Association for Information Systems

AIS Electronic Library (AISeL)

AMCIS 2020 Proceedings

Information Security and Privacy (SIGSEC)

Aug 10th, 12:00 AM

Rationalizing Online Romance Fraud: In the Eyes of the Offender

Jonathan Nii Barnor Barnor
University of Ghana Business School, jnbbarnor@st.ug.edu.gh

Richard Boateng
University of Ghana Business School, richboateng@ug.edu.gh

Emmanuel Awuni Kolog
University of Ghana Business School, eakolog@ug.edu.gh

Anthony Afful-Dadzie
University of Ghana Business School, aafful-dadzie@ug.edu.gh

Rationalizing Online Romance Fraud: In the Eyes of the Offender

Completed Research

Jonathan Nii Barnor Barnor
University of Ghana Business School
jnbbarnor@st.ug.edu.gh

Richard Boateng
University of Ghana Business School
richboateng@ug.edu.gh

Emmanuel Awuni Kolog
University of Ghana Business School
eakolog@ug.edu.gh

Anthony Afful-Dadzie
University of Ghana Business School
aafful-dadzie@ug.edu.gh

Abstract

This study seeks to understand romance scam from the offenders' perspective and how they rationalize their motivations, opportunities and abilities towards the commission of the crime. To this end, we adopt the Motivation-Opportunity-Ability framework and the Rationalization dimension of the Fraud Triangle Theory. The study employed a qualitative methodological approach to analyze the opportunities presented by emerging technologies to cyber fraudsters amid socio-economic drivers. One is the interplay of various socio-economic factors being a major driving force behind the commission of cybercrime. These include peer recruitment and training, poverty, unemployment, low level of education and low income. The uniqueness of this study stems from the fact that it deviates from previous studies to investigate cybercrime from the perspective of the perpetrators. Again, this study is arguably one of the first to put all three dimensions of the MOA framework and the rationalization dimension of the Fraud Triangle to study romance scammers' behaviors.

Keywords

Cybercrime, Romance Scam, Motivation, Opportunity, Ability, Rationalization.

Introduction

Cybercrimes are considered global crimes; they transcend geographical boundaries and can be perpetuated from anywhere against any individual, any organization and any technology (Donalds and Osei-Bryson 2019). Among the many forms of cybercrime is online romance scams (also called online dating scams or sweetheart swindles), which became apparent around 2008 and had its root in paper-mail based fraud (Whitty and Buchanan 2012). CNN (2019) for instance, reports that online romance scams cost Americans more than any other reported fraud in 2018. In 2018 alone, more than 21,000 vulnerable people were conned into sending $143 million in online romance scam cases from a reported $88 million in 2017. It is therefore not surprising that the internet has become a breeding ground for romance scammers, especially considering the spectrum of the growing market in that form of cybercrime. Apart from the financial losses, romance scam victims are also left with emotional and psychological damages to battle (Kopp et al. 2015; Luu et al. 2017).

Extant literature have studied the subject of online romance scam from various perspectives (Buchanan and Whitty 2014; Luu et al. 2017; Suarez-Tangil et al. 2019; Whitty 2013). For example, Buchanan and Whitty's (2014) study on causes and consequences of online dating scam victimhood made use of 853 online daters who completed a battery of online questionnaires. The finding of the study suggested that there are emotional as well as financial consequences of victimhood, and many people may be severely affected even if they do not lose money. Again, Luu et al. (2017) in a study that aimed at addressing issues of online dating fraud from an empirical risk mitigation approach suggested that an online dater's assessment of the protective mechanism (and protective response) generally has a more considerable influence on adopting protective behavior than the evaluation of the scam itself. Nonetheless, the authors aver that issues of online dating fraud have yielded increasing attention from diverse disciplines, though studies remain scarce. Particularly, investigation of romance fraud from a risk mitigation and information systems approach has been neglected.

Despite the growing body of studies in cybercrime and online romance scam for that matter, there seem to be a number of issues that can influence future research. First, the gaps in the literature point to the fact that there appears to be a dominance of studies on the various forms of online romance fraud from various disciplines (Kopp et al. 2015) while online romance scams in the field of information systems remain sparse. Again, extensive evaluation of the foregoing research revealed that most online romance scam studies had studied the phenomenon from the victim's perspective (see table 1). Hence, studies that consolidate the perpetrators' perspectives on the commission of internet romance crimes arguably remain scant. This study therefore seeks to address the objective of understanding the triggers of online romance fraudsters' behaviors. Thus, evaluating the motivational, opportunities and the abilities of the perpetrators and how they rationalize these triggers.

The remainder of this paper is organized as follows. The next section highlights a brief overview of online dating romance. The following sections present the theoretical foundation on which this study is based. We discuss the methodology for the study, followed by a summary of findings, and we conclude with discussions, conclusion and implications.

Online Dating Romance Scam

Online dating romance scam, otherwise known as *sweetheart swindles*, has been likened to have the *spirit* of the advance fee fraud (Huang et al. 2015). According to Whitty (2015) however, the portrayed end goal for the victim is typically that they will be in a committed relationship rather than merely in receipt of large sums of money. In this type of scam, criminals create fake social network site profiles to attract the trust of people into relationships to financially defraud them (Budd and Anderson 2011; Whitty 2019; Whitty and Buchanan 2016). They then upload photographs ranging from low-quality to heavily pixilated photographs of the same crafty socially engineered person in order to strengthen their credibility. The second stage is to maintain consistent contact with the would-be victim. This requires the establishment of a strong bond with the target through constant contact to engender trust, confidence and romantic connections (Rege 2009). Cross, Dragiewicz and Richards (2018) for instance, contend that once trust is proven, offenders resort to a variety of modes of communication, including email, telephone and text messaging to maintain the ruse. Stage three according to Whitty (2015) is the sting stage where scammers attempt to con the victim out of money. If they failed in the first instance, they go back to the grooming stage (stage two). In some instances in stage three, criminals craft tragic stories, theft of personal documents during travel, unexpected hospital expenses resulting from sudden accidents or illnesses (Rege 2009) to solidify their legitimacy.

Further, victims are sometimes unable to identify such scams considering the length of the period it takes to create a relationship and build trust in these scams. Rege (2009) posits that such relationships take as long as six to eight months until trust is built. The final stage is the revelation stage, where victims identify that they have been scammed. Whitty (2015) opines that some financial victims realize the scams themselves and seek out evidence to support their premonitions whiles victims who fairly quickly identify the scam exit at stage 3.

Theoretical Foundation

Online romance fraud is an ever-growing phenomenon and for that matter has been studied from diverse disciplines. Again, as indicated in the upper sections of this paper, Wada, Longe and Danquah (2012) contend that empirical evidence to the application and validation of theories in the context of cybercriminal activities is sparse. Though several online romance scam studies have been conducted, a few of them have employed theories to back their studies. With this, Table 1 summarises some online romance fraud studies that have been conducted in the past few years.

Study	Theory	Methodology	Perspective
Buchanan and Whitty (2014)	N/A	Quantitative	Victim
Kopp et al., (2015)	N/A	Qualitative	Victim
Sorell and Whitty (2019)	N/A	Qualitative	Victim
Luu et al., (2017)	Protection Motivation Theory	Quantitative	Victim
Jong (2019)	N/A	Quantitative	Dating platform

Table 1. Previous Online Romance Scam Studies

While these studies are valuable in studying cybercrime in the context of online dating romance fraud, most studies seem to be silent on the perpetrators' perspective of issues. Again, studies that have attempted to fill this gap (not necessarily from online romance fraud) have done that only focusing on one or a combination of two of motivation, opportunity, ability and rationalization dimensions. This therefore warrants the need to attempt a study from the viewpoint of the offender, which will put all these dimensions into perspective. To this end, we adopt the Motivation, Opportunity, Ability Framework postulated by MacInnis and Jaworski (1989) and the rationalization dimension of the fraud triangle theory proposed by (Cressey 1950).

The Motivation, Opportunity and Ability Framework

The motivation-opportunity-ability (MOA) framework was established to explain how consumers process information in advertisements (Clark et al. 2005). The MOA framework, which was postulated by MacInnis and Jaworski (1989) suggests that individuals process information based on their underlying motives, opportunities and abilities (Parra-López et al. 2012). It has successfully been used in various disciplines to explain a wide array of behaviors. This includes but not limited to knowledge sharing (Siemsen et al. 2008), social media (Parra-López et al. 2012), consumer choices and firm-level decision making (Maclnnis et al. 1991; Wu et al. 2004). Nonetheless, the framework has been used more recently as studies in knowledge-management practice and research (Argote et al. 2003; Siemsen et al. 2008) and also used in management disciplines when discussing an individuals' work performance (Siemsen et al. 2008).

The first component of the MOA framework is the *motivation* dimension, which has been identified as the driving force that pushes an individual to make a decision. In conceptualizing the motivation dimension of the framework, Murphy and Dacin (2011) referred to motivation as the pressures to commit fraud which includes social pressures such as how individuals wish to be seen by others. It is however worth noting that motivation is a unitary phenomenon as the level of motivation varies from one person to the other (Ryan and Deci 2000).

Relative to fraud perpetration, a number of existing studies have delineated some motivations toward the commission of online crimes. For instance, a study by Ngafeeson (2010) that developed a motivational model of cybercrime conceptualized motivation as the various factors that push people to carry out cybercrime. This push may be as a result of the determinants of crime; unemployment, low median income, poverty, wage inequality, social status, et cetera. According to Ngafeeson (2010) cybercriminals indulge in cybercrimes driven by their desire to satisfy personal needs. Such needs can be psychological, safety needs, belonging needs, esteem needs and self-actualization needs (Maslow 1981).

Opportunity is the second dimension of the MOA framework which is the circumstances that allow or facilitate people to perform a behavior (Hung and Petrick 2012). Opportunity reflects the presence of enabling environmental mechanisms that facilitate task performance and are the external contextual factors that enable performance. According to Gruen, Osmonbekov and Czaplewski (2005) this dimension of the framework reflects the extent to which a situation is conducive to achieving a desired outcome.

Situational factors such as the time available, attention paid, number of distractions, or number of repetitions that something is available were projected by MacInnis and Jaworski (1989) to be factors that can either impede or enhance the desired outcome. Based on extant research, opportunity in relation to the commission of fraud has been identified as one that arises when a fraudster sees a way to use his or her position of trust to solve a financial problem, knowing he or she is unlikely to be caught (Kassem and Higson 2012).

Ability concerns the person's internal skills or proficiencies that are required to complete a task (Fadel and Durcikova 2014). Ability is synonymous with skills and competences and reflects individuals' beliefs about their capacity during their performance and in the obtaining of results (Bigné et al. 2010). In brand information ads processing for instance, Maclnnis et al. (1991) conceptualized ability as the consumers' skills or proficiencies in interpreting brand information in an ad. Relative to cybercrimes and for that matter romance fraud, there seems to be a lack of studies that emphasize the abilities of the criminal, particularly with the MOA framework in perspective. Among the few studies reviewed include Hunton (2012) which aimed at extending his earlier research that first introduced the concept of the Cybercrime Execution Stack by examining in detail the underlying data objectives of the cybercriminal. In establishing why cybercriminals initiate data attacks, the author pointed out that the cybercriminal's ability to use technology and exploit the internet to access, manipulate and communicate electronic data directly is a fundamental feature in the commission of cybercrime and other illicit or criminal behaviors. This assertion by Hunton (2012) was found to be an essential aid to support the ability dimension of this study.

Rationalization

Rationalization is the mechanism by which an individual determines that his or her fraudulent behavior is *okay* in his or her mind (Coenen 2008) to reduce or avoid the negative effect that would normally accompany it (Murphy and Dacin 2011). It is a feeling of indifference assumed by an offender to justify the guilt resulting from his or misconduct. Rationalization as a justification for one's fraudulent behavior may be as a result of lack of personal integrity or other moral reasoning (Kassem and Higson 2012). During fraudulent activities, individuals must reconcile contradictions between their intended actions and general attitudes, which existing studies (Dellaportas 2013; Harrison 2018; Ramamoorti 2008) have referred to as cognitive dissonance.

The rationalization dimension of the theory has been studied in previous researeches (Albrecht et al. 1995; Anand et al. 2004; Peterson and Gibson 2003; Said et al. 2017) mostly in relation to fraudulent organizational activities. Studies that have studied why criminals rationalize offenses in cybercrime arguably remain very few. Again, one study that explicitly stated why cybercriminals rationalize their offenses was that of Whitty (2018). However, there are few studies even though silent on rationalization pointed out some traits of how and why cybercriminals justify their activities (Longe et al. 2009; Tade 2013).

In studying the pathways to cyberfraud criminality emanating from West Africa, specifically Nigeria, Whitty (2018) identified some reasons that cyber fraudsters attribute to the reasons why they commit internet crime as well as the justifications for the commission of those crimes. First among these justifications is the fact that West African cybercriminals target Westerners that they perceive to be greedy and stupid, popularly known in their vernacular as Maga or Muga. Cybercriminals rationalize the legitimacy of their crimes against such people as revenge for the perceived injustice they believe were meted out by their forefathers during the era of the Transatlantic slave trade. Secondly, cybercriminals (not only West African cybercriminals) tend to ride on the gullibility of their victims by claiming that the onus lies on the victims to recognize when they are being scammed. Finally, cybercriminals from the region rationalize other crimes to be worse than cyber offenses.

Methodology

This study employed a qualitative research approach in understanding cybercrime by investigating the perspectives and behaviors of romance fraud perpetrators in situations and the context within which they act. In that regard, we used semi-structured interviews as the primary means of data collection in which we asked case subjects questions related to cybercrimes. The snowballing technique was adopted for the recruitment of respondents for this study. First, internet café operators were interviewed, who then led us to potential perpetrators. A total of 10 perpetrators were interviewed from Accra in Ghana whom we interviewed face-to-face for 45 minutes to an hour, followed by phone conversations for clarification on unclear issues. All 10 respondents for the study were males with female accomplices who declined to take part in the study. Out of the 10 perpetrators, 4 operated as a group with shared facilities. The remaining 6 were interviewed randomly from 4 different internet cafés.

The validity of the data was further tested through the convergence of information from multiple sources. For instance, 8 bankers from two banks in Ghana (1 foreign and 1 indigenous) were interviewed to ascertain how they detect which withdrawals are legitimate and which ones are cybercrime-related. Again, lawyers and other law enforcement units were also interviewed to understand laws and policies that are in place to combat cybercrimes in the country. But for the purpose of this study, only the data collected from the perpetrators will be presented and analyzed.

Analytical techniques were drawn from Miles and Huberman (1994) qualitative data analysis approach, which identifies three other stages after data collection; data reduction, data display and drawing conclusion and verification. At the data reduction stage of the analysis, raw data collected from the field were organized by means of coding, where the data was reduced into meaningful segments and assigned labels for onward analysis. The next step was to write summaries of the coded data, which was further to reduce the weighty statements expressed by the data subjects into fewer words in efforts to move closer to the essence of the purpose of the research. While at this, the researchers kept focus on not losing the substance of the data as a result of data reduction. Secondly, in efforts to simplifying the complex nature of the phenomenon under study, we made use of tables (e.g. tables 3). This was done in consonance to Verdinelli and Scagnoli's (2013) claim that a visual display should be as uncomplicated as possible, and it should possess the right balance of valuable information and minimum detail, avoiding irrelevant off-topic content or information to achieve efficiency in helping the reader gain the intended message. At the early stages of the data collection and analysis, we identified and noted possible conclusions. However, those conclusions were ambiguous and revealed inadequate awareness of the facts. These conclusions in that regard were held tentative pending further review and were organized for presentation during analysis when all data were collected and reduced.

Summary of Findings

The main source of data for this study was collected among a cybercrime syndicate, which started in 2015. The group operates with four male members and female affiliates. The coming together of the group was as a result of specialization. The chief informant avers that *"people in this business have their strengths and weaknesses… I am very good at shopping. One of the guys is also good at chatting clients"*.

Pseudo-names	**Age***	**Educational Qualification**	**Years of Experience**
Chief Informant	27	Senior High School Leaver with partial IT training	Since 2008
GM2	25	Senior High School Leaver	Since 2011
GM3	25	Senior High School Leaver	Since 2011
GM3	26	Dropped out of senior high	Since 2013

Table 2. Profile of gang members

As evidenced in Table 2, the group is primarily made up of a young male cohort between the ages of 25 and 27 (at the time of data collection; 2017/18), with senior high school as the highest educational level. At the time of data collection, the Chief Informant (CI) had completed senior high school and had dropped out of IT training because his focus for enrolling in the IT training school was not met. Being the first of six, the CI claims that *"my family is not a rich family. My mother is a trader and my father is also a watchman. I am the firstborn and I have three brothers and two sisters"* and believes that the financial strength of the parents was inadequate to sustain a large family size as his. He avers that *"being the firstborn I need to sacrifice and help my parents to take care of the rest*." His position on cybercrime is that cybercrime is less a crime than traditional crimes (robbery). In his words, *"It is better to do something than do nothing… I can't go and steal from people…No it is bad to do that"*. At the time of data collection, the CI owned a car, a MacBook Pro and uses an iPhone 6.

Discussion of Findings

Motivated Scammer

Evidence from the data collected for this study suggested that peer recruitment and training, poverty, unemployment, low level of education and low-income influence individuals' decisions to commit romance scams. For instance, the romance scam syndicates interviewed for this study were young unemployed persons aiming to live meaningful lives from cybercriminal activities. Even though they give non-confirmatory responses to questions of traditional crimes, they believed cybercrime is less a crime than traditional crimes. Further, one of the respondents posits that *"I have five siblings. My father is a watchman* (security man) *and my mother is a trader. They can't take care of all of us, … so I have to do something to survive."* Another member of the group also opines that "*I didn't continue because of school fees; my senior sister too didn't finish because of school fees. My junior brother is also going to school but I don't know what will happen"*. On why he engages in internet scams, he simply explains that *"there are no jobs and man must eat"* however he joined the group as a result of association. The dynamics of this acknowledgment are not too different from that of the other members in the case group. This finding lends credence to Olayemi's (2014) finding that criminals engage in cybercrime principally as a result of unemployment, deprivation and a need to aspire to the higher socio-economic statuses of some others they see with no readily visible income-generating activities to justify such affluence.

Online romance scams take a lot of time and effort in getting accomplished. However, scammers take their time to walk victims through the romance scam trajectory. According to scammers, one's awareness of his or her situation (poverty, unemployment, among others) is enough motivation to be patient. For example, an independent scammer interviewed opined that *"the thing is about patience but it also depends on your level of intelligence. You can chat a client for 2 hours and everything falls into place. Sometimes too some of them are stubborn, so it takes a while to break them."*

Opportunities

In considering the motivations for the commission of internet crimes, a complete explanation must ultimately consider the sociocultural environments in which people conduct their daily lives (Choo and Tan 2007). This then leads the discussion to the configurations of the forces in the environment of a person that enables the person's work performance; opportunity (Blumberg and Pringle 1982)

Findings from the current study suggest that cybercriminals take advantage of weaknesses in existing laws to commit internet crimes. For example, our lead informer has been perpetuating cybercrime since 2008 and he enquires, "*how will the police know where I stay … They don't have the technology*?" This underlines their confidence that the police and agencies responsible for clamping down on cybercriminal activities lack the capabilities to do so. That is, they believe the authorities live in a different world with no technical knowledge of tackling the phenomenon head-on. For instance, one of the perpetrators claimed that *"We have a WhatsApp group where anytime there are new moves to beat the systems, someone will come and teach. So, they (the police) are always playing catchup."* A finding which corroborates with Olayemi's (2014) assertion that laws to combat cybercrimes are useless if law enforcement agencies do not have the education and training necessary even to operate a computer. Again, this finding supports claims by Mui and Mailley (2015) that opportunity becomes more attractive to perpetrators when the probability of being caught is low.

Ability

Ability has been identified as a person's internal skills or proficiencies that are required to complete the task. Lickiewicz (2011) pointed out some traits perceived to be abilities of cybercriminals in that regard; social and technical abilities. Social skills constitute the ability of an individual to function in a group as well as internalize social norms. Technical skills on the other hand are the general knowledge concerning programming languages, computer systems, network functioning.

Evidence from the data collected for this study points to the fact that online romance scammers possess both social and technical abilities. Social in the sense that the perpetrators are able to function as a group and also understand the functional duties of all members in the group. For instance, in their decision to come together as a group, the leader of narrates that "*everybody has his strength and weakness. I am good* *at shopping. Another person is good at chatting with clients. So, we decided to come together since we are all doing the same thing. At one point, my light will shine. At another point, another person's light will shine so we will all not go dry at the same time".* Again, their social relationships and ability to maintain constant storylines with victims cannot be overlooked. Scammers hold a high level of interactional social ability that helps them keep their victims to believe seemingly legitimate truth which turns out to be lies.

Further, confidence romance scammers possess technology-related abilities that cannot be overemphasized. While most of the people interviewed for the study had no formal computer training, they use basic functions of computers and related technologies in their daily operations. Except for the leader of the group who had some level of computer training, the rest learned the act on the job. Also, the perpetrators' awareness of the needed technology and applications to use at particular points in time affords them the leverage of outpacing their victims. For example, when asked how they deal with anonymity, one of our respondents narrated, *"There a number of them like the Dollar VPN, SOCKS, RDP. With the RDP, it is like having access to someone's computer in the US and using it. So, you will get access to the person's user ID and password and browse on the person's laptop without his knowledge.*

This outcome of the study is in line with Clough's (2010) assertion that the ability to commit computer crimes was largely limited to those with access and expertise. Today, the technology is ubiquitous and increasingly easy to use, ensuring its availability to both offenders and victims.

Rationalizing Online Romance Scam

This study has given a background of why individuals engage in cybercrime as well as their abilities and the environmental opportunities. This section of the study therefore presents the justification that romance fraud criminals impute to their involvement in the crime. It is important to note that the justification given by perpetrators of online romance scams may differ from person to person. Rationalization may be understood in this sense as the justification for one's unlawful behavior. In studying cybercriminal rationalization strategies, it is easy for one to misjudge offender motivation to the offender's crime rationalization. For example, while poverty may be the driving force for one's financial needs (motivation), the justification for whom he/she steals the money from is his/her rationalization for the commission of the crime.

Evidence from the data points to the fact that cybercriminals' targets are mostly the wealthy and financially sound westerners desperately seeking romantic relationships. While one of the respondents believe, the victims are wealthy and for that matter do not lose anything when they are scammed, an astonishing revelation was when one of the group members said *"They are credit cards from the Osama Bin Laden Bombing… those who died didn't die with their cards."* Even though this assertion may not be directly related to online romance fraud, the respondent believed the victims of the September 11 World Trade Center attack still have their monies on their cards and for that matter they are robbing from no one.

Again, online romance scam fraudsters interviewed for this study rationalize their activities as not being as dangerous as traditional crimes like robbery and murder. For example, a respondent claimed that "*No one can judge me with what I am doing unless a judge tells me that I am a criminal; nobody can call me a criminal."* He is of the view that cybercriminal activities are standard practices that people commit even without knowing. He again questions that *"those who have been downloading movies from pirate sites, do they pay? Do you call them cyber criminals?".* The respondent further maintains that cybercrime is less a crime than traditional crimes *"it is better to do something than do nothing… I can't go and rob people … No, it is bad to do that".* Romance scammers also claim that they take advantage of greedy, gullible and unintelligent westerners who are slow at identifying scam relationships. This, they believe, is a payback for the pain inflicted on their ancestors by the westerners during the era of the slave trade. This finding even though is in line with that of Whitty (2018) the claim of 9/11 victims being the target seems to be an eye-opener.

Conclusion and Implications

This study sought to consolidate how online romance fraudsters rationalize their motivations, opportunities available in the environment and their ability to commit online romance scams. Using a qualitative approach, four romance fraud perpetrators who operated as a group and six independent cybercrime perpetrators were interviewed and observed. The findings of this study brought to bear some findings with respect to the drivers, opportunity and ability of cybercriminal activities. First, an interplay of various socio-economic factors is a major driving force behind the commission of cybercrime. These include peer recruitment and training, poverty, unemployment, low level of education and low income. Second, cybercrime perpetrators ride on the availability of affordable technologies and network services. Third, the lack of confidence in law enforcement grants cybercriminals the opportunity to commit crimes. Again, online romance scammers possess basic computer and social skills which helps them in the commission of online scams. Finally, they find justifications to make sense of their unlawful behaviors.

The uniqueness of this study stems from the fact that it is arguably one of the first studies in information systems research to apply the MOA framework in the study of cybercriminal behaviors. This study again is arguably the first study to combine all four dimensions. Thus, motivation, opportunity, ability and rationalization. Previous studies that have attempted to understand the triggers of cybercrime have done so from either motivation, or motivation and rationalization. This implication cannot be overlooked as the study aims to add to the existing body of knowledge regarding cybercrime studies as well as respond to research gaps considering the sparsity of studies that employed the use of social or criminology theories.

Concerning policy and practice, this study will form a strong basis for banks, internet service providers as well as shipping and clearing agencies to collaborate with the police in the crack-down of cybercriminals. This research will also provide adequate findings for the Government of Ghana as well as law enforcement agencies responsible for enacting laws to expedite ongoing processes in formulating policies and regulations to govern irresponsible use of the internet among the citizenry.

While this study is unique in bringing the four dimensions together in a single study, there are few limitations that can guide future studies. First, we sought out to explore the motivation, ability and opportunity rationalization among romance fraud perpetrators. It is essential to note that the spectrum of cybercrime cuts across a wide range of internet offences. Future studies can therefore triangulate our findings with other forms of crimes (e.g. hacking, cyberbullying, child pornography) using the dimensions established in this study. Secondly, while some of our respondents include law enforcement agencies, our study did not entirely focus on combative measures in combatting cybercrime in Ghana. Future studies should consider venturing into countries' readiness in efforts to combat crimes.

REFERENCES

Albrecht, W. S., Wernz, G. W., and Williams, T. L. 1995. *Fraud: Bringing Light to the Dark Side of Business*, Irwin Professional Pub.

Anand, V., Ashforth, B. E., and Joshi, M. 2004. “Business as Usual: The Acceptance and Perpetuation of Corruption in Organizations,” *Academy of Management Perspectives* (18:2), Academy of Management Briarcliff Manor, NY 10510, pp. 39–53.

Argote, L., McEvily, B., and Reagans, R. 2003. “Managing Knowledge in Organizations: An Integrative Framework and Review of Emerging Themes,” *Management Science* (49:4), Informs, pp. 571–582.

Barn, R., and Barn, B. 2016. *An Ontological Representation of a Taxonomy for Cybercrime*.

Bigné, E., Hernández, B., Ruiz, C., and Andreu, L. 2010. “How Motivation, Opportunity and Ability Can Drive Online Airline Ticket Purchases,” *Journal of Air Transport Management* (16:6), Elsevier, pp. 346–349.

Blumberg, M., and Pringle, C. D. 1982. “The Missing Opportunity in Organizational Research: Some Implications for a Theory of Work Performance,” *Academy of Management Review* (7:4), Academy of Management Briarcliff Manor, NY 10510, pp. 560–569.

Buchanan, T., and Whitty, M. T. 2014. “The Online Dating Romance Scam: Causes and Consequences of Victimhood,” *Psychology, Crime & Law* (20:3), Taylor & Francis, pp. 261–283.

Budd, C., and Anderson, J. 2011. *Consumer Fraud in Australasia: Results of the Australasian Consumer*

Fraud Taskforce Online Australia Surveys 2008 and 2009, Australian Institute of Criminology.

Choo, F., and Tan, K. 2007. "An 'American Dream' Theory of Corporate Executive Fraud," *Accounting Forum* (31:2), pp. 203–215. (https://doi.org/10.1016/j.accfor.2006.12.004).

Clark, B. H., Abela, A. V, and Ambler, T. 2005. "Organizational Motivation, Opportunity and Ability to Measure Marketing Performance," *Journal of Strategic Marketing* (13:4), Taylor & Francis, pp. 241–259.

Clough, J. 2010. *Principles of Cybercrime*, Cambridge University Press, Cambridge.

CNN. 2019. "Americans Lost $143 Million in Online Romance Scams Last Year. That's Way More than Any Other Reported Fraud." (https://edition.cnn.com/2019/08/23/us/online-romance-scams-losses-trnd/index.html, accessed January 12, 2020).

Coenen, T. L. 2008. *Essentials of Corporate Fraud*, (Vol. 37), John Wiley & Sons.

Cressey, D. R. 1950. "The Criminal Violation of Financial Trust," *American Sociological Review* (15:6), JSTOR, pp. 738–743.

Cross, C., Dragiewicz, M., and Richards, K. 2018. "Understanding Romance Fraud: Insights from Domestic Violence Research," *The British Journal of Criminology* (58:6), Oxford University Press UK, pp. 1303–1322.

Dellaportas, S. 2013. "Conversations with Inmate Accountants: Motivation, Opportunity and the Fraud Triangle," *Accounting Fórum* (37:1), Taylor & Francis, pp. 29–39.

Donalds, C., and Osei-Bryson, K.-M. 2019. "Toward a Cybercrime Classification Ontology: A Knowledge-Based Approach," *Computers in Human Behavior* (92), Elsevier, pp. 403–418.

Fadel, K. J., and Durcikova, A. 2014. "Enhancing the Motivation, Opportunity, and Ability of Knowledge Workers to Participate in Knowledge Exchange," in *2014 47th Hawaii International Conference on System Sciences*, IEEE, pp. 3605–3614.

Gruen, T. W., Osmonbekov, T., and Czaplewski, A. J. 2005. "How E-Communities Extend the Concept of Exchange in Marketing: An Application of the Motivation, Opportunity, Ability (MOA) Theory," *Marketing Theory* (5:1), Sage Publications Sage CA: Thousand Oaks, CA, pp. 33–49.

Harrison, A. 2018. "The Effects of Media Capabilities on the Rationalization of Online Consumer Fraud," *Journal of the Association for Information Systems* (19:5), p. 1.

Huang, J., Stringhini, G., and 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*, Springer, pp. 216–236.

Hung, K., and Petrick, J. F. 2012. "Testing the Effects of Congruity, Travel Constraints, and Self-Efficacy on Travel Intentions: An Alternative Decision-Making Model," *Tourism Management* (33:4), Elsevier, pp. 855–867. (https://doi.org/10.1016/j.tourman.2011.09.007).

Hunton, P. 2012. "Data Attack of the Cybercriminal: Investigating the Digital Currency of Cybercrime," *Computer Law & Security Review* (28:2), Elsevier, pp. 201–207.

Jong, K. 2019. *Detecting the Online Romance Scam: Recognising Images Used in Fraudulent Dating Profiles*, University of Twente.

Kassem, R., and Higson, A. 2012. "The New Fraud Triangle Model," *Journal of Emerging Trends in Economics and Management Sciences* (3:3), Scholarlink Research Institute, pp. 191–195.

Kopp, C., Layton, R., Sillitoe, J., and Gondal, I. 2015. "The Role of Love Stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles.," *International Journal of Cyber Criminology* (9:2).

Lickiewicz, J. 2011. "Cyber Crime Psychology-Proposal of an Offender Psychological Profile," *Problems of Forensic Sciences* (2:3), pp. 239–252.

Longe, O., Ngwa, O., Wada, F., Mbarika, V., and Kvasny, L. 2009. "Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives," *Journal of Information Technology Impact* (9:3), pp. 155–172.

Luu, V., Land, L., and Chin, W. 2017. *Safeguarding Against Romance Scams–Using Protection Motivation Theory.*

MacInnis, D. J., and Jaworski, B. J. 1989. "Information Processing from Advertisements: Toward an Integrative Framework," *Journal of Marketing* (53:4), SAGE Publications Sage CA: Los Angeles, CA, pp. 1–23.

Maclnnis, D. J., Moorman, C., and Jaworski, B. J. 1991. "Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads," *Journal of Marketing* (55:4), SAGE Publications Sage CA: Los Angeles, CA, pp. 32–53.

Maslow, A. H. 1981. *Motivation and Personality*, Prabhat Prakashan.

Miles, M. B., and Huberman, A. M. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*, sage.

Mui, G., and Mailley, J. 2015. “A Tale of Two Triangles: Comparing the Fraud Triangle with Criminology’s Crime Triangle,” *Accounting Research Journal* (28:1), Emerald Group Publishing Limited, pp. 45–58.

Murphy, P. R., and Dacin, M. T. 2011. “Psychological Pathways to Fraud: Understanding and Preventing Fraud in Organizations,” *Journal of Business Ethics* (101:4), Springer, pp. 601–618.

Ngafeeson, M. 2010. “Cybercrime Classification: A Motivational Model,” *College of Business Administration, The University of Texas-Pan American* (1201).

Olayemi, O. J. 2014. “A Socio-Technological Analysis of Cybercrime and Cyber Security in Nigeria,” *International Journal of Sociology and Anthropology* (6:3), Academic Journals, p. 116.

Parra-López, E., Gutiérrez-Taño, D., Diaz-Armas, R. J., and Bulchand-Gidumal, J. 2012. “Travellers 2.0: Motivation, Opportunity and Ability to Use Social Media,” *Social Media in Travel, Tourism and Hospitality: Theory, Practice and Cases*, Ashgate Publication.

Peterson, B. K., and Gibson, T. H. 2003. “Student Health Services: A Case of Employee Fraud,” *Journal of Accounting Education* (21:1), Elsevier, pp. 61–73.

Ramamoorti, S. 2008. “The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component into Fraud and Forensic Accounting Curricula,” *Issues in Accounting Education* (23:4), pp. 521–533.

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).

Ryan, R. M., and Deci, E. L. 2000. “Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions,” *Contemporary Educational Psychology* (25:1), Elsevier, pp. 54–67.

Said, J., Alam, M. M., Ramli, M., and Rafidi, M. 2017. “Integrating Ethical Values into Fraud Triangle Theory in Assessing Employee Fraud: Evidence from the Malaysian Banking Industry,” *Journal of International Studies* (10:2), pp. 170–184.

Siemsen, E., Roth, A. V, and Balasubramanian, S. 2008. “How Motivation, Opportunity, and Ability Drive Knowledge Sharing: The Constraining-Factor Model,” *Journal of Operations Management* (26:3), Elsevier, pp. 426–445.

Sorell, T., and Whitty, M. 2019. “Online Romance Scams and Victimhood,” *Security Journal* (32:3), Springer, pp. 342–361.

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., and Whitty, M. 2019. “Automatically Dismantling Online Dating Fraud,” *IEEE Transactions on Information Forensics and Security* (15), IEEE, pp. 1128–1137.

Tade, O. 2013. “A Spiritual Dimension to Cybercrime in Nigeria: The ‘Yahoo plus’ Phenomenon,” *Human Affairs* (23:4), Versita, pp. 689–705.

Wada, F., Longe, O., and Danquah, P. 2012. “Action Speaks Louder than Words-Understanding Cyber Criminal Behavior Using Criminological Theories,” *The Journal of Internet Banking and Commerce* (17:1), Research and Reviews, pp. 1–12.

Whitty, M. T. 2013. “Anatomy of the Online Dating Romance Scam,” *Security Journal* (28:4), Springer, pp. 443–455.

Whitty, M. T. 2018. “419-It’s Just a Game: Pathways to Cyber-Fraud Criminality Emanating from West Africa.,” *International Journal of Cyber Criminology*.

Whitty, M. T. 2019. “Who Can Spot an Online Romance Scam?,” *Journal of Financial Crime* (just-accepted), Emerald Publishing Limited, p. 0.

Whitty, M. T., and Buchanan, T. 2012. “The Online Romance Scam: A Serious Cybercrime,” *CyberPsychology, Behavior, and Social Networking* (15:3), Mary Ann Liebert, Inc. 140 Huguenot Street, 3rd Floor New Rochelle, NY 10801 USA, pp. 181–183.

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), Sage Publications Sage UK: London, England, pp. 176–194.

Wu, Y., Balasubramanian, S., and Mahajan, V. 2004. “When Is a Preannounced New Product Likely to Be Delayed?,” *Journal of Marketing* (68:2), SAGE Publications Sage CA: Los Angeles, CA, pp. 101–113.