

# The client's consent strengthens the 'Gamers' hand; The deterrence theory's perspective of the Internet romance fraudsters.

Martin Otu Offei<sup>1</sup>, Lomatey Toku<sup>1</sup>

Koforidua Technical University, Koforidua, Ghana. **Correspondence**: <u>lomatey.isaactoku@ktu.edu.gh</u>

# Abstract

Internet romance fraud (IRF) is an international crime which has great consequences for individuals, businesses and nations. This emerging crime is based on a romantic love relationship over the internet between a victim (with love intention) and an offender with a criminal intention. Offenders recruit victims from dating sites with the sole intention of defrauding these victims by deception. This study surveyed 320 respondents from validated internet romance fraud (IRF) hotspots which includes, internet cafés and university campuses in Ghana. Structural equation modelling (SEM), with partial least square (PLS) was use to model and analyze the casual relationships of the dependent and independent variables. The evidence from this study suggests, deterrence dimensions of punishment (certainty, severity) and shame (certainty severity) negatively influence intention to commit internet romance fraud (IRF) however, intention to commit internet romance fraud (IRF) positively influence the actual IRF crime. Whereas, punishment dimensions are negative and significant ( $\beta$ =-0.201, t- value =2.380, p- value>0.000:  $\beta$ =-0.424, t-value =7.016, pvalue>0.000), shame dimensions are negative and insignificant ( $\beta = -0.037$ , t-value = 1.008, p-value >0.000;  $\beta$  =-0.047, t-value =0.959,p-value >0.000), implying IRF are not ashamed in their quest to defraud their victims. Internet romance fraudsters are not deterred by any form of punishment by the law enforcement and or shame to defraud their victims, although they know their acts are criminal in nature and punishable by law. Offenders' criminal intention ensures that victims are ultimately defrauded under the pretense of romantic love relationship. This emboldens attitude of internet romance offenders must inform law enforcement and prosecutions. Maybe the punishment meted to IRF criminals are not deterrent enough, to IRF criminals and encouraging more young persons to participate in internet romance fraud (IRF) activities.

Keywords: deterrence, punishment and shame (certainty, severity), internet romance fraud

# 1.0 Introduction and background

Internet romance is online dating which involves a male or female looking for love with an opposite or same sex partner. The fraud where the offenders take advantage of their victims' genuine quest for romantic relationship to deceive their victims through false pretense, impersonation, counterfeiting, forgery and other fraudulent representation of facts (Ibrahim 2016). Internet romance fraudsters are not deterred by punishment or shame. They are not deterred, because the reward they accrue from this crime is far greater than the sanctions associated with their deviant behavior. Internet romance fraud activities are global in nature. Generally, deterrence prevents future crime occurrence but it is

context specific. Internet romance fraud crime spans continents and is increasing at an alarming rate in both developing and developed countries which often bear the brunt of this self-indulging crime. The nature of this crime involves a well-motivated offender who mostly live in a developing country with a naïve online victim who resides in a developed economy. In the African context where poverty is prevalent the incidence of crime in general is quite high (Heller, 2011) and by extension internet romance fraud relatively high (Barnor et. al., 2021). Offenders involve in internet romance fraud activities go on the internet, on an online recruitment spree from dating sites (match. com, pof.com, okcuip.com, etc.) with the sole aim of recruiting online lovers who are not aware of the criminal intent of the offender. The victims of internet romance fraud, are referred to as "clients' by their offenders' partners. Offenders take their clients on a love journey from a dating site to a more personalize social media platform site like WhatsApp etc. to continue with the love journey with the intention to defraud the client.

These offenders create an atmosphere of love on the internet with their partners who are made to believe their online offenders. These internet romance fraudsters have a pre-prepared template of a conversation pattern that has been tried and tested with other victims over time, the pre-prepared template offenders call 'format' (Offei, et al., 2020). Many victims have fallen prey to these criminals who use different formats for different victims. On the dating platform the offenders' profile their clients by informing themselves adequately, i.e., where they work, their salary and wages profile, whether they have mortgage and the type of mortgage, where they live etc. With all this information and more from the conversation that ensues between victims and their offenders, the offenders are weaponized with this information which forms the basis of their plan of action to be taken subsequently. These offenders are not in any way deterred by their criminal activities and the carry it out in the dark and mostly at internet cafés. The openly display their worth without fear of law enforcement agencies. Fear of shame and punishment does not deter the offenders of internet romance fraudsters. What the offenders intend to gain from their criminal activities far outweighs their perceived shame and punishment.

## 2.0 Research Model

This study focuses on internet romance fraudsters disposition to deterrence to fraud intention and subsequently actualizing the fraud intention. The paper seeks to investigate how these offenders appreciate deterrence in the quest to defraud their victims. We explore and explain two dimensions of deterrence, shame and punishment and show whether these will influence the criminal intention of the internet romance fraudster and whether the criminal intention drives the offender to commit the crime against their clients.

These dimensions of deterrence have been chosen because of the contradiction that exit in findings in other study context.

## 2.1 Deterrence theory

The deterrence theory has three distinctive constructs from different studies in information systems and criminology literature. We identify them as; shame, punishment (sanction) and celerity (Trang and Brendel, 2019). Shame and punishment have two sub constructs each, severity and certainty. For the purpose of this study we use shame and punishment and their two dimensions. Celerity as a construct was not fit for the purpose of this study as nature of internet romance fraud, crime require a lot more time to have a conviction.

## 2.2 Deterrence Theory

For the purposes of this study, shame certainty, shame severity, punishment certainty and punishment severity will be used as the deterrence constructs in the context of internet romance fraud.

Table 1. Summary of deterrence theory and the context used

Source	Criminal / malicious context?	Participants	DV type	Other theories / constructs	Method	Findings / application to DT	
Barlow et al. (2013) (ISI)	No (IT policy violation intention)	Employees	Scenarios (negative)	Neutralization theory	Factorial Survey	Focused on "communication of deterrent sanctions" as one overall deterrent theory (DT)-related construct. Showed this construct and some neutralization constructs lowered intentions to violate IT policies.	
Bulgurcu et al. (2010) (ISI)	No (ISP compliance intention)	Employees	Intentions (positive)	RCT and TPB	Cross- sectional Survey	Study was not a true DT study, but is often miscited as such. It was primarily based on Rational Choice Theory and Theory of Planned Behavior (RCT and TPB. However, they showed that sanctions had a positive relationship with cost of noncompliance, which predicted compliance attitude, and then intentions.	
Chen et al. (2014) (ISI)	No (ISP compliance intention)	Employees	Scenarios (positive)	Reward, security training, monitoring, training, policy	Factorial Survey	In addition to severity and certainty, they added reward. All were shown to positively influence compliance intentions.	
Cheng et al. (2014) (ISI)	No (ISP violation intention)	Employees	Scenarios (negative)	Social control (social bonds and pressure)	Factorial Survey	Added several sub constructs of social bonds and social pressure to certainty and severity. Certainty was insignificant; severity was significant. Several of the social control constructs were significant.	
Chuma (2012) (thesis)	No (noncompliant, nonmalicious security behavior)	Employees at one company	Behaviors (negative)	Self-control theory, social bonding	Cross- sectional Survey	Used certainty, severity, and celerity. Severity was insignificant whereas certainty and celerity were significant. Dealt with nonmalicious noncompliance behaviors such as write down password, share password, not verifying sending of email, opening email attachments without knowing.	
D'Arcy & Devaraj (2012) (ISI)	Partial (IS misuse intentions; not strong criminal intent)	Employees, including part-time MBA students	Scenarios (negative)	Informal sanctions as DT extension	Factorial Survey	Examined formal sanctions (combined severity/certainty) and added informal sanctions (social desirability and moral beliefs). All three were significant. All participants were given four scenarios and all measures were averaged from the four scenarios and analyzed together.	
D'Arcy & Hovav (2007) (ISI)	Partial (IS misuse intentions; not strong criminal intent)	Employees, including part-time MBA	Intentions (negative)	n/a	Factorial Survey	Did not directly use DT constructs, but argued that ISPs, System Engineering and Technical Assistance (SETA) programs, monitoring, and preventive security software are deterrence surrogates that reduce IS misuse intentions. All were significant except computer monitoring.	

 $58 \ {\odot}\ 2023$  International Journal of Technology and Management Research ISSN 2026-6480

students	

## 2.1.1 Shame certainty

Shame certainty refers to the sense of feeling guilty of a deviant behavior that is not socially unacceptable by society. Shame is normally used in information systems environment to deter deviate behaviour (Siponen and Willison, 2012). When shame is certain then then we would expect that deviant behaviour will be minimized. Name and shame are a deterrent tool used to prevent unacceptable behaviour. When deviants know that they will be named and shamed it will prevent them from committing the offenses they intend to commit. Where pictures of deviants are openly displayed for all to see will certainly deter offenders of deviant behaviour, however among internet romance fraudster that is not the case, they are not deterred. We therefore, hypothesized that,

## H1a: Shame certainty negatively influence internet romance fraud intention

Shame severity is the how punitive the embarrassment the offender receives. Shame which is selfimpose or sometimes administered by a body has been studied in criminology using rational choice theories to appreciate how it influence the deterrence argument (Willison et. al., 2018). Shame can be severe if it serves the intended purpose and the gravity of shame is unbearable within the circles of deviant. In the context of the internet romance fraudsters, they are not deterred by the severity of shame. They flout their wealth openly and are well connected to some law enforcement officers, thereby emboldened to continue their deviant activities. We, therefore hypothesized that,

H1b: Shame severity negatively influence internet romance fraud intention

## **Punishment certainty**

Formal punishment is normally enshrined in laws. They are punitive and formal. Sanctions stipulating clearly what and how the offender should be dealt with. The more certain an offender will be punished for a deviant behaviour, the effective of the punishment will guarantee the needed results. Certainty of punishment determine how significant the sanction is will be (D'Arcy et al., 2014). In the context of internet romance fraudsters, punishment does not deter them from the activities. Although they know what they do is a crime, they are not deterred in any way. We therefore hypothesized that;

## H2a: Punishment certainty negatively influence internet romance fraud intention

## **Punishment severity**

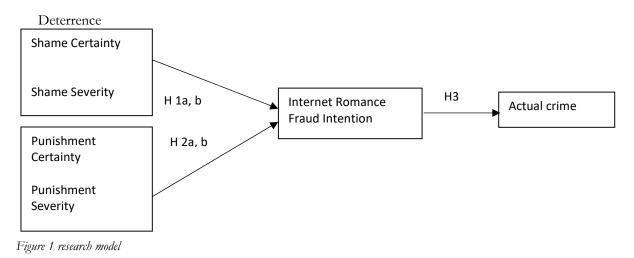
Scholars have argued that the deterrent effects of severe punishment can be strong —in some studies, even a single execution produced a statistically significant reduction in homicide rates (Dezhbakhsh and Shepherd 2006). Severity and certainty are important factors that determine the effectiveness of a sanction. (D'Arcy et al., 2014) found that the severity of formal sanctions had a significant negative effect on users' intentions to commit computer abuse. In the context of internet romance fraud offenders are not deterred by the severity of the punishment since they perceive they could come back from the punishment to enjoy their booty. We therefore hypothesized that;

## H2a: Punishment severity negatively influence internet romance fraud intention

Criminal intention of a deviant may not necessarily lead to the committal of the offence. This is because intention can change at any time during the criminal decision-making process. So not every criminal intention is carried out to the fullest as intended. However, the perceived reward from the offence (Próspero-Luis et al., 2017), positively influence the criminal intention of an offender. Offenders hide their nonverbal criminal intention (Koller et al., 2015) among crowds. The internet romance fraudsters hide their criminal intention from their victims. They go into online relationships with clear intention to deceive their victims but this intention is not known and hidden (nonverbal) (Koller et al., 2016) to their victims. We therefore hypothesized that;

H3: Intention to commit internet romance fraud positively influence the actual crime

#### Research Model



#### 3.0 Methodology

## 3.1 Context of the study

The targeted population is of internet romance fraudsters who understand what they do and have known their victims over a period of time. These offenders are called "gamers" and they are often young persons who are above 16 years of age. The offenders called their victims as "clients". By seeing their victims as 'clients' the offenders are not ashamed to deal with them nor are they ashamed to be caught. The offenders are not deterred by future punishment as a result their fraudulent activities. Due to anonymous nature of the internet and how private these online love relationships of their activities are, snowball and convenience sampling techniques were combined as internet hotspots were the main target areas. The internet cafes are public places where individual have private booths where they practice their trade, because the internet café constitute the recruiting place for both new gamer entrants and the workshop to practice fraud activities. These internet cafés are validated internet romance fraud activity grounds (Whitty, 2018, Barnor et al., 2020). Table 1 represents the descriptive statistics for the gamers

## 3.2 Measurement and instrumentation

A 5-point Likert-type scale was used as a measurement tool to elicit responses from the gamers. The subconstructs of deterrence adapted for this study are shame and punishment. Shame and punishment have two sub-constructs. This study used second order reflective constructs of shame certainty, shame severity, punishment certainty and punishment severity as deterrence dimensions. The mediating effect of fraud intention to actual defraud represent the final phase of this study. The internet romance fraud intention is measured by three sub constructs, they include; 'format', deception and intention to defraud. The actual defraud was measured by one construct i.e., crime (extortion of money from clients). Content validity was ensured through two times meeting of three hours each with eighteen (18) practitioners of internet romance fraudsters and two information systems experts to validate these contracts. Furthermore, to ensure construct validity a pilot sample study was conducted as a second face of validity and the measurement instrument

## 61 © 2023 International Journal of Technology and Management Research ISSN 2026-6480

revise to improve the quality of constructs. The instruments that represent the final survey is represented in the table 2

## 3.3 Collection of Data

The study sample data includes responses from different internet café hotspot which are the main areas within which internet romance fraud takes place. Data was elicited by referrals of internet romance fraudsters who are aware of their associate's involvement in internet romance fraud activities.

The secrecy and anonymity of internet romance fraud make it difficult to know the population of internet romance fraudsters. The sample technique used was convenient, three hundred and fifty (350) questionnaires were administered to internet romance fraudsters hotspots and also the referrals of internet romance fraudsters. A total of three hundred and twenty (320) response were received from the respondents which represents 91% of respondents' rate. Most of the respondents are between the ages of 18-40 years and the average age of these respondents is at least senior high school student. The table 2 below represents the demographic representation of the respondents in this study.

## 4.0 Results and Discussions

## 4.1 Data analysis and results

Reviews from both criminology and information systems literature suggest contradiction in the findings from different crime contexts (Nagin and Snodgrass 2013; Chen et al., 2014; Paternoster 2010). The theoretical model of the study is based on two victim precipitation dimensions of deterrence (shame and punishment) with their sub constructs of certainty and severity. Those constructs are mediated by fraud intention to the actual defraud which is the dependent variable. This model is an explanatory in nature of these constructs as studied in the context of internet romance fraud. Covariance-based structural model was used to confirm these dimensions of deterrence, fraud intention and actual defraud. Theoretically, the findings of this study can help predict future accuracy of this model. A structural model assessment was done by using SmartPLS.

## 4.2 Measurement Model Validation

To ascertain model measurements of validity, reliability and common method-biased co-variance SEM was employed with SmartPLS software to ensure psychometric properties were properly analyzed. Construct validity was examined by using the measurements of convergent and discriminant validity, these two measurements represent Confirmatory factor analysis (CFA). The following results of the model measurement represents a rigorous psychometric property. Construct reliability (CR), Cronbach alpha (CA), Average variance extracted (AVE) and rho A. The reliability of variables under study can also be assessed by using convergent validity; variable reliability, average variance extracted (AVE) and performing factor analysis (Fornell and Larcker 1981). In ensuring that this measure is reliable the loading of variables or construct whose loading are insignificant are removed to ensure that construct understudy is adequately represented by the measures and the cross loading of constructs were noted to be insignificant. The table 2 is the composite reliability construct understudy. Shame certainty (DetSc = 0.924), shame severity (DetSs =0.954), punishment certainty (DetPc=0.886), punishment severity (DetPs =0.804), Internet romance fraud intention (ICIRF =0.861) and Actual defraud (ADF=0.797), the AVE for the constructs ranges from (0.510-.0.873) meeting the threshold value of 0.5 and above (Hair et. al., 1995). The table below shows all the construct reliability values from the analysis of the data from the study. The rho\_A values rages from (0.767-0.928) reinforcing construct reliability.

Constructs	CR	AVE	<b>R</b> <sup>2</sup>	CA	rho_A
ADF	0.797	0.510	0.610	0.612	0.881
DetSc	0.924	0.803	0.715	0.877	0.814
DetSs	0.954	0.873	0.534	0.927	0.928
DetPc	0.886	0.721	0.542	0.807	0.893
DetPs	0.804	0.584	0.300	0.706	0.878
IcifDp	0.868	0.569	0.712	0.807	0.767
IcifFm	0.849	0.531	0.331	0.789	0.793
Icirf	0.861	0.541	0.301	0.767	0.780
IcifId	0.866	0.684	0.356	0.766	0.809

Table 3 Constructs validity HTMT, Fornell Lacker results

Constructs	CR	AVE	ADF	DetSc	DetSs	DetPc	DetSp	IcifDp	IcifFm	IcifId
ADF	0.767	0.62	0.7887							
DetSc	0.924	0.803	-0.019	0.870						
DetSs	0.954	0.873	0.100	0.497	0.934					
DetPc	0.886	0.721	0.098	0008	0.009	0.849				
DetSp	0.804	0.584	0.036	0.372	0.007	0.208	0.764			
IcifDp	0.868	0.569	0.141	0.018	0.134	0.056	0.099	0.755		
IcifFm	0.849	0.531	0.059	0.016	0.001	0.005	0.003	0.210	0.728	
IcifId	0.866	0.684	0.109	0.024	0.03	0.03	0.037	0.272	0.135	0.827

ADF-Actual defraud, DetSc-Deterrence shame certainty, DetSs-Deterrence shame severity, DetPc-Deterrence punishment certainty, DetPs-Deterrence punishment severity, IcifDp-Intention to commit internet fraud (Deception), IcifFm-Intention to commit internet fraud (format), IcifDp-Intention to commit internet fraud (Intention to defraud)

Table 4 Model results

Hypotheses	<b>Deterrence Dimensions</b>	<b>R</b> <sup>2</sup>	ß	<b>T-values</b>	<b>P-values</b>	Support?
H1a	DetPc>>ICIRF	0.361	-0.201	2.380	0.000	Supported
H1b	DetPs>>ICIRF	0.693	-0.424	7.016	0.000	Supported
H2a	DetSc>>ICIRF	0.566	-0.037	1.008	0.000	Not
						Supported
H2b	DetSs>>ICIRF	0.168	-0.047	0.959	0.000	Not
						Supported
Hypothesis	Fraud Intention	<b>R</b> <sup>2</sup>		T-value	P-value	Support?
Н3	ICIRF>>ADF	0.330	0.300	3.934	0.000	Supported

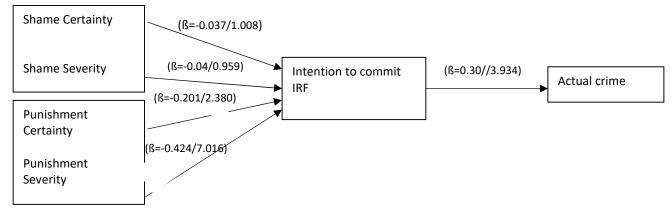


Figure 2 model results showing Second order significant paths (T-values)

# 5.0 Results, Analysis and Discussions

The Structural Equation Modeling (SEM) was used to investigate the causal paths hypothesized in this study. A two-step approach was used to analyze the data. In the first step, the covariance-based technique was used to assess the appropriateness of the measurement model. The covariance-based technique was used as it minimizes the differences between the covariance of the collected sample and that of the ones predicted by the model and reproduces the covariance matrix of the observable variable. Foresting the structural model, variance based partial least square (PLS) SEM was used as it maximizes the variance of the dependent variable which is explained by the independent variables.

We used the Cronbach Alpha, Composite Reliability and Average Variance Extracted (AVE) to test for reliability and validity of the constructs. Discriminant validity tests were performed to test for accuracy of the measurement items by using Furnell Lecker Criterion and Heterotrait-Monotrait (HTMT). A HTMT is a more resilient test for discriminant validity than cross loadings. As shown in Table 3, constructs reliability is confirmed as composite reliability (CR) values for all factors were above the recommended 0.7 value threshold, indicating item consistency. The variance explained (AVE) is above the satisfactory threshold of 0.5, confirming convergent validity.

The findings of this research are shown in Table 4 and figure 2. From this study, the findings suggest internet romance fraud offenders are not deterred either by shame or punishment. They also carry out their criminal intent to defraud victims through. Victims are actually defrauded by offenders because their intent to defraud is what drives them into internet romance fraud activities. However, from previous studies punishment have an overall positive effect on deviant behavior (Trang and Brendel, 2019; Johnston et al. 2015).

Punishment certainty – the evidence from this suggest that internet romance fraudsters are not deterred by punishment certainty (( $\beta$ =0.201, t-value = 2.230, p<000). Punishment certainty is the guarantee that a crime will definitely be sanctioned and research has proven that it is much more effective than the severity of the punishment (Paternoster and Simpson, 1996; Hollinger and Clark, 1983). There are contradictions with punishment certainty in different context. Punishment certainty decreases in information misuse intentions (D'Arcy et al., 2009) but was significant in ISP compliance intention (Herath and Rao, 2009) and was not supported (Cheng et al., 2013) in ISP violation intention. Punishment certainty, in IS security environment is supported (Kuo et al., 2020; Trang, 2018;). The evidence suggests that punishment certainty is context specific. This is because the evidence varies with the crime context.

Punishment severity – punishment severity is generally thought of as a deterrent to criminal behavior (Antunes and Hunt, 1973; Kelli, 2016) but the evidence contradicts this assertion, from this study, internet romance fraudsters are not deterred by punishment severity ( $\beta$ =0.424, t-value = 7.016, p <0.000). The evidence from this study is supported by crimes in the context of "rape, assault, larceny, robbery, burglary, and auto theft" (Antunes and Hunt, 1973; p.5). However, in homicides severity of punishment deters deviant behavior (Antunes and Hunt, 1973; Dezhbakhsh and Shepherd 2006). The context subjectivity is evident in

the various studies conducted in different environments (Trang and Brendel, 2019). Formal sanctions had no significant effect on intention to commit software piracy

Second, the fact that our results suggest that certainty and severity of shame have a significant deterrent effect on software piracy opens up an avenue for campaigns and education strategies that stress the likelihood and severity of shame. Fig. 2 research model show results of PLS analysis. Note: N.S., non-significant; \*p < 0.10; \*\*p < 0.01. M. Siponen et al. / Information & Management 49 (2012) 334–341 337 anti-piracy organizations need to make a justified and convincing case that software piracy is not morally acceptable.

Shame certainty – Although shame is self-inflicted, it severs as a significant deterrence element in the deterrence literature. In this study shame certainty does not deter internet romance fraudsters from their intention to defraud victims ( $\beta$ =-0.037, t-value=1.008, p<000). Shame certainty significantly deter software piracy (Siponen et al., 2012). Several studies in rational choice criminology have used shame to mitigate deviant behaviour (Moody et al., 2018; Siponen and Vance, 2010; Paternoster and Simpson, 1996).

Shame severity -Shame severity significantly deter software piracy (Siponen et al., 2012) but the evidence from this study contradicts this claim because internet romance fraudsters are not deterred by the severity of shame ( $\beta$ =-0.040, t-vale =0.959, p<000). Internet romance offenders openly display their ill-gotten wealth without bothering about their apprehension by the security agencies. Brushes with the law and prison does not deter them because they know their victims are far away in develop countries and the evidence to prosecute them may not be available to law enforcement agencies. Some offenders also have close links with the security apparatus to help them to escape punishment should they be caught. This is evident in (Tade and Aliyu, 2011, p. 871), "Indeed, the nation has been described as chaotic, where order is scarified and shame no longer". Further evidence of police collaboration "Unfortunately most of the police officer knows some of this yahoo boys as well as the politicians. But, since most of them are highly placed, they usually go away unpunished." (Akanle et al., 2016, p. 219). This kind of collaboration does not make internet romance fraudster shameful of their activities because they know they have their backs covered.

Misbehavior intention may not always be carried out as the intention get conceived can be aborted later without execution. The evidence from this study suggests otherwise, internet romance fraudsters carry their criminal intention through to deceive and defraud their victims ( $\beta$ =0.153, t-value =2.813, p<000). According to Morton and Koufteros (2008), attitude influence intentions to commit online music piracy. In the case of the internet romance fraudster the 'get rich early' attitude drives their intention to defraud victims who have no idea of the criminal intention of their online fraud partners. Offenders' intention is clear from the beginning of the relationship they seek to develop with their online partners. They are driven by this intention until they finally succeed in defrauding their victims. This is collaborated by a study done in Nigeria of internet romance fraudsters. This is what one of the offenders had to say (Akanle et al., 2016, p. 215) "This is done with an intention to dupe others". Further evidence suggests confirms the findings of this study, "This entails feigning undying love towards a person with the true intention of committing fraud" (Ibitayo et al., 2021, p. 24). Offenders are driven by fraudulent intention to commit crime against the victims they have recruited as lovers for that purpose.

## 6.0 Implication of the study

This study has many implications for law enforcement, businesses, owners and operators of dating sites, governments and person looking for love online. For law enforcement, internet romance fraud is a new complex online crime fraud which requires the attention of prosecutors. The alarming nature of this crime makes it difficult for law enforcement to keep pace with it. There is the need to train law enforcement officers to be able to detect, arrest and have a successful prosecution. By swiftly dealing with this type of emerging crime may help deter its frequent occurrences. The empirical evidence from this study suggest that internet romance fraudsters are not deterred by shame or punishment. This should inform law enforcement agencies and legislators. Offenders also carry out their criminal intent by ultimately defrauding victims.

The booty from this crime is finding its way into legitimate businesses in many countries within the subregion. Money laundering is a serious crime which when uncheck will finance other criminal activities like terrorism, war, piracy, drugs, prostitution etc. Businesses should be careful how they get financial injection into their businesses. The sources of these funding should be authenticated at all times to ensure that illegitimate money does not find its way into legitimate businesses.

Online dating platform owners have to educate and constantly update themselves with research in this area to adequately inform the user of their platforms about current development to mitigate internet romance fraud. The frequency of this crime requires constant interface with the needed information to guard against fraudulent activities. The users of these sites should also acquaint themselves with the requisite information to minimize and eliminate this crime. Online daters will have to take personal responsibility by fact checking images and authenticate information they share with their lovers online.

The incidence of internet romance fraud is becoming one too many and we need to do all we can to protect vulnerable online daters from the fraud offenders seek to perpetuate against victim. Crime reduction is a collective responsibility and society will have to be serious about this crime.

#### References

Akanle, O., Adesina, J.O. and Akarah, E.P., 2016. Towards human dignity and the internet: The cybercrime (yahoo) yahoo) phenomenon in Nigeria. African Journal of Science, Technology, Innovation and Development, 8(2), pp.213-220.

Antunes, G. and Hunt, A.L., 1973. The impact of certainty and severity of punishment on levels of crime in American states: An extended analysis. *The Journal of Criminal Law and Criminology (1973-)*, 64(4), pp.486-493.

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.

Barnor, J.N.B., Boateng, R., Kolog, E.A. and Afful-Dadzie, A., 2020. Rationalizing Online Romance Fraud: In the Eyes of the Offender.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, pp.523-548.

Chen, H., Hailey, D., Wang, N. and Yu, P., 2014. A review of data quality assessment methods for public health information systems. *International journal of environmental research and public health*, *11*(5), pp.5170-5207.

Chuma, D.A., 2012. Customers' Attitude Towards Mobile Phone Advertising: A Case Study of Undergraduate Students of Sokoine University of Agriculture (SUA), Morogoro Campus, Tanzania (Doctoral dissertation, SAUT).

Cross, C., 2020. Romance fraud. The Palgrave Handbook of International Cybercrime and Cyber deviance, pp.917-937.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security, 22(5), 474–489. <u>https://doi.org/10.1108/IMCS-08-2013-0057</u>.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643–658. <u>https://doi.org/10.1057/ejis.2011.23</u>.

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. Journal of Business Ethics, 89(SUPPL. 1), 59–71. https://doi.org/10.1007/ s10551-008-9909-7.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping Perspective. Journal of Management Information Systems, 31(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210.

D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160.

D'Arcy, J. and Devaraj, S., 2012. Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences*, 43(6), pp.1091-1124.

D'Arcy, J. and Hovav, A., 2007. Deterring internal information systems misuse. *Communications of the ACM*, 50(10), pp.113-117.

Dezhbakhsh, H. and Shepherd, J.M., 2006. The deterrent effect of capital punishment: Evidence from a "judicial experiment". *Economic Inquiry*, 44(3), pp.512-535.

Faluyi, B.I., Fele, T. and Ayeni, A.O., 2020. Impact of ICT-facilitated fraud on Sustainable Socio-economic Development in Nigeria.

Fornell, C. and Larcker, D.F., 1981. Structural equation models with unobservable variables and measurement error: Algebra and statistics.

George Antunes, A. Lee Hunt, Impact of Certainty and Severity of Punishment on Levels of Crime in American States: An Extended Analysis, The, 64 J. Crim. L. & Criminology 486 (1973). Heller, K.J., 2011. The Nuremberg military tribunals and the origins of international criminal law. Oxford University Press on Demand.

Herath, T. and Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, 18(2), pp.106-125.

Hollinger, R.C. and Clark, J.P., 1983. Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social forces*, 62(2), pp.398-418.

Ibitayo, A. and Beckmann, N.M., 2021. Imaging evaluation of traumatic carpal instability. *Emergency Radiology*, 28(2), pp.349-359.

Johnston, L.D., O'Malley, P.M., Bachman, J.G., Schulenberg, J.E. and Miech, R.A., 2015. Monitoring the Future national survey results on drug use, 1975-2014: Volume II, college students and adults ages 19-55.

Kelli D. Tomlinson, "An Examination of Deterrence Theory: Where Do We Stand?" Federal Probation 80, no. 3 (December 2016): 33-38.

Koller, C.I., Wetter, O.E. and Hofer, F., 2015. What is suspicious when trying to be inconspicuous? Criminal intentions inferred from nonverbal behavioral cues. *Perception*, 44(6), pp.679-708.

Koller, C.I., Wetter, O.E. and Hofer, F., 2016. 'Who's the Thief?'The Influence of knowledge and experience on early detection of criminal intentions. *Applied Cognitive Psychology*, *30*(2), pp.178-187.

Kuo, K.M., Talley, P.C. and Huang, C.H., 2020. A meta-analysis of the deterrence theory in security-compliant and security-risk behaviors. Computers & Security, 96, p.101928.

Moody, G.D., Siponen, M. and Pahnila, S., 2018. Toward a unified model of information security policy compliance. *MIS quarterly*, 42(1).

Morton, N.A. and Koufteros, X., 2008. Intention to commit online music piracy and its antecedents: An empirical investigation. *Structural Equation Modeling: A Multidisciplinary Journal*, 15(3), pp.491-512.

Nagin, D.S. and Snodgrass, G.M., 2013. The effect of incarceration on re-offending: Evidence from a natural experiment in Pennsylvania. *Journal of Quantitative Criminology*, 29(4), pp.601-642.

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

Paternoster, R. and Simpson, S., 1996. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, pp.549-583.

Paternoster, R., 2010. How much do we really know about criminal deterrence. J. crim. l. & criminology, 100, p.765.

Próspero-Luis, J., Moreira, P.S., Paiva, T.O., Teixeira, C.P., Costa, P. and Almeida, P.R., 2017.

Psychopathy, criminal intentions, and abnormal appraisal of the expected outcomes of theft. Legal and Criminological Psychology, 22(2), pp.314-331.

Siponen, M. and Vance, A., 2010. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, pp.487-502.

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.

Tade, O. and Aliyu, I., 2011. Social organization of Internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, 5(2).

Trang, S. and Brendel, B., 2019. A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, 21(6), pp.1265-1284.

Whitty, M.T., 2018. Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking*, 21(2), pp.105-109.

Willison, R., Lowry, P.B. and Paternoster, R., 2018. A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence in Inspiring New Directions in Behavioral and Organizational Security," Journal of the Association for Information Systems (JAIS), 19(12), pp.1187-1216.