8-15-2020

How Do Individuals Justify and Rationalize their Criminal Behaviors in Online Romance Fraud?

Martin Offei

Francis K. Andoh-Baidoo
The University of Texas Rio Grande Valley

Emmanuel Wusuhon Yanibo Ayaburi
The University of Texas Rio Grande Valley

David Asamoah

Recommended Citation

Offei, M., Andoh-Baidoo, F.K., Ayaburi, E.W. et al. How Do Individuals Justify and Rationalize their Criminal Behaviors in Online Romance Fraud?. Inf Syst Front (2020). https://doi.org/10.1007/s10796-020-10051-2

How do scammers justify and rationalize their criminal behaviors in online romance fraud?

Martin Offei, Francis Kofi Andoh-Baidoo[2], Emmanuel W. Ayaburi[2], David Asamoah[3*]

Department of Computer Science, Koforidua Technical University, Koforidua, Ghana
[2]Department of Information Systems, The University of Texas Rio Grande Valley, Edinburg, TX, USA
[3]Department of Supply Chain and Information Systems, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

[*]Correspondence:
David Asamoah, Ph.D.
Kwame Nkrumah University of Science and Technology
School of Business
Department of Supply Chain and Information Systems
Kumasi, Ghana
e-mail: dasamoah.ksb@knust.edu.gh

Abstract Online romance fraud (ORF) is a growing concern with such serious negative consequences as financial loss or suicide to the victim. Majority of empirical studies on online romance fraud using attachment, deception, protection motivation and relation theories focus on the victim. While neutralization offers insights into how individuals justify their deviant behaviors, the results have not been consistent in different contexts. In the ORF context, offenders may not only rely on justifying techniques but also rationalize their actions by denying risk both to the victim and the offender. Thus, drawing from the neutralization and denial of risk theories, we develop a research model to explain how online romance offenders justify and rationalize their intended criminal activities. To confirm our theoretical model, we collected 320 responses from individuals at Internet Cafés alleged to be online romance fraud hotspots. Our results highlight the boundary conditions of neutralization techniques in the context of online romance fraud. The study shows that denial of risk, a rationalization mechanism, moderates the relationship between denial of victim, a justification technique, and intention to commit romance fraud. This insight advances the frontiers of neutralization theory. We offer both theoretical and managerial implications of the findings.

Keywords: Online romance fraud, offenders, neutralization theory, denial of risk theory, scammers, internet fraud

How do Individuals justify and rationalize their criminal behaviors in online romance fraud?

1. Introduction

Rigorous academic studies of online romance fraud (ORF), especially those involving empirical evidence, are still evolving. Widely accepted theories or theoretical frameworks in the literature such as attachment theory, deception, protection motivation theory and relational theory have been used to investigate the online romance fraud phenomenon (Buchanan and Whitty 2014; Ho et al. 2017; Luu et al. 2017; Mosley et al. 2020). Much of the studies focus on the victims and their vulnerabilities. However, understanding why offenders commit such illegal acts without regard to the harm to the victims is evolving and unclear. Online romance fraud offenders use online dating and social networking sites to deceive and defraud their victims in a target nation, mostly Western countries. The offenders take advantage of the victims' genuine quest for romantic relationship to deceive their victims through false pretense, impersonation, counterfeiting, forgery and other fraudulent representation of facts (Ibrahim 2016). Online fraud has received attention from criminology, information systems and other disciplines (Buchanan and Whitty 2014; Moore et al. 2009; Williams et al. 2017; Wong et al. 2012). One of the unique features of online romance fraud is that the victim is more driven by the quest for romantic relationship and not the financial reward (Buchanan and Whitty 2014). The romantic relationship distinguishes romance scam or romance fraud from any other fraud and for that matter, any other cybercrimes, and therefore demands special attention (Cross 2018). Illegal activities of deceit or extortion of individuals on the dating sites is aided by the ability of the perpetrators to justify their actions due to the way dating sites operate. A troubling aspect of the online romance fraud is that, most of the offenders reside in jurisdictions outside that of the victims. Most perpetrators are usually technically savvy and about college aged.

In this study, we investigate how individuals employ neutralization techniques to justify online romance fraud prior to committing the crime (Sykes and Matza 1957). Neutralization theory, from criminology, has been employed to explain deviant behaviors in societies and organizations. In proposing the neutralization theory, Sykes and Matza (1957) suggest that, deviants do not generally oppose the law-abiding society but find ways to convince the society that their deviant behavior results from treatment and harm that they have suffered from their environment. They put across a

sorry and apologetic disposition to gain sympathy and shield themselves from blame from the society. Sykes and Matza (1957) refer to these actions as neutralization techniques which are learned by deviants and used as the basis for legitimizing their crimes or victims. A neutralization technique is a temporary insulator that a criminal or an offender uses to absolve themselves from self-blame and from the blame of society in general (Sykes and Matza 1957).

Neutralization techniques as justifications are critical in lessening the effectiveness of social controls. Characteristics of the perpetrators where neutralization may explain delinquent behavior include: 1) feeling of shame or guilt 2) identification of appropriate and inappropriate target 3) avoiding harm to any individual within their community and 4) accepting at least partially dominant social order (Sykes and Matza 1957). It behooves academia and the society in general to understand why an abled college age individual who might otherwise aspire to productive socially acceptable careers engage in such delinquent behavior as ORF. Our first research question: *(i) how does neutralization influence the intention to commit online romance fraud?*

This study acknowledges that neutralization techniques alone may not be enough to explain intention to commit crime, since other factors may be at play (Siponen et al. 2012). While neutralization is the basis for forming justifications prior to committing a crime, rationalization can be deployed to masquerade the main motivation after committing the crime. Rationalization is aimed at making a case for why the actions make sense. In the context of online romance, victim and offender establish a relationship in which the offender commits time, effort and in some cases monetary gifts into maintaining the relationship. The victim equally invests same if not more. However, the offenders know ahead of committing the crime that online romance fraud is not only illegal but also has heavy negative consequences. Thus, offenders may rationalize their actions by denying the existence of risk through their confidence in evading law enforcement or that their specific crime is not as bad or harmful as other crimes. Therefore, we postulate that denial of risk perception may interact with the effect of neutralization on intention to commit crime. To address the need to understand the motivation of online romance offender, we focus on the effect of denial of risk and address our second research question: *(2) how does denial of risk perception interact with the effect of neutralization on the intention to commit online romance fraud?*

Drawing from the neutralization theory (Sykes and Matza 1957) and denial of risk theory (Peretti-Watel 2003), we develop a research model that explains how online romance scammers justify and rationalize their criminal activities. To empirically test our model, we collected 320 responses from individuals at Internet Cafés alleged to be online

romance fraud hotspots. The study results contribute to the cyber fraud literature by complementing the existing criminology theories used to understand deviant behaviors. While prior research has identified the positive effect of denial of responsibility, denial of injury and denial of victim, subset of the neutralization techniques, on intention to commit crime, this study finds that their positive effects vary depending on the offender level of denial of risk perception. Thus, this study contributes to building theory about ORF phenomenon and providing boundaries to the neutralization theory. For practical implication, our results show that it may be useful for administrators of online platforms to provide their members at the point of joining the platform information that contain such pointers as levels of over-confidence levels or empathy about of their potential partners. Such pointers illustrate the tendencies to justify or rationalize delinquent intentions . The rest of the paper is organized as follows. We present theoretical development and research model highlighting some of the prior relevant studies in the next section. We then discuss our research method in section 3, followed by section 4, which covers our results, findings, and implications.

2. Background literature and model development

In this section, we provide definition of online romance fraud and then present theoretical model and related hypotheses.

2.1. Online romance fraud

In the traditional relationship setting, romance fraud has been defined as "instances where a person is defrauded by an offender through what the victim perceives to be a genuine relationship" (Cross 2018 p.1). Romance fraud has also been referred to as "sweetheart swindles", dating and relationship fraud (Moss et al. 2018). Online fraud is defined as "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 that has led to a financial or nonfinancial loss or impact of some kind" (Cross 2018, p.1). Advancements in information and communication technologies have enabled offenders to deploy novel schemes to commit ORF, also referred to as "catfish" (Rege 2009); Cross 2018; Mosley et al. 2020). The number of victims and amount of financial losses involved with online romance fraud that were reported by several countries in 2016 depict a devastating global problem. In the United States, about 15,000 victims reported combine losses in excess of $230 million to the Federal Bureau of Investigations (FBI) Internet Crime Complaint Center (IC3) (Brenhoff 2017). The Canadian Anti-Fraud Center reported losses of about $21 million to 831 victims (CBC News 2017). The Australian Competition and Consumer Commission reported losses of over $25.5 million to 1,017 victims. The Action Fraud in the United Kingdom reported losses of about € 39 million to 3,899 victims. A CNN story

referenced the Federal Trade Commission report which suggests that online romance fraud resulted in more losses than any form of online fraud that was reported (Karimi 2019). A syndicate involving offenders from multiple countries was recently apprehended by the FBI for allegedly using the internet and other technological tools to scam their victims and launder their bounty by moving them through multiple bank accounts using several fake identities (U.S. Department of Justice 2019).

Table 1 presents summaries of some prior theory-based online romance fraud research (Aransiola and Asindemade 2011; Buchanan and Whitty 2014; Rege 2009). Most of these empirical studies focus on the victim using theories such as attachment, deception, protection motivation and relation. Drawing from the description of online romance fraud, definitions of both romance and online frauds in prior literature, we define online romance fraud as instances where a person is defrauded or scammed by an offender through an internet-enabled medium such as an online dating site or a social networking site in what the victim perceives to be a genuine relationship. Generally, in online romance fraud, the scammer masquerades as initiating a genuine relationship on an online dating or social networking sites. Using stolen pictures and other false information, the offender creates a profile and then professes their love to a target victim. When the victim responds, the offender quickly demands that the relationship is moved from the dating or social networking site to a more personal form of communication such as email, chat, messenger, text messages, phone calls, and webcams. Following the establishment of perceived trust, the scammer demands money from the victim and this demand increases in size over time. Victims are made to believe that there are some mutual benefits for both parties. This situation continues until the victims realize that they have been scammed. While some victims may believe such a lie, most focus on the romantic relationship ignoring financial benefits. We focus on the theoretical explanation of the offender actions in this study.

Table 1: Summary of relevant prior theory-based research on Online Romance Fraud

Objective	**Context**	**Theory**	**Independent variable**	**Outcome**	**Reference**
Understand perpetrators of online dating deception	Online dating site	Attachment theory Relational theory	attachment anxiety, avoidance and gender	attachment avoidance and males are less likely to be catfished	(Mosley et al. 2020)

cognitive factors that influence a user's ability to detect or deceive based on gender	Computer mediated game	Deception	Gender self-efficacy, motivation	Whilst males have higher belief in their ability to hide their gender, females have higher perception of detecting gender deception	(Ho et al. 2017)
Do victims self-blame for getting scammed?	Case study of online dating site	None	None	Repeated victims claim some degree of responsibility for not pursuing well-informed love	(Sorell and Whitty 2019)
To understand the adoption of protective motivation behavior as risk mitigation against romance fraud.	online dating sites	Protection Motivation Theory	Response efficacy, self-efficacy, response cost, coping appraisal, threat awareness, perceived severity, perceived vulnerability, threat appraisal	Key dimensions of PMT support intention to use protective technologies except response cost and threat awareness against ORF.	(Luu et al. 2017)
What psychological factors make one vulnerable to romance scam victimization?	European online dating site	Five factor personality model (FMM)	Loneliness, romantic beliefs, sensation seeking, FMM	Romantic and idealization beliefs are more likely to make one a victim	(Buchanan and Whitty 2014)
Psychological impact of online dating romance scam on victims	Case study of online dating site	None	None	Victims experience emotional abuse that leaves them depressed, shamed, worthless or cyber gang raped.	(Whitty and Buchanan 2016)

2.2 Neutralization Theory

The neutralization theory presents techniques that people employ to justify crimes. The theory was first introduced by criminologists to explain how juveniles neutralize values within themselves when they commit delinquent acts (Sykes and Matza 1957). The theory's philosophical underpinning gave a new direction and perspective to explaining other crimes and deviant acts. In the information system discipline, the theory has been used to explain illegal acts and deviant acts such as software piracy (Siponen et al. 2012), cyberbullying (Zhang and Leidner 2018), and security policy compliance (Vance et al. 2019). Most of the studies have examined a subset of the neutralization techniques namely denial of injury, denial of responsibility, denial of victim, condemning of the condemners, metaphor of the ledger, appeal to higher loyalties, and defense of necessity, when all the techniques may not be applicable. While denial of the victim and metaphor of the ledger have been found to influence computer abuse intention (Willison et al. 2018), only

defense of necessity influences intention to violate security policy (Barlow et al. 2013). The use of subsets has been employed in several contexts (e.g., Cao 2004; Zhang and Leidner 2018). In fact, rape offenders employed denial of injury, denial of victim and denial responsibility subset of neutralization techniques to justify their actions (Williams 1986). In the online romance fraud context, victim build perceived personal bond through the supposed romantic relationships with the offender. Therefore, the offender's denial of injury, denial of responsibility and denial of victim can shock and devastate the victim. Some of the devastating consequences suffered by victims of online romance fraud include homelessness, unemployment, financial loss, deterioration in health and well-being, and suicide. Meanwhile, in order to gain sympathy and shield themselves from blame from the society, the offender must convince themselves and others that there is no harm and if even there were, they cannot be held responsible. In some instances, such thoughts provides basis for the offender to legitimize their victims (Williams 1986). Therefore based on the preceding and like (Zhang and Leidner 2018), in the study of online romance fraud , we use denial of responsibility, denial of injury and denial of victim subset.

Second, we seek to examine how denial of risk moderates the relationship between the denial techniques in neutralization and intention to commit online romance fraud. The offender can employ denial of risk to rationalize that the specific crime, in this case, online romance fraud, is safer with less serious consequence than other crimes such as murder. In addition, offenders believe they have the skills and knowledge to successfully defraud their victims (Willison et al. 2018). We argue that higher level of denial of risk exacerbates the effect of neutralization on intention to commit an illegal or deviant act. Thus, the denial of risk rationalization should be focused on the neutralization techniques where the offender seeks to deny. Thus, denial of risks can serve as a boundary condition for neutralization, in particular, in the context of online romance fraud. The failure to identify boundary conditions when using neutralization techniques could explain why there is inconsistencies in neutralization studies (Barlow et al. 2013; Willison et al. 2018). Next, we discuss and hypothesize how the three neutralization techniques influence the justification of illegal acts in the context of online dating.

Table 2: Summary of sample prior research based on Neutralization Theory

Objective	**Context**	**Techniques**	**Dependent variable**	**Outcome**	**Reference**
How neutralization moderates	financial organization	denial of injury, denial of the victim,	computer abuse	Only denial of the victim and metaphor of the ledger	(Willison et al. 2018)

deterrence theory, organizational justice and computer abuse intention		metaphor of the ledger, distributive injustice, procedural injustice, sanction severity, sanction certainty		influence the effect of procedural injustice	
Employs Neutralization theory to examine employees' security policy compliance	administrative personnel of various large organizations	denial of injury, denial of responsibility, metaphor of the ledger, condemnation of the condemners, appeal to higher loyalties, defense of necessity, Formal sanction, Informal sanction, Shame	Security policy compliance	Only neutralization influence intention to violate security policy	(Siponen and Vance 2010)
Understand if communication focused on mitigating neutralization rather than deterrence will influence policy compliance	full-time employees of an organization	denial of injury, defense of necessity, metaphor of the ledger	intentions to violate IT security policies	Only defense of necessity influences intention to violate security policy	(Barlow et al. 2013)
Understand usage of workplace network for personal purposes	Large organizations	Neutralization techniques Deterrence techniques	Intention to use workplace network	Neutralization techniques, sanction severity and benefits influence the intention to use workplace network for personal purposes	(Cheng et al. 2014)
How to alter individuals' neutralization technique tendencies	Large organizations	Denial-of-responsibility, denial-of-injury defense-of-necessity, condemnation-of-the-condemners, appeal-to-higher-loyalties, entitlement, relative acceptability, defense-by-comparison	Compliance with password policy	Training programs inspired by cognitive dissonance theory encourage less use of the neutralization techniques considered in the study	(Siponen et al. 2020)

What influence shadow IT usage in organizations?	Large organizations in Europe	Neutralization techniques Deterrence techniques	Intention to use shadow IT	Only metaphor of the ledger influence intention to use shadow IT	(Silic et al. 2017)
How employees justify workplace cyberbullying	Large organizations	Denial of responsibility, denial of victim, denial of injury, anonymity, visibility, asynchrony	Intention to cyberbullying	Social presence features mitigate the effect of denial of responsibility, denial of victim and denial of injury on cyberbullying intention	(Zhang and Leidner 2018)
To understand the motivation for setting up websites that illegally offer denial-of-service attacks for a fee.	Dark web	Association Neutralization techniques Rational choice	Operating an illegal service	Appeal to higher loyalties is mostly used because offenders believe they are providing services that were for the common good. Additionally, some participants denied responsibility claiming the end user is to be blamed.	(Hutchings and Clayton 2016)
Understanding race and rape.	society	Neutralization techniques	Legitimization of rape victim	Perpetrator use denial of responsibility, denial of victim and denial of injury to legitimize rape against black victims.	(Williams 1986)
Which neutralization techniques influence software piracy?	College Students	Denial of injury denial of the victim denial of the responsibility metaphor of the ledger condemnation of the condemners appeal to higher loyalties defense of necessity Formal sanction Moral beliefs Shame	Intention to pirate software	Only metaphor of the ledger, condemnation of the condemners, shame and moral beliefs were important predictors of software privacy	(Siponen et al. 2010)

Factors that influence students' intention to pirate music	College students	Five techniques: denial-of-responsibility, denial-of-injury, denial of victim, condemnation-of-the-condemners, appeal-to-higher-loyalties	Intention to pirate music	Denial of responsibility, denial of injury, denial of victim, and appeals to higher loyalty are moderately associated with music piracy	(Ingram and Hinduja 2008)

Neutralization theory has been employed to study criminal and deviant behaviors in diverse contexts, but the results have not been consistent. Neutralization techniques act as antecedents to intention to commit IS security violation in the workplace (Siponen and Vance 2010). In the context of IS security policy compliance, employees justify their violation of the IS security despite their awareness of the consequences associated with these violations. Neutralization techniques have also been found to be strong predictors of other deviant behaviors in different contexts including the military (Pershing 2003), and abuse of illicit drugs (Priest and McGrath III 1970). However, neutralization was found to be a weak determinant of online software piracy (Hinduja 2007). The inconsistencies of findings from prior research regarding neutralization theory calls for more studies to investigate the effect of context on the boundary condition of the theory. Although, neutralization may be enough to understand crime, the theory is developed and applied as discussed in the preceding section in the context where the victim and offender may have little prior relationship, emotional bond and/or mutual trust. In most of the contexts of prior neutralization studies, the offender employs neutralization techniques to justify their intention to commit crime.

Most of the studies on online romance fraud are centered on organizational context. However, the perpetrators of online romance fraud operate at the individual level in which no organizational governance mechanism are applicable. This study is closer to studies on software and music piracy that have no governance mechanism to mitigate all techniques. Thus, like Ingram & Hinduja (2008), this study explores a subset of the neutralization techniques that are relevant to understand how perpetrators justify their decision to engage in online romance fraud. We also investigate how denial of risk moderates the relationship between neutralization and intention to commit online romance fraud.

2.3 Model development

Figure 1 presents our research model which is based on two theories, neutralization and denial of risk theories. We draw on these theories to answer our research questions. In the following, we describe the two theories and discuss how they inform our inquiry, the research model and associated hypotheses.

Following prior studies (e.g., Ingram & Hinduja, 2008) that have examined Neutralization in non-organizational context, this study focuses on the first set of techniques proposed by Sykes and Matza (1957). The five initial techniques are denial-of-responsibility, denial-of-injury, denial of victim, condemnation-of-the-condemners, and appeal-to-higher-loyalties. However, Condemnation-of-the-condemners dimension of the original five techniques is not considered in this study. In condemnation-of-the-condemners, it is assumed that the perpetrator would shift the focus from their deviant inclinations to the deviant tendencies and unethical propensities of the potential victims. If they were to use this technique, they will point out how their victims made themselves vulnerable and worthy of harm they suffer. Scammers also known as "sakawa" or Yahoo boys" in some jurisdiction go to dating site falsely representing themselves as a potential romantic partner (Mosley et al. 2020). Perpetrators are on the offensive and are willing to harm even the most vigilant user on the platform. However, the victim comes to the platform in search of true love. Their decision to engage in romantic association is usually based on the convincing messages by their perpetrators. Searching for true love off or online should not be a crime as others have found true love on dating sites. Thus, the perpetrator cannot justify condemning their victims for being scammed in their pursuit of true love.

The other technique of neutralization that is not examined in this study is appeal to higher loyalties. If perpetrators of fraud on dating platforms were to deploy this technique, such perpetrator would claim their actions are championing and supporting a good cause or entity outside of and above oneself. Offenders would believe that their actions do not cause the victim to suffer any emotional and financial pain. Perpetrators sign up to dating platforms with preconceived schemes to siphon as much money as possible from their victims. Thus, there is no adherence to or support of a higher purpose by scam perpetrator on dating sites. Next, we discuss the three neutralization techniques employed in this study and follow with the hypotheses.

Denial of responsibility: The concept of denial of responsibility is the situation where offenders justify their action by claiming that they are victims of the environment (Evans and Porche 2005; Zhang and Leidner 2018). Such as in traditional romantic settings, a partner may claim that they are unable to attain a certain status because of their

background, the love relationship or their environment (Boateng et al. 2011). Thus, a perpetrator can believe that they can convince themselves and others that they are blameless for their deviant acts. They may use these reasons to minimize their unrestrained desire to exploit their partners. The perpetrator's background characteristics may explain their drive to online romance platform. Through learning, perpetrators exploit their experience or familiarity to present stories that depict them in a dire situation requiring immediate actions by their victims. Unfortunately, due to romantic beliefs, the victims fall prey to these tricks.

In the context of online dating, the lack of face-to-face interactions and sensory cues such as sound and visual appearance affords the offenders opportunity to misrepresent their identities making it difficult for the victim and the platform operators to authenticate users prior to establishing any personal bonds (Rege 2009). Romantic beliefs result in cognitive lock-in of the victim in investigating the partner who later becomes an offender and the situation is exacerbated in the online dating context where a victim does not have the benefit of non-verbal communication (Buchanan and Whitty 2014). However, the offender comes to the online dating platform preconditioned to defraud. The offenders are likely to feel no guilt for the lack of effort or ability by the victim to determine genuineness of a partner. While the goal of the victim in the online dating is a romantic relationship, that of the offender is financial gain. The offenders in some situations invest a lot of working hours into satisfying their victims emotionally to the point where they are unable to focus on other avenues of making income. Thus, offenders do convince themselves and others that they deserve gains from the relationship that should not be perceived as exploitation since they had a romantic involvement with the victims. Hence, we expect that:

H1a: Denial of responsibility as a neutralization technique is positively related to intention to commit online romance fraud.

Denial of injury: The denial of injury technique is used by offenders/criminals to defend their activities as it is not harmful to the victims. The offenders justify the acts by minimizing the resultant effect on the victim (Sykes and Matza 1957). Neutralization techniques are used when identification of appropriate and inappropriate target is possible. In online dating sites, the offenders use profiling to target their victims. The perpetrators have in mind a profile of potential victims. Through the platform and associated communications, perpetrators can confirm that they are targeting the right victims. Furthermore, the victims might provide more indicators that they are able to part away with some money and the perpetrators exploit such indicators by requesting for small amount of money and with the amount increasing with

time. For instance, offenders target older individuals for romance fraud because they believe they are wealthy and have high disposable income and savings (Cross 2015). The offenders believe that, their actions are tools for wealth redistribution which is a key tenet of neutralization.

In addition, online romance fraud reporting is low (Cross 2018), and victims generally do not receive enough support from authorities and in some instances are blamed for their losses (Cross 2015). The shift in blame will not only discourage victims from reporting to legal authority but also, reduce the likelihood of discussing their situation with their families and friends. The low reporting of online romance fraud may result from victims' belief that they can gain financially from the relationship (Whitty 2013). In some cases, the offender asks the victim to pre-finance a fictitious transaction promising that it will bring both the offender and the victim great financial benefit. The offenders claim that the environment allows them to achieve their personal gain and may argue that the victim has equal opportunity to such financial benefits and or to withdraw from the relationship to avoid such loss. The potential for financial reward for both parties insulate the perpetrators from feeling they have caused any harm and demotivates the victims from reporting. Taken together, we postulate that:

H1b: Denial of Injury as a neutralization technique is positively related to intention to commit online romance fraud.

Denial of victim: In denial of victim, the offenders think their actions do not affect the victims. This is because victims are not physically present in jurisdiction of the perpetrators. Perpetrators have diminished awareness of the victims. Thus, the victims are an abstraction to the perpetrators minimizing any emotional connection. The lack of emotion makes the perpetrators view the victim as an object who suffers no harm. The perpetrators believe that any financial gain is a form of payment for time spent and other romantic acts the victim has benefited from their relationship. Furthermore, after establishing perceived trusted relationship, the offenders initiate their intended crime by requesting financial assistance to resolve a problem that will bring financial reward to both the offenders and victims and absolve themselves of guilt (Cross 2015). We hypothesize that:

H1c: Denial of victim as a neutralization technique is positively related to intention to commit online romance fraud.

2.2.1. Denial of risk theory

While most studies find neutralization to have a strong significant relationship with deviant behaviors, others have found that relationship to be weak (Costello 2000). Neutralization techniques alone may not be enough because - a) other psychological factors may be present (Sykes and Myers) and b) not every perpetrator will justify their actions but will give reason for why their actions make sense. The reasons provided are not the main motivation for committing the crime but after thought to rationalize their actions. The contradictions in the findings using neutralization could be attributed to situation specific factors. Therefore, the online dating platform may present intervening factors that influence neutralizations techniques. For instance, online dating situation fosters the growth of trusted relationship in which the victims may disproportionally exhibit emotional involvement. Offenders invest time and effort into the development of the romantic relationship. Therefore, offenders will consider their investment in rationalizing any outcome to their victims.

Denial of risk involves criminals rationalizing their behaviors by developing adaptations to risky behaviors (Peretti-Watel 2003). The components of denial of risks are scapegoating, self-confidence, and comparison between risks. These adaptations allow the offenders to reject the presence or effect of risk (Apostolidis et al. 2006). The denial of risk theory has been employed to study cannabis use among French adolescents and it was found to be a good predictor of cannabis use which was regarded as an illegal act at the time (Peretti-Watel 2003). This theory has sparingly been used in the information systems field. In this research, we argue we can enhance our understanding of online romance fraud by examining the interactive effect of denial of risk on the relationship between neutralization and intention to commit online romance fraud. Challenges with the criminal justice systems, the international dimension of the crime, and anonymity of offenders converge to influence risk perception and worsen the online romance fraud dilemma (Hadzhidimova and Payne 2019).

The self-confidence of individuals who engage in online romance fraud is reckoned to be relatively higher which gives them the zeal to propagate online romance fraud. The use of self-confidence to deny the presence of any risk, is used as a technique to hunt their victims and subsequently defraud them. Offenders trust in their ability to remain anonymous in using technology features to build stronger bonds with their victims. For instance, individuals that have been victimized in online dating sites go ahead to continue in the relationship because they trust in the strong relationship that they have developed with the offenders. The offenders compare risks among crimes and believe that online romance is not as risky as other crimes such as murder or corruption. In the context of online romance fraud, we expect

that: The offenders expect to depersonalized others (Harrington 1996), in this case the platform operators, and/or the victims to authenticate the veracity of information provided. Thus, the offenders shift blame for any successful fraud to the platform or the victims.

H2: Denial of risk is positively related to the intention to commit internet romance fraud.

2.2.2 Moderating Role of Denial of Risk

Offenders that perceive a high denial of risk do so through self-confidence in performing a crime and that they can evade law enforcements. When offenders justify their illegal acts by denying any responsibility, injury on their victims, they are more likely to be committed to pursue rigorous and seek innovative ways to commit online romance fraud when they believe there is no risk to their actions. Offenders who use comparison of risk, believe that defrauding clients is not as bad as other crimes and will not feel guilty inflicting injury on their victims. Furthermore, offenders who believe that they know how to convince their victims than the average person will not feel accountable to any loss by the victims. The offenders have confidence in determining victims who are less willing to be defrauded and so denial their victims. Thus, the higher the denial of risk perceived by the offenders, the higher the effect of neutralization on the intention to commit online romance fraud. We argue that:

H3a-c: The positive relationship between neutralization techniques and intention to commit internet romance fraud will be stronger if the individual perceive higher denial of risk.

Following prior research on neutralization (Siponen and Vance 2010; Zhang and Leidner 2018), in this research, we control for individual's gender, experience, age of offender, level of education, level of IT skills or competency. The research model and hypotheses are presented in Figure 1.

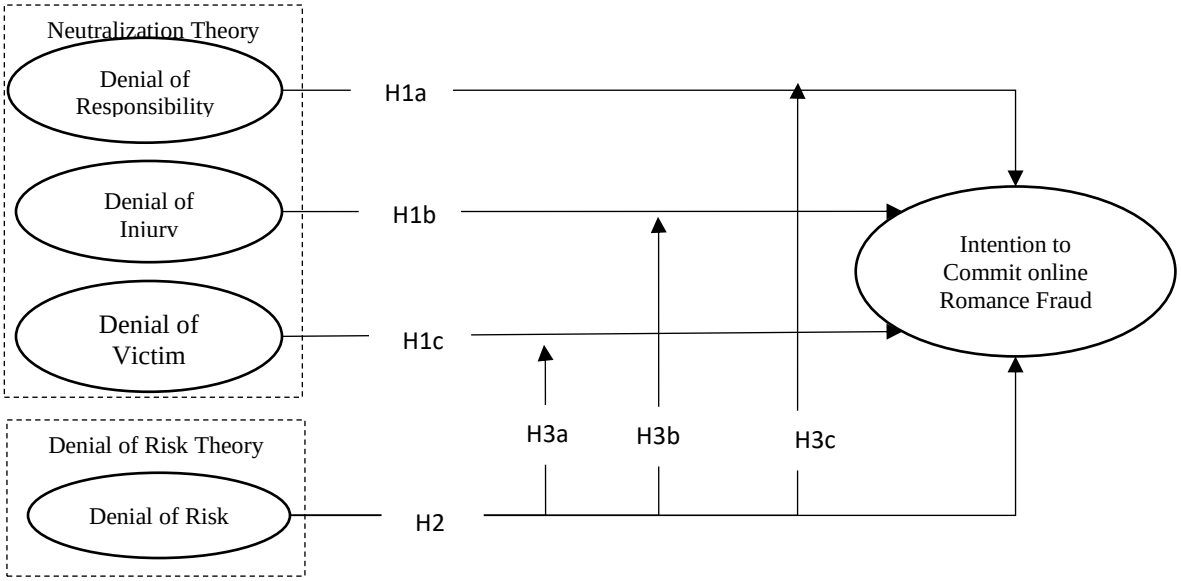

Figure 1. Conceptual model

3. Methodology

3.1 Study context

The target population of this study comprises of individuals with knowledge about online romance fraud. Preliminary observation of those involve in romance fraud are 18 years or older and are called "gamers" or "sakawa" in the study context. The offenders, "gamers", usually refer to their victims as "clients". This indicates that the offenders see their relationship with their victims as transactional in nature. Due to the secretive nature of the romance fraud activities and potential social desirability, snowball sampling technique was used to identify hotspots for internet romance fraud. These hotspots are internet services providers' location where offenders are alleged to carry out their activities on public network and reduce any trace. It is also at these hotspots that new offenders are recruited and trained. Table 1 provides descriptive information on our final study sample.

3.2 Instrumentation

All the items of the construct in the study were measured on a 5-point Likert-type scale. The items for the neutralization techniques were adopted from (Siponen and Vance 2010; Zhang and Leidner 2018) and adapted to the online romance fraud context. The three dimensions of Neutralization; denial of responsibility, denial of injury, and denial of victim, were modelled as first order reflective constructs with each construct measuring a different aspect of the unobservable

neutralization construct relevant in this context. Items measuring denial of risk were adapted from (Peretti-Watel 2003). To ensure content validity, two IS faculty with research expertise in security and privacy and six individuals (obtained through the first author's contact) with first-hand knowledge of online romance fraud evaluated the face validity of each item. Revisions were made according to their recommendations. To assess construct validity, we conducted a pilot test of our measuring instrument with a 70 sample. We revised our measuring instrument and our final survey instrument is presented as Appendix I.

3.3 Data

Our focal sample includes data from respondents from different identified hot spots for internet fraud (also called cyber cafes or yahoo yahoo). We do not have an estimate of the total number of individuals who might be engaged in online romance fraud. Conveniently, three hundred and fifty (350) questionnaires were distributed to individuals located at hotbed internet fraud areas within the selected regions of the study area. A total of three hundred and twenty (320) completed responses were retrieved. Majority (85.6%) of the respondents were between the ages of 20-30 years. Most (82.2%) of our respondents have at least secondary education.

Table 3. Demographics of the respondents

Control variables	Frequency	Percent	Valid Percent	Cumulative Percentage
Age				
<20 years	127	39.7	39.7	39.7
21-30 years	147	45.9	45.9	85.6
31-40 years	43	13.4	13.4	99.1
41-50 years	3	0.9	0.9	100
Gender				
Male	237	74.1	74.1	74.1
Female	83	25.9	25.9	100
Educational Level				
Basic	57	17.8	17.8	17.8
Secondary	189	59.1	59.1	76.9
Tertiary	74	23.1	23.1	100
Access to internet device				
Yes	311	97.2	97.2	97.2
No	9	2.8	2.8	100
Level of computer competence or skills				
Extremely Competent	71	22.2	22.2	22.2
Very Competent	124	38.8	38.8	60.9

Competent	111	34.7	34.7	95.6
Rarely Competent	14	4.4	4.4	100
ORF Experience				
Yes	316	98.8	98.8	98.8
No	4	1.3	1.3	100
Rate of level of experience (skills)				
Extremely Experience	124	38.8	38.8	38.8
Very Experience	110	34.4	34.4	73.1
Experience	81	25.3	25.3	98.4
Rarely Experience	2	0.6	0.6	99.1
Not Experience	3	0.9	0.9	100

3.4 Analysis and results

Neutralization theory has been used to understand several security issues in the information systems context. However, denial of risk theory has been sparsely used to study security problems. This study developed a theoretical model based on the two theories to explain individuals' intention to commit online romance fraud. Thus, the goal of this study is the confirmation of the integrated theory and less of the explanatory power of the model. Thus, our study was assessed using the covariance-based structural equation modeling (SEM) because we are attempting to confirm a theoretical model, and are less concerned with predictive accuracy of each of the constructs (Reinartz et al. 2009). A two-step process: measurement model assessment and structural model testing was followed using Mplus 8.0 software (Muthén and Muthén 2005).

3.4.1. Measurement Model Validation

The measurement model was first analyzed to ensure psychometric properties of validity, reliability, and common method bias using co-variance-based SEM with Mplus software. Confirmatory factor analysis (CFA) was used to assess construct validity by examining convergent and discriminant validity. The results of the CFA analysis show that our measurement model exhibited sound psychometric properties (CFI=0.936, TLI=0.916, RMSEA= 0.059 and Chi/dff = 2.383).

The convergent validity of variables can also be assessed by ensuring the reliability of the researched constructs, construct reliability, average variance extracted (AVE) and performing factor analysis (Fornell and Larcker 1981). After removing the items with poor loadings, each of the items loaded well on their own constructs and cross loadings were noted to be insignificant between the constructs. As shown in Table 3, the composite reliability for denial of risk

(DOR) is 0.926, denial of injury (NDoI) is 0.857, denial of responsibility (NDoR) is 0.883, denial of victim (NDoV) is 0.819 and intention to commit online romance fraud (FRD) is 0.865; the average variance extracted (AVE) ranged from 0.609 to 0.791, and most of the item loadings were higher than 0.60 (Hair Jr et al. 1995). Table 4 shows the convergent validity assessment of the measurement model.

Table 4. Psychometric properties of measures

Theory	Construct	Items	Estimate	S.E.	Est./S.E.	CR	AVE
Denial of Risk Theory	Denial of Risk (DoR)	Dor1	0.695	0.060	11.495		
		Dor2	0.969	0.017	58.102		
		Dor3	0.522	0.066	7.898		
		Dor4	0.678	0.047	14.468		
		Dor5	0.998	0.012	86.057	0.926	0.679
		Dor5	0.522	0.065	8.075		
Neutralization Theory	Denial of Injury (NDoI)	Neutdoi1	0.922	0.044	20.10		
		Neutdoi2	0.655	0.051	12,933		
		Neutdoi3	0.628	0.053	11.764	0.857	0.670
	Denial of Responsibility (NDoR)	Neutdor2	0.802	0.084	9.500		
		Neutdor3	0.746	0.093	8.011	0.883	0.791
	Denial of Victim (NDoV)	Neutdov1	0.542	0.070	7.777		
		Neutdov2	0.738	0.078	9.427		
		Neutdov3	0.730	0.061	11.871	0.819	0.609
	Online Romance Fraud Intention (FRD)	Frd1	0.847	0.066	12.821		
		Frd2	0.826	0.053	15.635		
		Frdd3	0.517	0.064	8.022	0.865	0.684
	Goodness-of-Fit Measure	Recommended Threshold			Observed Value		
	Chi-square/degrees of freedom	≤3.0			217.93/104 =2.383		
	CFI: Comparative Fit Index	≥0.90			0.936		
	TLI: Tucker-Lewis Index	≥0.90			0.916		
	Root mean squared error of approximation (RMSEA)	<0.10			0.059		

Discriminant validity of each latent construct was tested by the method recommended by (Fornell and Larcker 1981). The square root of AVE of each construct (diagonal of Table 5) should be higher than the correlation between that construct and any other constructs. This criterion is satisfied by all latent constructs. Therefore, our measurement model exhibits sound reliability and validity necessary for further testing of the research hypotheses.

Table 5 Discriminant Validity

	DOR	FRD	NDoI	NDoR	
DOR	(0.824)				
FRD	0.197	(0.827)			
NDoI	0.0.079	0.163	(0.819)		
NDoR	0.015	0.157	0.333	(0.889)	
NDoV	-0.028	0.227	0.163	0.092	(0.780)

Note: Diagonal elements in brackets are the square root of the Average Variance Extracted (AVE). Off-diagonal elements are the correlations among latent constructs all with $p<0.01$

Common method bias occurs when the measuring instrument employed affects the scores or measures that are being gathered (Straub et al. 2004). Common method bias could threaten the validity and conclusion of a study. This study has taken steps to lessen the potential effects of common method bias. Two approaches for reducing common method bias in a research instrument have been proposed (Podsakoff et al. 2003). These two techniques centre on ensuring anonymity in the research instruments and improving measurement measures for the research constructs. In this study, anonymity was maintained in the research instrument by protecting the identity of the respondents from the general public. Respondents were asked to be honest and express themselves freely (Podsakoff et al. 2003). Secondly, the pilot test ensured that the measurement scale is validated, vague concepts removed, unknown and unclear terms eradicated, and duplicate questions removed (Podsakoff et al. 2003). When measuring some research constructs, the study relied on scales previously examined. A verified and well-tested scale helps to reduce the ambiguity of an item. Finally, counterbalancing the question order was also used to control for priming effect and other item-context induced mood states.

3.4.2 Structural model and hypotheses testing

The next step after establishment of the soundness of the psychometric properties of the measurement is the testing of the theoretical model (Hair et al. 2019). Estimates of the path coefficients and the values for the research model are shown in Table 6. The path coefficients depict the strength of the relationships between the constructs. Our base model indicated that the three dimensions of neutralization theory positively influence the intention to commit online romance fraud. Thus, we began the examination of our model by testing the effect of neutralization theory. The neutralization only model explained 7.3 % the variance in online romance fraud. This is similar to the effect of neutralization in other context such as security policy violation where neutralization explained about 9.3% of the variance (Vance et al. 2019).

Finally, when effect of denial of risk theory was added to the model, the variance explained increased by 3.8% to 11.1%. The structural model results revealed that not all pathways in the study model are statistically significant.

The relationship between neutralization and the intention to commit online fraud is significant for one of the three dimensions. Denial of responsibility (NDoR) was found not to have a significant positive relationship with intention to commit online romance fraud in the study context ($b = 0.136$, $t= 1.446$, $p>0.05$). Thus, H1a is not supported. Also, H1b is not supported ($b = 0.020$, $t=0.259$, $p > 0.05$) in that denial of injury (NDoI) as neutralization technique is not significantly related to the intention to commit online romance fraud (FRD) in this study context. H1c states that, denial of victim (NDoV) as neutralization technique is positively related to tendency of committing online romance fraud. This hypothesis was supported ($b = 0.211$, $t=2.988$, $p < 0.05$). Based on Denial of Risk theory, we hypothesized in H2 that denial of risk (DOR) is positively related to intention to commit romance fraud and we found support for our conjecture ($b = 0.199$, $t= 2.661$, $p<0.05$).

3.4.3 Exploring the moderating role of Denial of Risk

The study postulated that denial of risk will strengthen the effect of the three dimensions of neutralization on intention to commit online romance fraud. Therefore, three interaction terms which are the product of the two variables were created and added to the model. The analysis results show that, while DOR works as strong positive moderator between denial of victims (NDoV) as neutralization technique and intention to commit romance fraud ($b = 0.115$, $t=2.083$, $p < 0.05$), it does not influence the relationship between denial of responsibility (NDoR) as neutralization technique and intention to commit romance fraud ($b = -0.048$, $t=1.013$, $p > 0.05$) nor the relationship between denial of injury (NDoI) and intention to commit fraud ($b = 0.053$, $t=0.073$, $p > 0.05$).

As stated in the preceding section, perceived denial of risk acts as a strong positive moderator, it influences denial of victim but not denial of responsibility nor denial of injury as neutralization techniques. This suggests that individuals who employ denial of victim technique are more influenced by denial of risk in intentions to commit online romance fraud. We conducted a simple slopes test to explore the intricacies of the interaction.

Table 6: Results of simple slope test

	simple slope	**S. E.**	**t-stat**	**Df**	**p-value**

Low DoR	0.060	0.063	0.949	316	>0.05
High DoR	0.338	0.089	3.779	316	<0.05

In addition, we examined the plot interaction to visually present how low and high degrees of denial of risk influence the effect of denial of victim on intention to commit internet romance fraud as shown in figure 2.

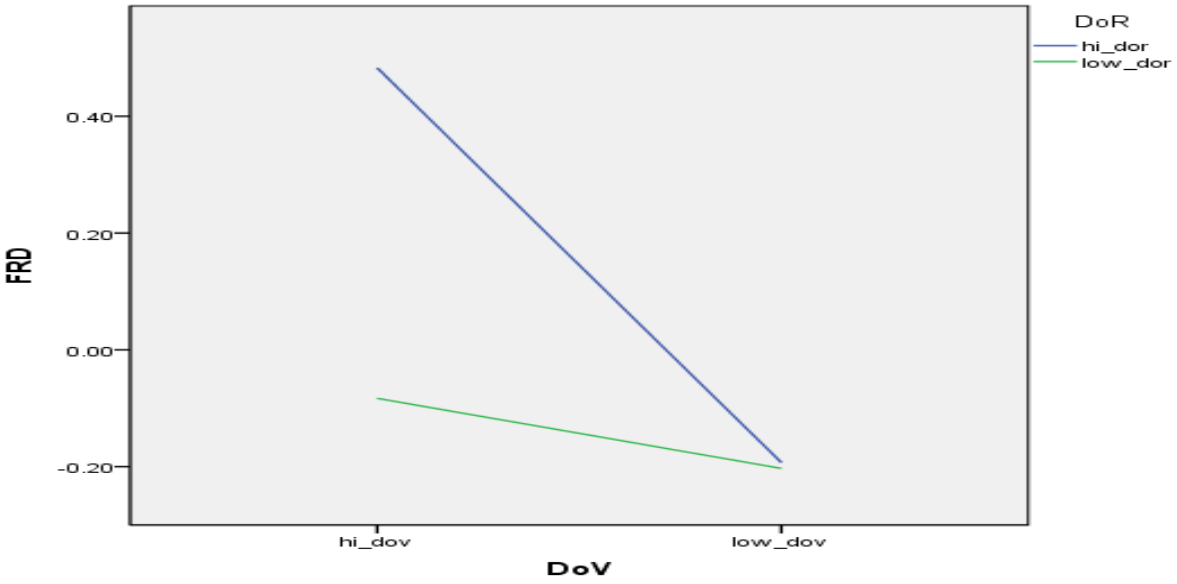

Figure 2: Interaction Plot

The plot (figure 2) shows that the relationship between NDoV and intention to commit online romance fraud is positive and significant only when denial of risk is high. As an offender moves from low to high denial of victim, the presence of low denial of risk is not significant on predicting intention to commit online fraud but it is significant under high denial of risk condition. Table 7 presents a summary of the analysis.

Table 7: Summary of structural model results

Hypothesis	Path	Coef.	S.E>	T Stat.	P Values
H1a	NDoR -> FRD	0.136	0.094	1.446	0.148
H1b	NDoI -> FRD	0.020	0.078	0.259	0.796
H1c	NDoV -> FRD	0.211	0.071	2.988	0.003

H2	DOR -> FRD	0.199	0.075	2.661	0.008
H3a	Mod_DoV -> FRD	0.115	0.057	2.083	0.038
H3b	Mod_NDoR -> FRD	-0.048	0.066	1.013	0.312
H3c	Mod_NDoI -> FRD	0.053	0.073	0.609	0.545

4. Discussion and Implications

Prior literature in both information systems security and criminology research suggest that individuals use several neutralization techniques to justify the intention to commit crime such as software piracy (Copes 2003; Siponen et al. 2012). However, different techniques of neutralization are deployed under different circumstances and each has different effectiveness (Barlow et al. 2013). We emphasize in this study the importance of understanding the techniques deployed under circumstances where emotional involvement may be high. Given the uniqueness of ORF due to the emotional involvement of the victims, the context would suggest that offenders seek to absolve themselves from self-blame and win the sympathy of others by demonstrating the denial of responsibility, injury and the victim. We deployed this subset of neutralization techniques in our inquiry. Following Zhang and Leidner (2018) and Williams (1986), we argue that three neutralization techniques; denial of injury, denial of victim and denial of responsibility, would be employed to justify online romance fraud. The evidence from this study suggests that only denial of victims is used to justify the intention to defraud victims in online romance. The explanation is that, the offenders seek to focus on the deception of benefits from both partners involved in the online romance and that any emotional or financial damage should be accepted. Therefore, to the offender, none of the partners can claim to be a victim. It is interesting to notice that the offenders realize that it is difficult to claim no responsibility and no injury. This is because, the victim could demonstrate when necessary, the loss of money and other emotional damages and that the offender is responsible. For the offender, if they can justify that there is no victim, then they alone cannot be held responsible, shifting the responsibility to both parties or eliminating any blame for who is and who is not responsible. In the same way if there is no victim then the issue of injury will be difficult to prove. Hence, offenders feel that all they must do to justify their action is to invest such resources as time. Perpetrators occasionally give gifts to their victims and spend considerable amount of time to provide companionship for their victims (Rege 2009). The seeming trust that is developed as result of offender investments blinds potential victims from suspicion. Victims do not initially regard their online romance partners as fraudsters but as friends who become their perceived romantic partners, share common interest and owe

each other responsibility of happiness. Thus, perception of no risk to the offender influences likelihood of delinquent acts (Farahmand and Spafford 2013).

The findings about the effect of denial of risk is consistent with literature on deviant behaviour in criminology where offender rationalize their actions to absolve themselves from any concerns. For instance, some individuals who use cannabis may scapegoat hard drugs users, emphasize their own ability to control their consumption, or consider their actions as less risky (Peretti-Watel 2003; Tombor et al. 2010). In the online romance fraud context, offenders consider their actions as a game in which they play using tools such as VPN's, credit card details, victims' personal information, dating websites, software (Ebenezer et al. 2016). Because offenders consider their actions as part of a game, they deny any risk by exhibiting a lot of self-confidence in their ability to avoid any negative consequences such as evading arrest. Additionally, online fraudsters rationalize their crimes by considering online romance as a game that is perceived as less aggressive and dangerous compared with other crimes such as murder or burglary. Lower perception of risk influence the tendency to commit delinquent acts (Farahmand and Spafford 2013).

4.1 Implications for research

This study has highlighted dimensions of neutralization theory and techniques used in online romance fraud context. Our empirical evidence suggests that even when individuals recognise that online fraud may be a criminal activity, they justify their actions by either denying the victim or responsibility for the crime. Our research in the online romance fraud context has revealed that the intent to commit crime by justifying the actions is entangled with significant rejections of the presence of risk. As expectation of perceived denial of risk increases, it changes the crime justification techniques and tendency to commit crime dynamics. This outcome explicates the boundary conditions of neutralization theory. By focusing on the boundaries of neutralization techniques, this study can provide insights into some of the inconsistencies in information systems studies on illegal acts (Siponen et al. 2012; Siponen and Vance 2010; Vance et al. 2019). An offender's perceived capacity and culpability affect their crime outlook (Liao et al. 2017). The presence or absence of risk alters the effect of techniques employed to justify illegal acts.

4.2 Implication for practice

The adoption of broad criminological theories has enhanced the understanding of why people commit various forms of crimes (Gilmour 2016). The evidence found in this study is that, a perspective involving only justification or only rationalization cannot fully explain the intention to commit fraud on dating sites. Some dimensions of neutralization

techniques and denial of risk are significantly associated with the intention to commit online romance fraud. The effect of each factor provides interesting insights for educating victims of online romance fraud, the operators of online dating sites and to a broader extent, the international effort to combat online romance fraud. Routine activity theory suggests that for crime to successfully occur, the motivation of the offenders, appropriate targets and absence of a capable guardian must converge (Cohen and Felson 1979; Xu et al. 2013). The findings of the study inform the three ingredients for successful crime occurrence.

First, for the motivation of the perpetrators, the results provide insight into the inspiration for committing the crime on dating sites. Specifically, lack of perception accountability and non-acceptance of the target are key justification and rationalization techniques. For jurisdictions that are saddled with increasing number of people involved in this type of crime, education should be designed to communicate the devastating toll their actions have on their victims including mental health crisis and death. The goal would be to influence the conscience of the perpetrators that their justification for the crime using such factors as physical separation from their victim or that victims' voluntary engaged in the scam is flawed narrative. The actions of online fraud can have negative impact on the communities they reside. For instance, PayPal has blacklisted some of the countries where most of the crimes originate (Karimi 2019). It therefore behoves the community where the perpetrators reside to frown on online romance fraud and other internet crimes because the whole community can suffer the consequences of the crime although they are not direct victims.

Second, for the appropriate target, educational materials should aim to advance how victims make themselves vulnerable to such scam. Although, dating sites are provided with some level of immunity from legal prosecution for content posted or scam through the platform (Derzakarian 2017), the operators can still contribute to combating the online romance fraud phenomenon. The development of quick guide similar to tips provided by the FTC (Karimi 2019) or anonymous contact shell on dating sites where potential victims can crosscheck if they are falling victim would reduce likelihood of victimization. Also, administrators of dating websites should design screening mechanism that can help flag individuals who have denial of risk or victim perceptions on their platforms. For instance, pointers of over-confidence by a participant on the dating platform, would serve as signal to both the administrator and other participants, the likelihood of a potential offender using denial of risk to defraud. Similarly, a measurement of and communication of participants level of empathy, would provide insights for administrators and other participants about denial of victim tendencies. Such pointers can minimize the occurrence of romance fraud through these platforms. Such

mechanisms would help prevent individuals with genuine interest in online dating sites from falling prey to romance fraudsters.

Third, for the absence of capable guidance, the results suggest that perpetrators' perception of low or no risk increases their justification and motivation to engage in online romance fraud. Thus, there should be visible evidence that there are institutions equipped and backed by legislation to combat online romance fraud irrespective of where the victim or perpetrator resides. As law enforcement agencies work to prevent the occurrence of online romance fraud, they can educate individuals on dating websites on techniques used by individuals to rationalize their criminal conduct in addition to techniques used to justify such actions.

4.3 Limitations

The study was restricted to only one context and therefore the results may not be generalizable to another contexts. Also, we were unable to obtain the income levels of our respondents. The level of income would influence the decision to engage in online romance. Therefore, future research that includes such information would advance our understanding of motivations for online romance fraud. Additionally, the survey method used by the researchers depended largely on the state of mind of the respondents at the time of filling the questionnaire. Our study is at the individual level and non-workplace environment context. There is potential for social desirability in responding to the survey. That may explain why the r^2 of the study is 0.111 which is lower than prior studies such as Siponen et al., (2012) with r^2 of about 0.3, that employ neutralization theory along with other theories. Using obtained objective data that may reveal more insights on the neutralization dynamics in the context of online romance fraud and other psychological factors that maybe at play. Thus, future research should adopt other research technique to obtain objective data from respondents or survey respondents from multiple contexts to provide further insights to the phenomenon under consideration.

References

Apostolidis, T., Fieulaine, N., Simonin, L., and Rolland, G. 2006. "Cannabis Use, Time Perspective and Risk Perception: Evidence of a Moderating Effect†," *Psychology & Health* (21:5), pp. 571–592. (https://doi.org/10.1080/14768320500422683).

Aransiola, J. O., and Asindemade, S. O. 2011. "Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria," *Cyberpsychology, Behavior, and Social Networking* (14:12), pp. 759–763. (https://doi.org/10.1089/cyber.2010.0307).

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. 2013. "Don't Make Excuses! Discouraging Neutralization to Reduce IT Policy Violation," *Computers & Security* (39), pp. 145–159. (https://doi.org/10.1016/j.cose.2013.05.006).

Boateng, R., Olumide, L., Isabalija, R. S., and Budu, J. 2011. "Sakawa - Cybercrime and Criminality in Ghana," *Journal of Information Technology Impact* (11:2), pp. 85–100.

Brenhoff, A. 2017. "How a Billion-Dollar Internet Scam Is Breaking Hearts and Bank Accounts," *HUFFPOST*. (https://www.huffpost.com/entry/romance-scams-online-fbi-facebook_n_59414c67e4b0d318548666f9).

Buchanan, T., and Whitty, M. T. 2014. "The Online Dating Romance Scam: Causes and Consequences of Victimhood," *Psychology, Crime & Law* (20:3), pp. 261–283. (https://doi.org/10.1080/1068316X.2013.772180).

Cao, L. 2004. *Major Criminological Theories: Concepts and Measurement*, CA: Wadsworth Publishing Company.

CBC News. 2017. "Flirting with Fraud: Police Take Aim at Romance Scams," *CBS*. (https://www.cbc.ca/news/canada/manitoba/romance-scam-fraud-prevention-month-winnipeg-1.4004692).

Cheng, L., Li, W., Zhai, Q., and Smyth, R. 2014. "Understanding Personal Use of the Internet at Work: An Integrated Model of Neutralization Techniques and General Deterrence Theory," *Computers in Human Behavior* (38), pp. 220–228. (https://doi.org/10.1016/j.chb.2014.05.043).

Cohen, L. E., and Felson, M. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* (44:4), p. 588. (https://doi.org/10.2307/2094589).

Copes, H. 2003. "Societal Attachments, Offending Frequency, and Techniques of Neutralization," *Deviant Behavior* (24:2), pp. 101–127. (https://doi.org/10.1080/01639620390117200).

Costello, B. J. 2000. "Techniques of Neutralization and Self-Esteem: A Critical Test of Social Control and Neutralization Theory," *Deviant Behavior* (21:4), pp. 307–329. (https://doi.org/10.1080/016396200404113).

Cross, C. 2015. "No Laughing Matter: Blaming the Victim of Online Fraud," *International Review of Victimology* (21:2), pp. 187–204. (https://doi.org/10.1177/0269758015571471).

Cross, C. 2018. "(Mis)Understanding the Impact of Online Fraud: Implications for Victim Assistance Schemes," *Victims & Offenders* (13:6), pp. 757–776. (https://doi.org/10.1080/15564886.2018.1474154).

Derzakarian, A. 2017. "The Dark Side of Social Media Romance: Civil Recourse for Catfish Victims," *Loyola of Los Angeles Law Review* (50), p. 25.

Ebenezer, A. J., Paula, A. M., and Allo, T. 2016. *Risk And Investment Decision Making In The Technological Age: A Dialysis Of Cyber Fraud Complication In Nigeria*. (https://doi.org/10.5281/ZENODO.58522).

Evans, R. D., and Porche, D. A. 2005. "The Nature and Frequency of Medicare/Medicaid Fraud and Neutralization Techniques among Speech, Occupational, and Physical Therapists," *Deviant Behavior* (26:3), pp. 253–270. (https://doi.org/10.1080/01639620590915167).

Farahmand, F., and Spafford, E. H. 2013. "Understanding Insiders: An Analysis of Risk-Taking Behavior," *Information Systems Frontiers* (15:1), pp. 5–15. (https://doi.org/10.1007/s10796-010-9265-x).

Fornell, C., and Larcker, D. F. 1981. "Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics," *Journal of Marketing Research*, pp. 382–388.

Gilmour, N. 2016. "Preventing Money Laundering: A Test of Situational Crime Prevention Theory," *Journal of Money Laundering Control* (19:4), pp. 376–396. (https://doi.org/10.1108/JMLC-10-2015-0045).

Hadzhidimova, L., and Payne, B. 2019. *The Profile of the International Cyber Offender in the U.S.*, (2:1), pp. 40–55.

Hair, J. F., Risher, J. J., Sarstedt, M., and Ringle, C. M. 2019. "When to Use and How to Report the Results of PLS-SEM," *European Business Review* (31:1), pp. 2–24. (https://doi.org/10.1108/EBR-11-2018-0203).

Hair Jr, J. F., Anderson, R. E., Tatham, R. L., and William, C. 1995. *Multivariate Data Analysis with Readings*, New Jersy: Prentice Hall.

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257–278. (https://doi.org/10.2307/249656).

Hinduja, S. 2007. "Neutralization Theory and Online Software Piracy: An Empirical Analysis," *Ethics and Information Technology* (9:3), pp. 187–204. (https://doi.org/10.1007/s10676-007-9143-5).

Ho, S. M., Lowry, P. B., Warkentin, M., Yang, Y., and Hollister, J. M. 2017. "Gender Deception in Asynchronous Online Communication: A Path Analysis," *Information Processing & Management* (53:1), pp. 21–41. (https://doi.org/10.1016/j.ipm.2016.06.004).

Hutchings, A., and Clayton, R. 2016. "Exploring the Provision of Online Booter Services," *Deviant Behavior* (37:10), pp. 1163–1178. (https://doi.org/10.1080/01639625.2016.1169829).

Ibrahim, S. 2016. "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals," *International Journal of Law, Crime and Justice* (47), pp. 44–57. (https://doi.org/10.1016/j.ijlcj.2016.07.002).

Ingram, J. R., and Hinduja, S. 2008. "Neutralizing Music Piracy: An Empirical Examination," *Deviant Behavior* (29:4), pp. 334–366. (https://doi.org/10.1080/01639620701588131).

Karimi, F. 2019. "Americans Lost $143 Million in Online Romance Scams Last Year. That's Way More than Any Other Reported Fraud," *CNN*. (https://www.cnn.com/2019/08/23/us/online-romance-scams-losses-trnd/index.html).

Liao, R., Balasinorwala, S., and Raghav Rao, H. 2017. "Computer Assisted Frauds: An Examination of Offender and Offense Characteristics in Relation to Arrests," *Information Systems Frontiers* (19:3), pp. 443–455. (https://doi.org/10.1007/s10796-017-9752-4).

Luu, V., Land, L., and Chin, W. 2017. "Safeguarding Against Romance Scams – Using Protection Motivation Theory," in *In Proceedings of the 25th*, Guimarães, Portugal, June 5, pp. 2429–2444.

Moore, T., Clayton, R., and Anderson, R. 2009. "The Economics of Online Crime," *Journal of Economic Perspectives* (23:3), pp. 3–20. (https://doi.org/10.1257/jep.23.3.3).

Mosley, M. A., Lancaster, M., Parker, M. L., and Campbell, K. 2020. "Adult Attachment and Online Dating Deception: A Theory Modernized," *Sexual and Relationship Therapy* (35:2), pp. 227–243. (https://doi.org/10.1080/14681994.2020.1714577).

Muthén, L. K., and Muthén, B. O. 2005. *Mplus: Statistical Analysis with Latent Variables: User's Guide*, Los Angeles.

Peppeh, K. O. 2018. "'Sakawa Boys': Meet the Professional Internet Fraudsters of Ghana," *IDG Connect*. (https://www.csoonline.com/article/3258549/sakawa-boys-meet-the-professional-internet-fraudsters-of-ghana.html).

Peretti-Watel, P. 2003. "Neutralization Theory and the Denial of Risk: Some Evidence from Cannabis Use among French Adolescents," *British Journal of Sociology* (54:1), pp. 21–42. (https://doi.org/10.1080/0007131032000045888).

Pershing, J. L. 2003. "Why Women Don't Report Sexual Harassment: A Case Study of an Elite Military Institution," *Gender Issues* (21:4), pp. 3–30. (https://doi.org/10.1007/s12147-003-0008-x).

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies.," *Journal of Applied Psychology* (88:5), pp. 879–903. (https://doi.org/10.1037/0021-9010.88.5.879).

Priest, T. B., and McGrath III, J. H. 1970. "Techniques of Neutralization: Young Adult Marijuana Smokers," *Criminology* (8:2), pp. 185–194.

Rege, A. 2009. *What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud*, (3:2), p. 19.

Reinartz, W., Haenlein, M., and Henseler, J. 2009. "An Empirical Comparison of the Efficacy of Covariance-Based and Variance-Based SEM," *International Journal of Research in Marketing* (26:4), pp. 332–344. (https://doi.org/10.1016/j.ijresmar.2009.08.001).

Silic, M., Barlow, J. B., and Back, A. 2017. "A New Perspective on Neutralization and Deterrence: Predicting Shadow IT Usage," *Information & Management* (54:8), pp. 1023–1037. (https://doi.org/10.1016/j.im.2017.02.007).

Siponen, M., Pahnila, S., and Mahmood, M. A. 2010. "Compliance with Information Security Policies: An Empirical Investigation," *Computer* (43:2), pp. 64–71.

Siponen, M., Puhakainen, P., and Vance, A. 2020. "Can Individuals' Neutralization Techniques Be Overcome? A Field Experiment on Password Policy," *Computers & Security* (88), p. 101617. (https://doi.org/10.1016/j.cose.2019.101617).

Siponen, M., Vance, A., and Willison, R. 2012. "New Insights into the Problem of Software Piracy: The Effects of Neutralization, Shame, and Moral Beliefs," *Information & Management* (49:7–8), pp. 334–341. (https://doi.org/10.1016/j.im.2012.06.004).

Siponen, and Vance. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487–502. (https://doi.org/10.2307/25750688).

Sorell, T., and Whitty, M. 2019. "Online Romance Scams and Victimhood," *Security Journal* (32:3), pp. 342–361. (https://doi.org/10.1057/s41284-019-00166-w).

Straub, D., Boudreau, M.-C., and Gefen, D. 2004. "Validation Guidelines for IS Positivist Research," *Communications of the Association for Information Systems* (13:1), p. 63.

Sykes, G. M., and Matza, D. 1957. "Techniques of Neutralization: A Theory of Delinquency," *American Sociological Review* (22:6), p. 664. (https://doi.org/10.2307/2089195).

Tombor, I., Urbán, R., Berkes, T., and Demetrovics, Z. 2010. "Denial of Smoking-Related Risk among Pregnant Smokers," *Acta Obstetricia et Gynecologica Scandinavica* (89:4), pp. 524–530. (https://doi.org/10.3109/00016341003678427).

U.S. Department of Justice. 2019. "10 Men Involved in Nigerian Romance Scams Indicted for Money Laundering Conspiracy," *The United States Department of Justice*. (https://www.justice.gov/opa/pr/10-men-involved-nigerian-romance-scams-indicted-money-laundering-conspiracy).

Vance, A., Mikko, T. S., and Detmar, W. S. 2019. "Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations Across Cultures," *Information & Management*, p. 103212.

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

Whitty, M. T., and Buchanan, T. 2016. "The Online Dating Romance Scam: The Psychological Impact on Victims – Both Financial and Non-Financial," *Criminology & Criminal Justice* (16:2), pp. 176–194. (https://doi.org/10.1177/1748895815603773).

Williams, E. J., Beardmore, A., and Joinson, A. N. 2017. "Individual Differences in Susceptibility to Online Influence: A Theoretical Review," *Computers in Human Behavior* (72), pp. 412–421. (https://doi.org/10.1016/j.chb.2017.03.002).

Williams, L. M. 1986. "Race and Rape: The Black Woman as Legitimate Victim," *National Inst. of Mental Health (DHHS), Rockville, Md.*, pp. 1–35.

Willison, R., Warkentin, M., and Johnston, A. C. 2018. "Examining Employee Computer Abuse Intentions: Insights from Justice, Deterrence and Neutralization Perspectives: Examining the Influence of Disgruntlement on Computer Abuse Intentions," *Information Systems Journal* (28:2), pp. 266–293. (https://doi.org/10.1111/isj.12129).

Wong, N., Ray, P., Stephens, G., and Lewis, L. 2012. "Artificial Immune Systems for the Detection of Credit Card Fraud: An Architecture, Prototype and Preliminary Results: Artificial Immune Systems for the Detection of Credit Card Fraud," *Information Systems Journal* (22:1), pp. 53–76. (https://doi.org/10.1111/j.1365-2575.2011.00369.x).

Xu, Z., Hu, Q., and Zhang, C. 2013. "Why Computer Talents Become Computer Hackers," *Communications of the ACM* (56:4), pp. 64–74. (https://doi.org/10.1145/2436256.2436272).

Zhang, S., and Leidner, D. 2018. "From Improper to Acceptable: How Perpetrators Neutralize Workplace Bullying Behaviors in the Cyber World," *Information & Management* (55:7), pp. 850–865. (https://doi.org/10.1016/j.im.2018.03.012).

Appendix 1

Denial of Risk (source) **1-Strongly Agree, 2-Agree, 3-Neither Agree nor Disagree, 4- Disagree, 5 - Strongly Disagree.**		1	2	3	4	5
Dor1	Defrauding “clients” is not as bad as ‘blood money’.					
Dor2	Defrauding “clients” is not as bad as ‘Sakawa’.					
Dor3	Defrauding “clients” is not as bad as corruption.					
Dor4	I know how to get “clients” believe in me than the average person.					
Dor5	It is not dangerous to maintain relationship with “clients” after defrauding them.					
Dor6	I have confidence in determining “clients” who are less willing to be defrauded.					
Denial of Victim **1-Strongly Agree, 2-Agree, 3-Neither Agree nor Disagree, 4- Disagree, 5 - Strongly Disagree.**		1	2	3	4	5
Neutdov1	It is not wrong to defraud “clients” because they live abroad					
Neutdov2	It is not wrong to defraud “clients” because they are wealthy.					
Neutdov3	It is not wrong to defraud “clients” because they live in the richest countries in the world.					
Neutdov4						
Intention to Commit Internet Romance Fraud **1-Strongly Agree, 2-Agree, 3-Neither Agree nor Disagree, 4- Disagree, 5 - Strongly Disagree.**		1	2	3	4	5
Frd1	What is the chance that you will defraud “clients”?					
Frd2	I am certain that I will defraud “clients”					
Frd3	I am likely to defraud “clients”					
Denial of Injury **1-Strongly Agree, 2-Agree, 3-Neither Agree nor Disagree, 4- Disagree, 5 - Strongly Disagree.**		1	2	3	4	5
Neutdoi1	It is ok to defraud “clients” if no one gets hurt.					
Neutdoi2	It is ok to defraud “clients” if no harm is done.					
Neutdoi3	It is ok to defraud “clients” if no damage is done.					
		1	2	3	4	5
Neutdor1	It is ok to defraud “clients”, if you are not aware of any law related to your action.					
Neutdor2	It is ok to defraud a “client” if you are not sure what the law is.					
Neutdor3	It is ok to defraud “clients” if you do not understand the implication of your action.					