) recruiting fraudsters from state or federal prisons, (2) increasing the "dosages" of treatments, and (3) conduct similar experiment on different platforms. In details, recruiting inmates who previously carried out online romance scam schemes can potentially assist in overcoming the issue of controlled environment. Such an approach requires researchers to establish certain connections with prison agents and make request on gathering offenders to participate in an online experiment (i.e., limited access to internet) where they will chat with researchers using pre-designed questions. Despite a number of potential hiccups with IRB and the internal permission from prison agencies, however this approach is possible and can be an ideal one to set experiment in a controlled setting to observe fraudsters' behaviors. With regards to operationalize the dosages of treatments and platforms, researchers in the future, if want to continue using experiments to incentivize or nudge offenders, can attempt to increase the amount of rewards sent to fraudsters or increase the differences of rewards sent to two or more groups of fraudsters. This approach can actualize the experiment setting and lessen the suspicions that

fraudsters may have towards the conversation. It can allow researchers to collect more information and authenticated data from fraudsters. Administering future experiments on different platforms, specifically those have higher or low surveillances, may enable researchers to observe any differences on the behavioral changes exhibited by online romance scammers. Such data could be used to determine if different platforms with different features may alter fraudsters' behaviors when facing potential reward or sanction cues.

Thirdly, future research should also consider recruiting more personals who are fluent not only in English but also other languages to (1) review all included studies, (2) provide assistances to translate and screen studies in foreign languages. Despite the type of review methodology that future scholars will use, both proposed approaches concerning increasing personals can help to achieve higher validity and objectivity when reviewing and screening for appropriate studies. Lastly, concerning the sample limitation existed in the experimental researches, it is unknown, for example to know if the emails are controlled by same or different individuals. Additionally, it is also unclear for future research to explore if the information for the fraudster is inappropriately listed on the website. And of course, knowing fraudsters' reactions when receiving the probing questions from scholars is also unobtainable as it is simply not possible to observe their actual responses when we are not in the same space. However, what future scholars can do to improve the sample selection is to incorporate diverse groups of fraudsters from different cultural contexts and genders operating on different OSP and financial platforms. The purpose is to see if those external differences can make specific impacts on fraudsters' responses toward rewards and sanctions. Specifically, prior studies have identified that cultural identity and engagement can significantly influence individuals' engagement in violent offending (e.g., Shepherd et al., 2018; Salvatore & Taniguchi, 2021; Posick & Gould,

2015). One previous study by Wang and Zhou (2022) identified that scammers operating in China use contrasted social engineering techniques as those operated in the Western context. As a result, one speculation that future researchers can have, particularly for those fraudsters who operated in another country, is the potential variability with cultural contexts could exert a more decisive influence on fraudsters' behaviors, for example, their selections of targets, their coping strategies with sanction and rewards and their manipulative strategies. Despite such speculation, additional research should be carried out if the potential observed behavior variations result from the social context or the sub-culture context within the criminal syndicates.

What's more, the current analysis of fraudsters' behaviors uses either experimental data or the interview/report data from victims (i.e., Wang et al., 2021; Whitty, 2013a & 2013b), future studies can attempt to obtain first or second-hand data through collaborating with law enforcement. One way of doing this is to interview fraudsters who were locked in state or federal prisons. Potential future projects that can be initiated can be relevant to the life trajectory of offenders or persistence & desistance of fraud operations. Moreover, it is also plausible to use offender data collected by law enforcement agencies, such as IC3, to make sense of offenders' strategic operations (i.e., who and why they target specific groups of victims).

Summary and Conclusion

Online romance scams have been consistently reported as a pressing issue, both in the U.S and board. However, sociological, psychological, criminological explanations of this phenomenon tend to largely emphasize on either fraudsters' general operations, deployed linguistic techniques or the vulnerable victimization factors in promoting the progressions of online romance scam incidents. In an attempt to generate a more comprehensive understanding of the behaviors of online romance fraudsters, I proposed a three-paper dissertation, one that

serve as early attempts to address several gaps existed in online romance scams and use interdisciplinary perspectives to garner insights into the rationality of fraudsters in cyber-environment. The current project first used the crime triangle to structure the scoping review study on current existed literature in online romance scams. Based on the proposed theoretical gap, using experimental methodology to collect fraudsters' responses and analyze datasets using appropriate approach, the following two studies employed theories derived from the criminological and communicational literature to demonstrate fraudsters' rationality. Specifically, results indicate that fraudsters strategically change their behaviors when facing rewards from different levels. Most importantly, they will use neutralizations during the criminal process to altercast victims' identities and situations to maximize the potential rewards.

As a result, future review studies can potentially advance their methodologies (i.e., meta-analysis and systematic review) based on the gradual increased empirical literature in online romance scams. Moreover, scholars who wish to continue using experiments to study offending patterns should engage in rigorous research practices, aiming to overcome the limitations presented in current two studies. Following practices initiated by Whitty (2013a and 2013b) and Cross and colleagues (2021 and 2022), online romance scams researchers should increase communications and connections with law enforcement agencies and cybersecurity industry to utilize the current unexplored datasets and empirical outcomes to make recommendations and introduce evidence-based approach to cybersecurity. Admittedly, online romance scams are such a complex worldwide crime. Thus, only by gathering efforts from academia, law enforcement and private industry can we see an obvious reduction of harms caused by this crime and its subsets (i.e., sextortion and blackmail)

List of References

ABC News (2014). *Nigerian police arrest online scammer linked to death of Australian woman Jette Jacobs*. https://www.abc.net.au/news/2014-02-04/nigerian-police-arrest-online-scammer-linked-to-australian27s-/5236188

ABC News (2021). *'Dating scammer' faces more time after escape, capture*. https://abcnews.go.com/Weird/wireStory/dating-scammer-faces-time-escape-capture-76472314.

Abele, A., & Petzold, P. (1994). How does mood operate in an impression formation task? An information integration approach. European Journal of Social Psychology, 24(1), 173-187.

Abu-Alhaija, A. S. A., Yusof, R. N. R., Hashim, H., & Jaharuddin, N. S. (2018). Religion in consumer behaviour research: the significance of religious commitment and religious affiliation. *International Journal of Economics, Commerce and Management*, *6*(1), 245-258.

Agnew, R. S. (1985). Neutralizing the impact of crime. *Criminal justice and behavior*, *12*(2), 221-239.

Agnew, R. (1994). The techniques of neutralization and violence. *Criminology*, *32*(4), 555-580.

Ahmed, E., Harris, N., Braithwaite, J., & Braithwaite, V. (2001). *Shame management through reintegration*. Cambridge University Press.

Alvarez, A. (1997). Adjusting to genocide: The techniques of neutralization and the Holocaust. *Social Science History*, *21*(2), 139-178.

Anderson, A. L., & Meier, R. F. (2004). Interactions and the criminal event perspective. *Journal of Contemporary criminal justice*, *20*(4), 416-440.

Anesa, P. (2020). "Lovextortion: Persuasion strategies in romance cybercrime." *Discourse, Context & Media* 35.

Archer, A. K. (2012). *"I Made a Choice": Exploring the Persuasion Tactics Used by Online Romance scammers in Light of Cialdini's Compliance Principles*. [Master Thesis, Regis University]. Criminology Common.

Bachman, R., Paternoster, R., and Ward, S. (1992), 'The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault', *Law and Society Review*, 26/2: 343-372.

Backman, C. W. (1985). Interpersonal congruency theory revisited: A revision and extension. *Journal of Social and Personal Relationships*, *2*(4), 489-505.

Barnor, J. N. B., Boateng, R., Kolog, E. A., & Afful-Dadzie, A. (2020). Rationalizing Online Romance scams: In the Eyes of the Offender. *AMCIS 2020 Proceedings. 21*. https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/21.

Baumer, E. P., and Gustafson, R. (2007), 'Social organization and instrumental crime: Assessing the empirical validity of classic and contemporary anomie theories', *Criminology*, 45/3: 617-663.

Baúto, R. V., Cardoso, J., & Leal, I. (2022). Child Sexual Offenders Typologies: An Exploratory Profile Model using Multiple Correspondence and Cluster Analysis of Portuguese Convicted Offenders Sample. *Journal of Forensic Psychology Research and Practice*, *22*(4), 331-356.

Beckhouse, L., Tanur, J., Weiler, J., & Weinstein, E. (1975). ... And some men have leadership thrust upon them. *Journal of Personality and Social Psychology*, *31*(3), 557.

Benson, M. L. (1985). Denying the guilty mind: accounting for involvement in a white-collar crime. *Criminology*, *23*(4), 583-607.

Berkowitz, L. (2000). *Causes and consequences of feelings*. Cambridge University Press

Bernstein, E. (2016, September 06). On relationships: If you want to persuade people, try 'altercasting' — Appealing to others' vanity can foster cooperation, psychologists say; beware the fine line to manipulation. *Wall Street Journal*.

Bohner, G., Reinhard, M. A., Rutz, S., Sturm, S., Kerschbaum, B., & Effler, D. (1998). Rape myths as neutralizing cognitions: Evidence for a causal impact of anti-victim attitudes on men's self-reported likelihood of raping. *European Journal of Social Psychology*, *28*(2), 257-268.

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, *42*(5), 495-499.

Breeze, R. (2012). Legitimation in corporate discourse: Oil corporations after Deepwater Horizon. *Discourse & Society*, *23*(1), 3-18.

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scams: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261-283.

Budd, C., & Anderson, J. (2011). *Consumer fraud in Australasia: Results of the Australasian consumer fraud taskforce online Australia surveys 2008 and 2009*. Australian Institute of Criminology.

Buller, D. B., Hunsaker, F., and Aitken, J. (1995), 'Interpersonal deception: XIII. Suspicion and the truth-bias of conversational participants', *Intrapersonal communication processes reader*, 237-257.

Buller, D. B., & Burgoon, J. K. (1996), 'Interpersonal deception theory', *Communication theory*, 6/3: 203-242.

Burgoon, J. K., & Buller, D. B. (2015). Interpersonal deception theory: Purposive and interdependent behavior during deceptive interpersonal interactions. *Engaging theories in interpersonal communication: Multiple perspectives*, 349-362.

Buse, W. (2005). Spam scams: Africa's city of cyber gangsters. Hamburg: Der Spiegel. https://www.spiegel.de/international/spiegel/spam-scams-africa-s-city-of-cyber-gangsters-a-384317.html.

Butler, L. C., Graham, A., Fisher, B. S., Henson, B., & Reyns, B. W. (2022). Examining the effect of perceived responsibility on online bystander intervention, target hardening, and inaction. *Journal of interpersonal violence*, *37*(21-22), https://doi.org/10.1177/08862605211055088

Button, M, Lewis, C, and Tapley, J. (2009). *Fraud Typologies and the Victims of Fraud: Literature Review*. Portsmouth, UK: University of Portsmouth.

Byers, B., Crider, B. W., & Biggers, G. K. (1999). Bias crime motivation: A study of hate crime and offender neutralization techniques used against the Amish. *Journal of Contemporary Criminal Justice*, *15*(1), 78-96.

Campbell, A. M. (2009). False faces and broken lives: An exploratory study of the interaction behaviors used by male sex offenders in relating to victims. *Journal of Language and Social Psychology*, *28*(4), 428-440.

Canadian Anti-Fraud Centre (2022). *Canadian Anti-Fraud Centre secures $32,000 for romance scams victim.* https://www.antifraudcentre-centreantifraude.ca/features-vedette/2022/02/romance-rencontre-eng.htm.

Carlson, J. R., George, J. F., Burgoon, J. K., Adkins, M., and White, C. H. (2004), 'Deception in computer-mediated communication', *Group decision and negotiation*, 13/1: 5-28.

Carter, E. (2021). Distort, extort, deceive and exploit: Exploring the inner workings of a romance scams. *The British Journal of Criminology, 61*(2), 283-302.

CBC News (2021), 'Romance scams bilked Huron County senior out of $700K', available online at https://www.cbc.ca/news/canada/london/huron-county-romance-scam-senior-1.6104450#:~:text=Statistics%20from%20the%20Canadian%20Anti,pretending%20to%20be%20in%20love.

Cheah, P. K., Unnithan, N. P., & Raran, A. M. S. (2020). Rehabilitation programs for incarcerated drug offenders in Malaysia: Experience-based perspectives on reintegration and recidivism. *The Prison Journal, 100*(2), 201-223.

Chibnall, S., & Saunders, P. (1977). Worlds apart: Notes on the social reality of corruption. *The British Journal of Sociology, 28*(2), 138-154.

China Daily (2019). *Top New Vocabulary in December 2019*. Retrieved from https://baijiahao.baidu.com/s?id=1654485997076525761&wfr=spider&for=pc.

Chopin, J., & Beauregard, E. (2020). Elderly sexual abuse: An examination of the criminal event. *Sexual Abuse, 32*(6), 706-726.

Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders, 11*(4), 534-555.

Cialdini, R. B. (1984). Influence: The Psychology of Persuasion, William Morrow.

Clarke, R. V., and Cornish, D. B. (1985), 'Modeling offenders' decisions: A framework for research and policy', *Crime and justice*, 6: 147-186.

Clark, J. (2022). UK victims lost £1.3bn in 2021 amid surge in online fraud, new data shows. *The Guardian*. https://www.theguardian.com/money/2022/jun/29/uk-victims-lost-13bn-in-2021-amid-surge-in-online-new-data-shows#:~:text=The%20amount%20lost%20to%20romance,41%25%20at%203%2C270%20last%20year.

Cochran, W. G. (1954), 'Some methods for strengthening the common χ 2 tests', *Biometrics*, 10/4: 417-451.

Cohen, L. E., & Felson, M. (1979). On estimating the social costs of national economic policy: A critical examination of the Brenner study. *Social indicators research*, 251-259.

Coleman, J. W (1994). *Neutralization Theory: An Empirical Application and Assessment.* [Ph.D. Dissertation, Oklahoma State University]. Stillwater.

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

Communal News (2020). New Internet Fraud on the Rise in China. Retrieved from https://communalnews.com/new-internet-fraud-on-the-rise-in-china/.

315 Consumer Association (2020). *Sha Zhu Pan* scam regains its force: the love of millions in debt is just a "misunderstanding". Retrieved from https://weibo.com/ttarticle/x/m/show/id/2309404582430601248861?_wb_client_=1&obj

ect_id=1022%3A230940458243060124886 1&extparam=lmid--4582430600338773&luicode=10000011&lfid=1076035784133871.
Copes, H. (2003). Societal attachments, offending frequency, and techniques of neutralization. *Deviant Behavior*, *24*(2), 101-127.

Copes, H., Hochstetler, A., & Sandberg, S. (2015). Using a narrative framework to understand the drugs and violence nexus. *Criminal Justice Review*, *40*(1), 32-46.
Copes, H., Vieraitis, L., & Jochum, J. M. (2007). Bridging the gap between research and practice: How neutralization theory can inform Reid interrogations of identity thieves. *Journal of Criminal Justice Education*, *18*(3), 444-459.

Copley, L. (2014). Neutralizing their involvement: Sex traffickers' discourse techniques. *Feminist Criminology*, *9*(1), 45-58.

Cornish, D.B., and Clarke, R. V. (2014), *The Reasoning Criminal: Rational Choice Perspectives on Offending.* Transaction Publishers: London.
Cornish, D. B., & Clarke, R. V. (2017). Understanding crime displacement: An application of rational choice theory. In *Crime opportunity theories* (pp. 197-211). Routledge.

Council of Europe. (2004). Organized Crime Situation Report 2004: Focus on the Threat of Cybercrime. Retrieved on October 15, 2005, from https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Organised%20Crime%20Situation%20Report%202004.pdf.
Cressey, D.R. (1953), *Other People's Money: The Social Psychology of Embezzlement*, The Free Press, New York, NY.
Cressey, D. R. (1973). *Other People's Money. Montclair*. New Jersey: Patterson Smith.
Cromwell, P., & Thurman, Q. (2003). The devil made me do it: use of neutralizations by shoplifters. *Deviant Behavior*, *24*(6), 535-550.

Cross, C., & Holt, T. J. (2021). The use of military profiles in romance scams schemes. *Victims & Offenders*, *16*(3), 385-406.
Cross, C., & Layt, R. (2022). "I Suspect That the Pictures Are Stolen": Romance scams, Identity Crime, and Responding to Suspicions of Inauthentic Identities. *Social Science Computer Review*, *40*(4), 955-973.
Cross, C., & Lee, M. (2022). Exploring fear of crime for those targeted by romance scams. *Victims & Offenders*, *17*(5), 735-755.
Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends and issues in crime and criminal justice*, (474), 1-6.
Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187-204.

Cross, C., & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing: A Journal of Policy and Practice*, *9*(2), 119-128.
Cross, C. (2016), 'I'm anonymous, I'm a voice at the end of the phone': A Canadian case study into the benefits of providing telephone support to fraud victims', *Crime Prevention and Community Safety*, 18/3: 228–243.
Cross, C., Richards, K., Smith, R (2016). *Improving responses to online fraud victims: An examination of reporting and support*. Report to the Criminology Research Advisory Council. https://www.aic.gov.au/sites/default/files/2020-05/29-1314-FinalReport.pdf.

Cross, C. (2018). Denying victim status to online fraud victims: The challenges of being a "non-ideal victim.". *Revisiting the ideal victim concept*, 243-262.
Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, *55*, 1-12.
Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance scams: Insights from domestic violence research. *The British Journal of Criminology*, *58*(6), 1303-1322.
Cross, C. (2020). Romance scams. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 917-937.
Cukier, W. & Levin, A. (2009). Internet Fraud and Cyber Crime. In F. Schmalleger & M. Pittaro. (Eds.), Crimes of the Internet (pp. 251-279). New Jersey: Pearson Prentice Hall.
Curry D. (2022). *App Data Report 2022.* Business of Apps. https://www.businessofapps.com/data/report-app-data/
Department of Homeland Security (2022). *Cybersecurity*. https://www.dhs.gov/topics/cybersecurity.
Deibert, G. R., & Miethe, T. D. (2003). Character contests and dispute-related offenses. *Deviant Behavior*, *24*(3), 245-267.
Dibdin, E (2019). *A Complete Timeline of the Events of Dirty John*. Bazaar: Reports. https://www.harpersbazaar.com/culture/film-tv/a25372275/dirty-john-true-story-timeline/.
Dickerson, S., Apeh, E., & Ollis, G. (2020). Contextualised Cyber Security Awareness Approach for Online Romance scams. In *2020 7th International Conference on Behavioural and Social Computing (BESC)* (pp. 1-6). IEEE.
Dickinson, T. (2017). Non-violent threats and promises among closed-market drug dealers. *International Journal of Drug Policy*, *42*, 7-14.
Dickinson, T., & Jacques, S. (2019). Drug sellers' neutralizations of guiltless drug sales and avoidance of "drug dealer" identities. *International Journal of Drug Policy*, *73*, 16-23.

Dreijers, G & Rudzisa, V. (2020). Devices of textual illusion: victimization in romance scams e-letters. *Research in Language*, *18*(1), 1-13. DOI: 10.18778/1731-7533.18.1.01.
Duhatschek, P. (2022). Toronto woman loses life savings in romance scams, warns others to 'be careful'. *CBC News*. https://www.cbc.ca/news/canada/toronto/toronto-woman-loses-life-savings-in-romance-scam-warns-others-to-be-careful-1.6347076.
Duron, J. F., Johnson, L., Hoge, G. L., & Postmus, J. L. (2021). Observing coercive control beyond intimate partner violence: Examining the perceptions of professionals about common tactics used in victimization. *Psychology of violence*, *11*(2), 144.

Edwards, M., de Tangil Rotaeche, G. N. S., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2018, May). The geography of online dating fraud. In *Workshop on technology and consumer protection (ConPro)*. https://doi.org/https://www.ieee-security.org/TC/SPW2018/ConPro/.
Eriksen, C. W., & Pierce, J. (1968). Defense mechanisms. *Handbook of personality theory and research*, 1007-1040.

Ermann, M. D., & Lundman, R. J. (2002). Corporate and governmental deviance. In M. D. Ermann & R. J. Lundman (Eds.), *Corporate and Governmental Deviance: Problems of Organizational Behavior in Contemporary Society* (pp. 3-49). New York: Oxford University Press.

Experian (2022). *2022 Global Identity and Fraud Report.* https://www.experian.com/content/dam/marketing/na/global-da/pdfs/GIDFR_2022.pdf.

Fendrich, M., Mackesy-Amiti, M. E., Goldstein, P., Spunt, B., & Brownstein, H. (1995). Substance involvement among juvenile murderers: Comparisons with older offenders based on interviews with prison inmates. *International Journal of the Addictions, 30*(11), 1363-1382.

Ferraro, K. J., & Johnson, J. M. (1983). How women experience battering: The process of victimization. *Social problems, 30*(3), 325-339.

FBI (n.d.). *Romance scams*. Retrieved from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/romance-scams.

Federal Trade Commission (2019), 'What you need to know about romance scams', available online at https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams.

Federal Trade Commission (2021), 'New Data Shows FTC Received 2.2 million Fraud Reports from Consumers in 2020', available online at https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.

Federal Trade Commission (2022). *New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021.* Retrieved from https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0.

Fiske, S. T. (1993). Controlling other people: The impact of power on stereotyping. *American psychologist, 48*(6), 621.

Fletcher, E (2021). *Romance scams take record dollars in 2020*. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020.

Forgas, J. P. (1992). Mood and the perception of unusual people: Affective asymmetry in memory and social judgments. European Journal of Social Psychology, 22(6), 531-547.

Fortin, F., Paquette, S., & Dupont, B. (2018). From online to offline sexual offending: Episodes and obstacles. *Aggression and violent behavior*, *39*, 33-41.

Fritsche, I. (2005). Predicting deviant behavior by neutralization: Myths and findings. *Deviant Behavior*, *26*(5), 483-510.

FX110 (2021). *The horrible aftermath of the Sha Zhu Pan scam: debts, ridicule and depression.* https://www.fx110.cool/special/5658.

Galdo, M. C., Tait, M. E., and Feldman, L. E. (2018), 'Money mules: Stopping older adults and others from participating in international crime schemes', *Dep't of Just. J. Fed. L. & Prac*, 66/7: 95-112.

Garrett, E. V. (2014). *Exploring internet users' vulnerability to online dating fraud: analysis of routine activities theory factors*. [Master Thesis, University of Texas Dallas]. ProQuest Dissertation Publishing.

Ghana-pedia.org (2009). *419 – Internet Dating Scams.* Retrieved September 2, 2009, from http://www.ghanapedia.org/org/index.php?option=com_content&task=view&id=29&Itemid=47.

Gibbs, J. P. (1975), *Crime, Punishment, and Deterrence.* New York: Elsevier.

Giordano, G. A., Stoner, J. S., Brouer, R. L., and George, J. F. (2007), 'The influences of deception and computer-mediation on dyadic negotiations', *Journal of Computer-Mediated Communication*, 12/2: 362-383.

Goffman, E. (1955). On face-work: An analysis of ritual elements in social interaction. *Psychiatry*, *18*(3), 213-231.

Goffman, E. (1959). *The presentation of self in everyday life*. New York, NY: Anchor Books.

Goldstein, P. J. (1985), 'The drugs/violence nexus: A tripartite conceptual framework', *Journal of drug issues*, 15/4: 493-506.

Goldstraw-White, J. (2011). *White-collar crime: Accounts of offending behaviour*. Springer.

Gottschalk, P. (2017). White-collar crime: Detection and neutralization in religious organizations. *International journal of police science & management*, *19*(2), 120-126.

Green, G.S (1997). *Occupational Crime*. Chicago, IL: Nelson-Hall Publishers.

Guadalupe-Diaz, X. L., & Anthony, A. K. (2017). Discrediting identity work: Understandings of intimate partner violence by transgender survivors. *Deviant Behavior*, *38*(1), 1-16.

Guadalupe-Diaz, X. L. (2019). *Transgressed: Intimate partner violence in transgender lives*. NYU Press.

Hancock, J. T., Curry, L. E., Goorha, S., and Woodworth, M. (2007), 'On lying and being lied to: A linguistic analysis of deception in computer-mediated communication', *Discourse Processes*, 45/1: 1-23.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113.

Hazama, K., & Katsuta, S. (2019). Cognitive distortions among sexual offenders against women in Japan. *Journal of interpersonal violence*, *34*(16), 3372-3391.

He, L.R (2018). Analysis on the necessity of adding the crime of cyber-fraud into Chinese legislation. *Social Scientist* 8(256): 108-113.

Heffernan, R., & Ward, T. (2015). The conceptualization of dynamic risk factors in child sex offenders: An agency model. *Aggression and Violent Behavior*, *24*, 250-260.

Higginson, J. G. (1999). Defining, excusing, and justifying deviance: Teen mothers' accounts for statutory rape. *Symbolic Interaction*, *22*(1), 25-44.

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Digital piracy: An examination of three measurements of self-control. *Deviant Behavior*, *29*(5), 440-460.

Hindelang, M. J. (1970). The commitment of delinquents to their misdeeds: do delinquents drift? *Social Problems*, *17*(4), 502-509.

Hirschi, T. (1969) Causes of Delinquency. Berkeley: University of California Press

Holguin, J. (2005). Beware Russian Web-Order Brides. Retrieved April 4, 2009, from http://www.cbsnews.com/stories/2005/04/14/eveningnews/main688311.shtml.

Holt, T. J. (2011). *Crime on-line: correlates, causes, and context*. Carolina Academic Press.

Holt, T. J. (2022). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*. https://doi.org/10.1016/j.chb.2022.107493.

Holt, T. J., & Copes, H. (2010). Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates. *Deviant Behavior*, *31*(7), 625-654.

Holtfreter, K., & Meyers, T. J. (2015). Challenges for cybercrime theory, research, and policy. *International and Transnational Crime*, 54.

Howell, C. J. (2021). *Self-Protection in Cyberspace: Assessing the Processual Relationship Between Thoughtfully Reflective Decision Making, Protection Motivation Theory, Cyber Hygiene, and Victimization.* [Graduate Theses and Dissertations, University of South Florida]. Scholar Common.

Huang, H. F & Paez F. M. (2019). China Cybersecurity Law Continues to Bring Enforcement Crackdown. *Jones Day*. https://www.jonesday.com/en/insights/2019/11/china-cybersecurity-law-continues-to-bring-enforce.

Huang, J., Stringhini, G., & Yong, P. (2015). Quit playing games with my heart: Understanding online dating scams. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 216-236). Springer, Cham.

Hudson, K. (2005). *Offending Identities: Sex Offenders' Perspectives of their Treatment and Management*. Cullompton: Willan Publishing.

IC3 (Internet Crime Complaint Center). (2022). *Federal Bureau Investigation Internet Crime Report 2021*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Jacques, S., Allen, A., and Wright, R. (2014). 'Drug dealers' rational choices on which customers to rip-off', *International Journal of Drug Policy*, 25/2: 251-256.

Jacobs, B. A. (1996), 'Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence', *Justice Quarterly*, 13/3: 359-381.

Jacobs, B. A. (2010), 'Deterrence and deterrability', *Criminology*, 48/2: 417-441.

Jacobs, B. A. (2010). Serendipity in robbery target selection. *The British Journal of Criminology*, *50*(3), 514-529.

Jacobs, B. A., and Cherbonneau, M. (2014), 'Auto theft and restrictive deterrence', *Justice quarterly*, 31/2: 344-367.

Jacobs, B. A., & Copes, H. (2015). Neutralization without drift: Criminal commitment among persistent offenders. *British Journal of Criminology*, *55*(2), 286-302.

Jacobs, B. A., Topalli, V., & Wright, R. (2000). Managing retaliation: Drug robbery and informal sanction threats. *Criminology*, *38*(1), 171-198.

James, V., & Gossett, J. (2018). Of monsters and men: Exploring serial murderers' discourses of neutralization. *Deviant Behavior*, *39*(9), 1120-1139.

Järvinen, M., & Kessing, M. L. (2021). Self-casting and alter-casting: Healthcare professionals' boundary work in response to peer workers. *Current Sociology*, 00113921211048532.

Jeffries, S., & Chuenurah, C. (2019). Vulnerabilities, victimisation, romance and indulgence: Thai women's pathways to prison in Cambodia for international cross border drug trafficking. *International Journal of Law, Crime and Justice*, *56*, 39-52.

Johnson, B. D., and Natarajan, M. (1995), 'Strategies to avoid arrest: Crack sellers' response to intensified policing', *Crime Prevention Studies*, 11: 273-298.

Joleby, M., Lunde, C., Landström, S., & Jonsson, L. S. (2021). Offender strategies for engaging children in online sexual activity. *Child Abuse & Neglect*, *120*, 105214.

Kalbfleisch, P. J. (1992), 'Deceit, distrust and the social milieu: Application of deception research in a troubled world', *Journal of Applied Communication Research*, 20/3: 308-334.

Kemper, T. D., and Collins, R. (1990), 'Dimensions of microinteraction', *American Journal of Sociology*, 96/1: 32-68.

Kim, H. Y. (2017), 'Statistical notes for clinical researchers: Chi-squared test and Fisher's exact test', *Restorative dentistry & endodontics*, 42/2: 152-155.

Klenowski, P. M., Copes, H., & Mullins, C. W. (2011). Gender, identity, and accounts: How white collar offenders do gender when making sense of their crimes. *Justice Quarterly*, *28*(1), 46-69.

Klenowski, P. M. (2012). "Learning the good with the bad" are occupational white-collar offenders taught how to neutralize their crimes?. *Criminal Justice Review*, *37*(4), 461-477.

Klockars, C. B. (1974). *The professional fence* (pp. 7899-7899). New York: Free Press.

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma, Violence, & Abuse*, *15*(2), 126-139.

Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology*, *9*(2), 205-217.

Kopp, C., Sillitoe, J., Gondal, I., & Layton, R.(2016a). Online romance scams: Expensive e-living for romantic happiness. *Proceedings of the 29th Bled eConference*, 175-189.

Kopp, C., Sillitoe, J., Gondal, I., & Layton, R. (2016b). The online romance scams: A complex two-layer scam. *Journal of Psychological and Educational Research*, *24*(2), 144.

Koon, H., Yoong, D. (2013). Preying on lonely hearts: a systematic deconstruction of an internet romance scammers's online lover persona. *Journal of Modern Language, 23*. 28-40.

Kopp, C., Sillitoe, J., & Gondal, I. (2021). "I am your perfect online partner" analysis of dating profiles used in cybercrime. *Asia Pacific Journal of Advanced Business and Social Studies*, *3*(2), 207-217.

Koon, H., Yoong, D. (2013). Preying on lonely hearts: a systematic deconstruction of an internet romance scammers's online lover persona. *Journal of Modern Language, 23*. 28-40.

Lea, S. E., Fischer, P., & Evans, K. M. (2009). *The psychology of scams: Provoking and committing errors of judgement.* Office of Fair Trading. https://ore.exeter.ac.uk/repository/bitstream/handle/10871/20958/OfficeOfFairTrading%202009.pdf?sequence=1&isAllowed=y.

Lemieux, V. (2003). Criminal Networks. Retrieved January 14, 2006, from http://www.rcmp.ca/ccaps/reports/criminal_net_e.pdf.

Leo, R. A. (1996). Miranda's revenge: Police interrogation as a confidence game. *Law and Society Review*, 259-288.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

Liu, L., Visher, C. A., & Sun, D. (2021). Do released prisoners' perceptions of neighborhood condition affect reentry outcomes?. *Criminal Justice Policy Review*, *32*(7), 764-789.

Loewenstein, G. (1996), 'Out of control: Visceral influences on behavior', *Organizational behavior and human decision processes*, 65/3: 272-292.

Lokatt, E., Holgersson, C., Lindgren, M., Packendorff, J., & Hagander, L. (2019). An interprofessional perspective on healthcare work: physicians and nurses co-constructing identities and spaces of action. *Journal of Management & Organization*, 1-17.

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thoughtfully reflective decision-making. *Journal of Research in Crime and Delinquency*, *54*(5), 639-679.

Loughran, T. A., Paternoster, R., Chalfin, A., and Wilson, T. (2016), 'Can rational choice be considered a general theory of crime? Evidence from individual-level panel data', *Criminology*, 54/1: 86-112.

Lyu, Z.W., (2018). How to Precisely Target Fraud in the Era of Big Data. *Social Governance*.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

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.

Maimon, D., Howell, C. J., Moloney, M., & Park, Y. S. (2020). An examination of email fraudsters' modus operandi. *Crime & Delinquency*, 0011128720968504.

Mao, J. D. (2020). Research on the countermeasures for detecting and preventing the "Sha Zhu Pan" telecom network fraud. *Journal of Hebei Vocational College of Public Security Police*, 20(3), 24-27.

Marcum, C. D., Higgins, G. E., Wolfe, S. E., & Ricketts, M. L. (2011). Examining the intersection of self-control, peer association and neutralization in explaining digital piracy. *Criminology, Criminal Justice, Law & Society*, *12*(3), 60.

Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards. *The British Journal of Criminology*, *60*(3), 559-578.

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research? *Crime and justice*, *32*, 221-320.

Maruna, S., & Copes, H. (2005). What have we learned from five decades of neutralization research? *Crime and justice*, *32*, 221-320.

Maruna, S. (2010), 'Mixed method research in criminology: Why not go both ways?', In Piquero R. A, and Weisburd, D, eds., *The Handbook of Quantitative Criminology*, 123-140, Springer, New York.

Matsueda, R. L., Kreager, D. A., and Huizinga, D. (2006), 'Deterring delinquents: A rational choice model of theft and violence', *American sociological review*, 71/1: 95-122.

Mayer, J. D., Gaschke, Y. N., Braverman, D. L., & Evans, T. W. (1992). Mood-congruent judgment is a general effect. *Journal of personality and social psychology*, *63*(1), 119.

Mayer, J. D., & Hanson, E. (1995). Mood-congruent judgment over time. *Personality and Social Psychology Bulletin*, *21*(3), 237-244.

McCall, G. J., & Simmons, J. L (1978). *Identities and Interactions*. Chicago, IL: University of Chicago Press.

McCarthy, B. (2002), 'New economics of sociological criminology', *Annual Review of Sociology*, 28/1: 417-442.
McGloin, J. M., and Thomas, K. J. (2016), 'Incentives for collective deviance: Group size and changes in perceived risk, cost, and reward', *Criminology*, 54/3: 459-486.
McGregor, S. L. (2008). Conceptualizing immoral and unethical consumption using neutralization theory. *Family and Consumer Sciences Research Journal, 36*(3), 261-276.

Meier, R. F., Kennedy, L. W., & Sacco, V. F. (2001). Crime and the criminal event perspective. *The process and structure of crime: Criminal events and crime analysis*, *9*, 1-28.
Minor, W. W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of research in crime and delinquency*, *18*(2), 295-318.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group*. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine*, *151*(4), 264-269.
Moore, R., & McMullan, E. C. (2009). Neutralizations and rationalizations of digital piracy: A qualitative analysis of university students. *International Journal of Cyber Criminology*, *3*(1), 441.
Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/.

Morris, R. G. (2011). Computer hacking and the techniques of neutralization: An empirical assessment. In *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 1-17). IGI Global.

Morris, R. G., & Higgins, G. E. (2009). Neutralizing potential and self-reported digital piracy: A multitheoretical exploration among college undergraduates. *Criminal Justice Review*, *34*(2), 173-195.

Mottner, S. (2007). Marketing and religion. *The Routledge companion to nonprofit marketing*, 92-107.

Nagin, D. S., and Paternoster, R. (1993), 'Enduring individual differences and rational choice theories of crime', *Law and Society Review*, 27/3: 467-496.
Nagin, D. S. (1998), 'Deterrence and incapacitation', In M. H. Tonry, eds, *The handbook of crime and punishment*, 345–368. Oxford University Press.
Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773.

Nothling, L. (2019). *Man posing as US soldier allegedly scams woman out of almost $400,000*. ABC News. https://www.abc.net.au/news/2019-01-11/romance-scam-man-charged-with-fraud/10707828.
O'Connell, R. (2003). *A typology of child cybersexploitation and online grooming practices.* Cyberspace Research Unit: University of Central Lancashire. https://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf.

Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W., & Asamoah, D. (2020). How Do Individuals Justify and Rationalize their Criminal Behaviors in Online Romance scams? *Information Systems Frontiers*, 1-17.

Offei, M. O. (2021). How does Victim Precipitation Theory explain Deviant Behaviours of Internet Romance Offenders? Gamer's Perspective of Victim Precipitation. *International Journal of Technology and Management Research*, *6*(2), 59-72.

Office of the comptroller of the currency (n.d.). *Type of consumer fraud*. https://www.occ.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/types-of-consumer-fraud.html#advance.

O'Key, S. (2008). *Looking for love? Keep an eye on your wallet*. Retrieved October 2, 2008, from http://www.cnn.com/2008/LIVING/04/21/romance.fraud/index.html.

Orbuch, T. L., Veroff, J., & Holmberg, D. (1993). Becoming a married couple: The emergence of meaning in the first years of marriage. *Journal of Marriage and the Family*, 815-826.

Orbuch, T. L. (1997). People's accounts count: The sociology of accounts. *Annual review of sociology*, 455-478.

Pak, J., & Zhou, L. (2014). Social structural behavior of deception in computer-mediated communication. *Decision Support Systems*, *63*, 95-103.

Pan, J., Winshester, D., Land, L., and Watters, P (2010), 'Descriptive data mining on fraudulent online dating profiles', paper presented at the 18th European conference on information system, available online at https://researchers.mq.edu.au/en/publications/descriptive-data-mining-on-fraudulent-online-dating-profiles.

Paternoster, R. (1987), 'The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues', *Justice Quarterly*, 4/2: 173-217.

Paternoster, R., and Pogarsky, G. (2009), 'Rational choice, agency and thoughtfully reflective decision making: The short and long-term consequences of making good choices', *Journal of Quantitative Criminology*, 25/2: 103-127.

Peachey, K. (2019). Scam victims to be refunded by banks. *BBC News*. https://www.bbc.com/news/business-48385426.

Peeters, M. A., & Rutte, C. G. (2005). Time management behavior as a moderator for the job demand-control interaction. *Journal of occupational health psychology*, *10*(1), 64.

Peretti-Watel, P., Guagliardo, V., Verger, P., Mignon, P., Pruvost, J., & Obadia, Y. (2004). Attitudes toward doping and recreational drug use among French elite student-athletes. *Sociology of Sport Journal*, *21*(1), 1-17.

Perkins, R. C., & Howell, C. J. (2021). Honeypots for cybercrime research. *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, 233-261.

Peterson, F., Pearce, A., Ferguson, A., & Langford, A. (2017). Understanding scoping reviews: Definition, purpose, and process. *Journal of the American Association of Nurse Practitioners, 29*(1), 12–16. https://doi.org/10.1002/2327-6924.12380

Pezzin, L. E. (1995), 'Earnings prospects, matching effects, and the decision to terminate a criminal career', *Journal of quantitative criminology*, 11/1: 29-50.

Piliavin, I., Gartner, R., Thornton, C., and Matsueda, R. L. (1986), 'Crime, deterrence, and rational choice', *American sociological review*, 15/1: 101-119.

Piquero, A., and Tibbetts, S. (1996), 'Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending', *Justice quarterly,* 13/3: 481-510.

Piquero, N. L., Tibbetts, S. G., & Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime.

Pino, N. W. (2005). Serial offending and the criminal events perspective. *Homicide Studies, 9*(2), 109-148.

Pogrebin, M., Stretesky, P. B., Prabha Unnithan, N., & Venor, G. (2006). Retrospective accounts of violent events by gun offenders. *Deviant Behavior*, *27*(4), 479-501.

Potter, T., (2022). Suffolk victims of 'romance scams' lose an average £13,500, study finds. *East Anglian Daily Times*. https://www.eadt.co.uk/news/crime/21274051.suffolk-victims-romance-scams-lose-average-13-500-study-finds/.

Presse-France, A. (2022). Global cost of cybercrime topped $6 trillion in 2021: defense firm. *The Barrons*. https://www.barrons.com/news/global-cost-of-cybercrime-topped-6-trillion-in-2021-defence-firm-01652198407.

Qiu, X. Y. (2019). The characteristics and prevention of network fraud crime—using gambling investment as an example. *Journal of Guangzhou Police College. 3*(3), 18-23.

Rege, A. (2009). "What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud." *International Journal of Cyber Criminology*, 3(2).

Rege, A (2013). A criminological investigation of online dating crimes. In *2013 APWG eCrime Researchers Summit* (pp. 1-9). IEEE. https://ieeexplore.ieee.org/abstract/document/6805773.

Reid, J. A., & Jones, S. (2011). Exploited vulnerability: Legal and psychological perspectives on child sex trafficking victims. *Victims and Offenders*, *6*(2), 207-231.

Renfrow, D. G., & Rollo, E. A. (2014). Sexting on campus: Minimizing perceived risks and neutralizing behaviors. *Deviant Behavior*, *35*(11), 903-920.

Reyns, B. W. (2017). Routine activity theory and cybercrime: A theoretical appraisal and literature review. *Technocrime and criminological theory*, 35-54.

Rinallo, D., & Alemany Oliver, M. (2019). The marketing and consumption of spirituality and religion. *Journal of Management, Spirituality & Religion*, *16*(1), 1-5.

Rogers, B. A. (2021). Inequitable Power Comes from and Creates Inequitable Structure: The Continued Relevance of Feminist Theory for Understanding Intimate Partner Violence in Transgender Lives. *Contemporary Sociology*, *50*(3), 197-201. https://doi.org/10.1177/00943061211006083a

Ross, S., & Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (420), 1-6.

Rush Burkey, C., & Ten Bensel, T. (2015). An examination and comparison of rationalizations employed by solo and co-offending female sex offenders. *Violence and Gender*, *2*(3), 168-178.

Saad, M. E., Abdullah, S. N. H. S., & Murah, M. Z. (2018). Cyber romance scams victimization analysis using Routine Activity Theory versus apriori algorithm. *International Journal of Advanced Computer Science and Applications*, *9*(12).

Sabo, K., & Chin, E. (2021). Self-care needs and practices for the older adult caregiver: An integrative review. *Geriatric Nursing*, *42*(2), 570-581.

SAGE Research Methods Datasets Part 2 (2017), 'Learn to Use Fisher's Exact Test in SPSS With Greater Manchester Police's Stop and Search Data', available online at https://methods.sagepub.com/base/download/DatasetStudentGuide/fishers-exact-gmss-2017#:~:text=Fisher\T1\textquoteright%20s%20Exact%20test%20is%20used,the%20analysis%20of%20small%20samples.

Scherer, K. R. (1984), 'On the nature and function of emotion: A component process approach', *Approaches to emotion*, 2293/317: 31.

Scott, M. B., & Lyman, S. M. (1968). Accounts. *American sociological review*, 46-62.

Shaari, A. H., Kamaluddin, M. R., Fauzi, W. F. P., & Mohd, M. (2019). Online-dating romance scams in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, *19*(1).

Shah, S. A., Azhar, S. M., & Bhutto, N. A. (2019). Halal marketing: a marketing strategy perspective. *Journal of Islamic Marketing*, *11*(6), 1641-1655. https://doi.org/10.1108/JIMA-11-2018-0211.

Shakeshaft, C. (2003). Educator sexual abuse. *Hofstra Horizons*, 10-13. https://www.hofstra.edu/pdf/orsp_shakeshaft_spring03.pdf.

Shakeshaft, C. (2004). *Educator sexual abuse: A synthesis of existing literature*. U.S. Department of Education, Office of the Under Secretary. http://www.ed.gov/rschstat/research/pubs/misconductreview

Shi, Y.A (2018). Personal Information Protection and Governance of Cyber Fraud. *Journal of National Prosecutors College* 25(6): 3-24.

Shields, I. W., & Whitehall, G. C. (1994). Neutralization and delinquency among teenagers. *Criminal Justice and Behavior*, *21*(2), 223-235.

Siebert, E. C., & Stewart, D. G. (2019). Neutralization technique use predicts delinquency and substance use outcomes. *Journal of substance abuse treatment*, *102*, 8-15.

Sigmon, J. N. (2008). Combating modern-day slavery: Issues in identifying and assisting victims of human trafficking worldwide. *Victims and Offenders*, *3*(2-3), 245-257.

Sina News (2019). An in-depth analysis of the *Sha Zhu Pan* scam: the trilogy of "pig hunting, pig nurturing and pig harvesting" in the "true-love" buchter-house. Retrieved from https://finance.sina.com.cn/tech/2021-09-27/doc-iktzscyx6617130.shtml.

Sitkin, S. B., & Bies, R. J. (1993). Social accounts in conflict situations: Using explanations to manage conflict. *Human relations*, *46*(3), 349-370.

Smith, G. R. et.al., (1999). Nigerian Advance Fee Fraud. *Trends and Issues in Crime and Criminal Justice*. (121): 1-6.

Smith, R. G., & Urbas, G. (2001). *Controlling fraud on the internet: A CAPA perspective*. Confederation of Asian and Pacific Accountants.

Smith, G., Button, M., Johnston, L., & Frimpong, K. (2010). *Studying fraud as white-collar crime*. Macmillan International Higher Education.

Spitzer, S. P., & Volk, B. A. (1971). Altercasting the difficult. *AJN The American Journal of Nursing*, *71*(4), 732-738.

Sorell, T., & Whitty, M. (2019). Online romance scams and victimhood. *Security Journal*, *32*(3), 342-361.

Stadler, W. A., & Benson, M. L. (2012). Revisiting the guilty mind: The neutralization of white-collar crime. *Criminal Justice Review*, *37*(4), 494-511.

Stark, E. (2012). Looking beyond domestic violence: Policing coercive control. *Journal of police crisis negotiations*, *12*(2), 199-217.

Stets, J. E., & Burke, P. J. (1996). Gender, control, and interaction. *Social Psychology Quarterly*, 193-220.

Stokes, R., & Hewitt, J. P. (1976). Aligning actions. *American sociological review*, 838-849.

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., and Whitty, M. T. (2019). 'Automatically dismantling online dating fraud', *IEEE Transactions on Information Forensics and Security*, 15: 1128-1137.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, *22*(6), 664-670.

Thomas, K. J., Loughran, T. A., and Hamilton, B. C. (2020), 'Perceived arrest risk, psychic rewards, and offense specialization: A partial test of rational choice theory', *Criminology*, 58/3: 485-509.

Tomita, S. K. (2000). Elder mistreatment: Practice modifications to accommodate cultural differences. *Journal of Multicultural Social Work*, *8*(3-4), 305-326.

Topalli, V. (2005). When being good is bad: An expansion of neutralization theory. *Criminology*, *43*(3), 797-836.

Topalli, V. (2006). The seductive nature of autotelic crime: How neutralization theory serves as a boundary condition for understanding hardcore street offending. *Sociological Inquiry*, *76*(4), 475-501.

Topalli, V., & Nikolovska, M. (2020). The future of crime: how crime exponentiation will change our field. *The Criminologist*, *45*(3), 1-8.

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., ... & Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. *Annals of internal medicine*, *169*(7), 467-473.

UK Finance (2021). *Romance scams on the up during lockdown*. https://www.ukfinance.org.uk/press/press-releases/romance-scams-during-lockdown.

Van Baak, C., Hayes, B. E., Freilich, J. D., & Chermak, S. M. (2018). Honor crimes in the United States and offenders' neutralization techniques. *Deviant Behavior*, *39*(2), 187-202.

Vandiver, D. M., Bowman, S., & Vega, A. (2012). Music piracy among college students: An examination of low self-control, techniques of neutralization, and rational choice. *Southwest Journal of Criminal Justice*, *8*(2), 92-111.

Vasquez, A., & Vieraitis, L. M. (2016). “It’s just paint”: Street taggers’ use of neutralization techniques. *Deviant Behavior, 37*(10), 1179-1195.

Vitola, M. N. (2018). *The Geese That Lay the Golden Eggs*, Litres.

Vysotsky, S., & McCarthy, A. L. (2017). Normalizing cyberracism: A neutralization theory analysis. *Journal of Crime and Justice, 40*(4), 446-461.

Xinhua Net (2019). *Sha Zhu Pan* scam investigations. Retrieved from http://www.xinhuanet.com/legal/2019-09/03/c_1124956701.htm.

Wang, F., Howell, C.J., Maimon, D., & Jacques, S. (2021). The restrictive deterrent effects of warning messages sent to active romance scamsters: an experimental approach. *International Journal of Cyber Criminology, 15*(1), 1-16.

Wang. X & Pan, X (2020). Research on telecom fraud crimes—taking “pig slaughtering” on the internet as an example. *Legality Vision*, 17-21.

Wang, S. L (2009). The empirical analysis and coping strategies on cyber-fraud --- a case study on Anhui Province. *Academics in China* 139(6): 198-204.

Wang, J (2020). Investigating on the effect of judicial control over telecom network fraud. *China Justice Magazine* 12(1): 160-176.

Wang, F., & Topalli, V. (2022). Understanding Romance scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context. *American Journal of Criminal Justice*, 1-37.

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

Ward, C. A. (1995). *Attitudes toward rape: Feminist and social psychological perspectives* (Vol. 8). Sage.

Ward, T., Hudson, S. M., Johnston, L., & Marshall, W. L. (1997). Cognitive distortions in sex offenders: An integrative review. *Clinical psychology review, 17*(5), 479-507.

Ward, T. (2000). Sexual offenders' cognitive distortions as implicit theories. *Aggression and violent behavior, 5*(5), 491-507.

Weinstein, E. A., and Deutschberger, P. (1963), ‘Some dimensions of altercasting’, *Sociometry*, 26: 454–466.

Weiss, K. G. (2009). “Boys will be boys” and other gendered accounts: An exploration of victims' excuses and justifications for unwanted sexual contact and coercion. *Violence Against Women, 15*(7), 810-834.

Weiss, K. G. (2011). Neutralizing sexual victimization: A typology of victims’ non-reporting accounts. *Theoretical criminology, 15*(4), 445-467.

Wentley, S. (2021). *Scamalytics Helps Online Dating Platforms Boost Security to Protect Singles from Fraud***.** DatingNews.com. https://www.datingnews.com/daters-pulse/scamalytics-helps-online-dating-platforms-boost-security/.

White, C. H., and Burgoon, J. K. (2001), ‘Adaptation and Communicative Design. Patterns of interaction in truthful and deceptive conversations’, *Human Communication Research*, 27/1: 9-37.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2015). A comparison of victim and offender perspectives of grooming and sexual abuse. *Deviant Behavior, 36*(7), 539-564.

Whitty, M. T., & Buchanan, T. (2012). The online romance scams: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181-183.
Whitty, M. T., & Buchanan, T. (2016). The online dating romance scams: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, *16*(2), 176-194.
Whitty, M. T. (2013a). Anatomy of the online dating romance scams. *Security Journal*, *28*(4), 443-455.
Whitty, M. T. (2013b). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scams. *British Journal of Criminology*, *53*(4), 665-684.
Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scams victims. *Cyberpsychology, behavior, and social networking*, *21*(2), 105-109.
Whitty, M. T. (2019). Who can spot an online romance scams? *Journal of Financial Crime*, *26*(2), 623-633. https://doi.org/10.1108/JFC-06-2018-0053.
Winters, G. M., Schaaf, S., Grydehøj, R. F., Allan, C., Lin, A., & Jeglic, E. L. (2022). The sexual grooming model of child sex trafficking. *Victims & Offenders*, *17*(1), 60-77.
Wise, J. (2022, December 4). How many people use dating app in 2022. *EarthWeb*. https://earthweb.com/how-many-people-use-dating-apps/.
Wu, L. P., Jian, Q, R. (2014). The Emergence, Continuation and Fracture of the Telecommunication Fraud by Rural Youth: A quantitative research based on six scammers from China's south-coastal area. *Youth Studies* 394(22): 22-30.
Wright, R. T., and Decker, S. H. (1997), *Armed robbers in action: Stickups and street culture*. UPNE.
Ye and Duan (2020). A case analysis and stimulation experimental research on *Sha Zhu Pan* scam. Journal of People's Public Security University of China (Social Science Edition). 5(5): 10-16.
Yuan, H.X., (2020). Qualitative and Punishment of the Criminal Case of "Killing Pigs" thoughts from different sentences in the same cases. *Beijing Social Science Review*. Doi: 10. 13262/j. bjsshkxy. bjshkx. 210208.
Zhang, L. J & Wu, X. L (2020). Research on the Governance of Cyber-Fraud. *Jiangxi Communication Science and Technology* 1: 42-45. DOI: 10.16714/j.cnki.36-1115/tn.2020.01.014

Vita

Fangzhou Wang was born in 1995 in Wuhan, China. She completed her Bachelor of Arts degree in Criminal Justice at Temple University in 2018. Immediately after, Fang obtained her Master of Science degree in Criminology at University of Pennsylvania in 2019. Her thesis was entitled "Public Housing and Crime", mentored by Dr. Gregory Ridgeway. She then pursued her Ph.D. in Criminal Justice and Criminology at Georgia State University, graduating in the Spring of 2023.

As a criminologist, Fang's main research interest aims to investigate the decision-making among offenders committing mainly cyber-enabled crimes. In addition, her research also relies on analyzing the relationship between victims and their offenders to determine offenders' motives. In general, her research is interdisciplinary. Recognizing the vital role of human and technical components of cybercrime, Fang employs both advanced computer science techniques and scientific analytical methodologies (quantitative and qualitative) to gather cybercrime intelligence and build profiles of active cyber-offenders and vulnerable victims. Her research aims to understand the modus operandi of online criminals and the social & behavioral interactions between victims and offenders as critical to establishing risk and protective factors of victims, which further inform preemptive prevention efforts.

Fang's research is often published in interdisciplinary outlets, including *Social Science Computer Review* (IF=4.578), *Victims & Offenders* (IF=2.045), and *International Journal of Cyber Criminology* (IF=1.208*), American Journal of Criminal Justice* (IF=6.037*), Deviant Behavior* (IF=1.716*),* and *Crime & Delinquency* (IF=2.307*).* Recently, she has submitted two manuscripts at *Criminology & Public Policy* and *Criminology*. In the sametime, Fang is also working with her collaborators to submit another first-authored manuscript to a communicational

journal. Her publication history illustrates my ability to expand the scope of criminological theory, aid in the development of the cyber-criminological literature, employ unique data collection strategies, and utilize advanced statistical models to answer timely research questions. Fang's familiarity with the technical components of cybercrime allows her to embed deeply within the illicit online ecosystem to monitor the behavior of active cyber-offenders and conduct field experiments aimed at disrupting their criminal operations. Findings from these field experiments provide law enforcement the knowledge required to investigate, mitigate, and prevent the occurrences of online crimes. Moreover, Fang's diverse background enables her to collect first-hand dataset from another country and analyze it using advanced methodology. As such, her current established research and future works can be informative in expanding the scope of cybersecurity and inform scholars in the United States on the issue of cybercrime in other countries.

Fang was the recipient of the Next Gen Fellowship at Georgia State University from 2019. She was also awarded with the Excellence in Doctoral Research Award in March 2022. In the following month, Fang received Provost's Dissertation Fellowship at Georgia State University for the duration of her dissertation.

Email: fzstacey712@gmail.com/fwang9@gsu.edu