Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria

Yetunde O. Ogunleye,[1] Usman A. Ojedokun[2] & Adeyinka A. Aderinto[3]
University of Ibadan, Nigeria

Abstract
Despite the enactment of the Nigerian Cybercrime Act in 2015, cyber fraud still remains largely pervasive among the youths, especially undergraduates. Against this background, this study examined the pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-west Nigeria. It adopted the exploratory cum cross-sectional research design. Social learning theory was employed as conceptual framework. Data were exclusively generated through in-depth interviews conducted with 17 female undergraduates selected using the snowball sampling technique. Results showed that female undergraduates got initiated into cyber fraud by their male relatives and associates. Financial gain and peer pressure were the major motivating factors for their involvement in the crime. Cyber fraud was seen by the students to be a source of income for meeting their own personal and relatives' financial needs. A multi-dimensional approach is suggested as a way of effectively dealing with this form of crime.

Keywords: Cyber fraud, Cybercrime, Female undergraduates, Nigerian Cybercrime Act 2015, Nigeria.

Introduction

The growing popularity of cyber fraud among Nigerian youths continues to be a major cause for concern for the Federal Government and other relevant stakeholders. Despite the enactment of the Nigerian Cybercrime Act in 2015, cyber fraud still remains largely pervasive among the youths, especially undergraduates. Although significant scholarly attention has been devoted to youths perpetrating cyber fraud in Nigeria, nonetheless,

[1] Department of Sociology, University of Ibadan, Ibadan, Nigeria.
E-Mail: ogunleyeyetundeolufunke@gmail.com
[2] Department of Sociology, University of Ibadan, Ibadan, Nigeria.
E-Mail: uaojedokun@gmail.com (Corresponding Author)
[3] Department of Sociology, University of Ibadan, Ibadan, Nigeria. E-Mail: aderinto@yahoo.com

most of these previous studies have essentially focused on male cyber fraudsters known in local parlance as the *yahoo boys* (Ojedokun & Eraye, 2012; Tade & Aliyu, 2011; Arowosaiye, 2008; Aghatise, 2006). Consequently, there is paucity of empirical information on the pathways, social organisation, motivations, and socioeconomic lifestyles of females involved in this form of criminality. Therefore, this present study was embarked upon for the purpose of filling this void.

Cyber fraud is the dominant and most popular form of cybercrime among undergraduates in Nigeria that is resulting into a huge economic and financial loss annually (Babatunde & Olanrewaju, 2015; Idehen, Ojewumi, & Olasupo, 2013; Okeshola & Adeta, 2013; Anyawnu, Oforegbu, Igbo & Obiyo, 2012; Amosun & Ige, 2009). The Nigerian Deposit Insurance Corporation's (NDIC) 2014 report indicated that cases of cyber frauds recorded on the Nigerian banking sector's e-payment platform between 2013 and 2014 increased by 183% (This Day, 2016). Similarly, the 2014 annual report of the Centre for Strategic and International Studies, UK estimated the annual cost of cybercrime in Nigeria to about 0.08% of the gross domestic product (GDP), representing about ₦127 billion (This Day, 2016). Indeed, the advancement in technology is increasingly transforming the nature, dimension, intensity and the magnitude of cyber fraud in Nigeria (Aderinto & Ojedokun, 2017; Tade & Aliyu, 2011; Adeniran, 2008).

Koong, Liu, and Wei (2006) view Internet (cyber) fraud as any type of fraudulent scheme that involves using one or more components of the Internet to perpetuate a crime. In their own submission, Tade and Aliyu (2011) articulate that the Internet is presenting a new opportunity for the development of another criminal sector of fraud. Similarly, Lee (2003) observes that the adoption of the Internet for commercial purposes is also facilitating the successful perpetration of fraudulent activities online. Smyth and Carleton (2011) assert that Internet fraud may occur under a wide a range of circumstances which may include the presentation of misleading or deceitful information online, failing to honour contractual agreements entered into online, or misappropriation of funds transmitted electronically. Equally, Dzomira (2014) submits that the growing patronage of e-banking services globally is contributing to the occurrence of financially motivated high-profile attacks. Levi and Burrows (2008) classified the two major victims of cyber fraud as primary victims and secondary victims. *Primary victims* are individuals and businesses or public bodies who initially suffer the harms of fraud, while *secondary victims* include financial institutions, insurance companies, and others who, by contract or regulation, agree to reimburse some or all of the costs to primary victims (Levi & Burrows, 2008).

Duffield and Grabosky (2001) divide cyber fraud into four major categories: (a) fraud committed against an organisation by a principal or senior official of that organisation; (b) fraud committed against an organisation by an "insider" or a "outsider" such as a client; (c) fraud committed by one individual against another in the context of face-to-face interaction; and (d) fraud committed against a number of individuals through print or electronic media or by other indirect means. Fraud perpetration typically requires some specialised skills because it takes the forms of trick, cunning, deceit and unfair means by which another is cheated (Singleton & Singleton, 2010). Cybercrimes that are financially driven usually requires a high degree of organization and specialization (United Nations Office on Drugs and Crime, 2013). In their analysis of the problem, (Jegede, Oyesomi, &

Olorunyomi, 2013) assert that cyber fraud constitutes a major threat to the modern global economy because of its attraction to criminal elements ranging from those committing simple fraud crimes to major organised crime activities. McConnel (2000) cited in Okeshola and Adeta (2013) posits that cyber fraud differ from other forms of crimes due to the fact that it is simple to learn and understand; it requires little resources to support the talent to cause damage or destruction; it can be committed in an environment or an area without the physical appearance of the criminal; and the illegality of the case may be difficult to prove. Generally, online fraudsters create their markets and products through surfing the Internet, and by maintaining complex relationship within the web through spatial interactions globally (Jegede, Oyesomi, & Olorunyomi, 2016).

Gender constitutes an important variable in the propensity for crime involvement, and the types of crime that people usually perpetrate (Jegede, Elegbeleye, Olowookere, & Olorunyomi, 2016; Steffensmeier, Schwartz, & Roche, 2013; Zhang, Chin, & Miller 2007; Miller 2001). With regard to cybercrime, Hutchings and Chua (2017) opine that gender imbalance in cybercrime resembles the gender imbalance in offending more generally. On their own part, Idehen, Ojewumi and Olasupo (2013) note that females are more likely to have a negative attitude towards Internet fraud than their male counterparts, and would rather prefer not to engage in it. Taylor (1999) notes that gender ratio at hacking conferences is often approximately one female to every hundred males, and that females are only transiently involved in the hackers' subculture. Similarly, Chantler (1995) posits that female hackers are perceived with either complete disdain or with high regard by the general hacker community. In a study conducted among students of a college, Hollinger (1993) discovered that 5.2% males and 1.8% females admitted to have gained unauthorised access to other peoples' computer account or computer files. Moreover, Skinner and Fream's (1997) study on music piracy and unauthorised computer access by a student population revealed that 13.6% of females sampled admitted to guessing peoples' passwords, while 9.5% admitted to accessing a computer account without permission to browse files. The percentages of males admitting to the same behaviours were 25.2% and 22.7% respectively.

The ubiquity of social media platforms in recent times has further aggravated the extent of cyber fraud involvement among undergraduates in Nigeria (Akor, 2017; Aileru, 2016; Onah & Nche, 2014). Indeed, the trend and patterns of this crime is fast changing with the increasing involvement of female students. For instance, in November, 2018, the Economic and Financial Crimes Commission (EFCC) arrested 34 undergraduates, including nine females suspected to be involved in cyber fraud perpetration at Awa-Ijebu, Ogun State (Akinkuotu, 2018). Moreover, Tade and Aliyu (2011) submit that cyber fraud has literally become a way of life for many undergraduates in Nigerian universities. Aghatise (2006) contends that 80% of cybercrime perpetrators in Nigeria are students in various institutions. Also, Aransiola and Asindemade (2011) lament that Internet fraud has gained wide popularity among Nigerian youths to the extent that those involved in the crime are easily known. Cross (2018) views cyber fraud as a symptom of the larger social and systemic ills bedeviling Nigeria as a nation. Furthermore, Cross (2018) asserts that online fraud in Nigeria is not only impacting negatively on the lives of many victims within its border and outside its territory, but it equally has devastating impacts on the country in terms of its security and economy. Against this background, this study

examined the pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-west Nigeria.

Theoretical Framework

The propositions of social learning theory were employed as the theoretical base for this study. The theory is essentially an integration of differential association and behavioural learning theories (Akers, 2000). It explicates the learning process that occurs through the interaction with deviant others in which individuals learn to define their attitudes and behaviours as deviant, imitate the behaviour of others, and have these ideas reinforced through a balance between experienced or observed rewards and punishments (Akers, 1998; Akers, 1995). Basically, social learning theory states that crime is a learned behaviour that results from the interaction of four principal components – (a) differential association (this refers to the people that an individual associates with and how interactions with others who engage in a certain type of behavior can affect the individual's patterns of norms and values); (b) definitions (this connotes the attitudes and meanings that an individual attaches to certain behaviours); (c) differential reinforcement (this entails the relationship between anticipated and actual rewards and punishments that follow a behaviour); and (d) imitation (this means observing behaviour that others are engaging in, and then engaging in that behaviour yourself) (Akers, 1998; Akers, 1995). In essence, social learning theory mainly assumes that a dual directional relationship exists between deviance and conformity, because both are influenced by the process of modelling and reinforcement. Therefore, deviant behaviour is more likely to result when an individual associates more with individuals who engage in and approve of deviant than with people who do not. Thus, if one associates disproportionately with groups that expressed, accepted and involved in deviant behaviour, one is more likely to engage in that same behaviour because these groups are likely to provide reinforcement and serve as models to imitate (Akers, 2000). Female undergraduates who have family member(s) or close friend(s) who are involved in cyber fraud are likely to be positively reinforced and encouraged towards taking to this form of crime.

Study Area and Study Population

Two universities in south-west Nigeria, Ladoke Akintola University of Technology, Ogbomosho and Olabisi Onabanjo University, Ago-Iwoye constituted the study locations. Ladoke Akintola University of Technology (LAUTECH) is a university jointly owned by Oyo and Osun state governments. It was established in 1987, and has a student population size of about 20,000. Equally, Olabisi Onabanjo University (OOU) was owned by the Ogun state government. It was established in 1982, and has a student population size of over 20,000. These institutions were purposively targeted for this research because previous studies have indicated that cyber fraud is pervasive among undergraduate students of these universities (Akinkuotu, 2018; Tade & Aliyu, 2011; Ojedokun, 2010). The primary target population for this study were female undergraduates of the two selected universities involved in cyber fraud.

Methodology

This study was exploratory and cross-sectional in design. Data were principally generated through the in-depth interview method. This method was employed to generate the desired information from 17 female undergraduates perpetrating cyber fraud. The snowball sampling technique was essentially employed for the selection of respondents. At the two Universities covered, initial contact with the first few female undergraduate cyber fraudsters were facilitated with the assistance of some of their male counterparts. Some of the questions raised during the interview sessions with the respondents were: (1) Why do you engage in cyber fraud? (2) How did you become involved in cyber fraud perpetration? (3) Since when have you been perpetrating cyber fraud? (4) Can you explain the type(s) of cyber fraud you normally engage in? (5) How did you learn the skills you are using to perpetrate cyber fraud? (6) How do you normally improve your skills for cyber fraud perpetration? (7) How do you normally identify and select your targets? (8) What methods do you normally deploy to get your targets? (9) What form of relationship exists between male and female students involved in cyber fraud perpetration? (10) What do you normally do with your proceeds from cyber fraud?

The process of data collection from the students was particularly demanding because they were initially skeptical about the mission of the researchers. Typically, pre-arranged meetings and mutually agreed appointments were routinely cancelled by them. In fact, most of them initially declined participation, and it actually took the intervention of some of their close friends before they became fully reassured and gained enough confidence to participate. Nevertheless, some of them totally declined to partake in the interview despite several assurances. Furthermore, those that consented were given the privilege to determine the time and location that were most convenient for them. Generally, the interaction with the respondents typically became easy and warm after the initial was broken. Data generated were subjected to manual content analysis and thematic reporting involving careful transcription, detailed description and interpretation.

Ethical Consideration

Owing to the sensitive nature of this study, conscious efforts were made to protect the rights and integrity of the respondents who were interviewed. Generally, the international ethical standard for the conduct of social research was strictly upheld. The objectives of the study were clearly explained to the respondents and their consent was sought before they were involved. Also, they were not subjected to any form of coercion or intimidation, and they were informed of their rights to withdraw participation whenever they deemed necessary. Painstaking efforts were made to ensure that their participation in the study did not expose them to any form of harm.

Results and Discussion

This section thematically presents and discusses the major findings that emanated in the course of this study. The issues covered involved the pathways to female undergraduates' involvement in cyber fraud, the motivating factors for female undergraduates' involvement in cyber fraud, the mode of operation of female undergraduates involved in cyber fraud, female undergraduates' sources of cyber fraud techniques, and the utilisation of their cyber fraud proceeds.

1. Pathways to Female Undergraduates' Involvement in Cyber Fraud

It was considered pertinent to consider the pathways to female undergraduates' involvement in cyber fraud as a way of generating useful information on the circumstances shaping their positive dispositions towards this form of crime. Generally, findings revealed that all the respondents disclosed that their trajectory into cyber fraud practice was strongly influenced by their significant others who were males. Most of the respondents were initiated into the criminal act by their boyfriend, while others got involved in the act through their brother. It was clearly established in the study that respondents did not delve into cyber fraud perpetration on their own. Rather, they were initiated into the criminal act by their significant others who were also involved in it.

In one of the interviews conducted, a respondent claimed:

> I do engage in cyber fraud with my brother. Once he has a *job* for me, he usually calls me because we are not staying together. He has my BVN (Biometric Verification Number) with him. He will give me the transaction ID and I will pick the money for him, but if he wants me to answer a phone call, I will have to go to his place. I am actually doing it (cyber fraud) with my brother, because what we are doing is not *legit*. So, I cannot do it with an outsider. I believe that I can still be protected if I am doing it with my own blood (relative) (IDI/Female Undergraduate/CyberFraudster/Islam/Yoruba/LAUTECH/200L/18years).

In the words of another respondent:

> My Godfather who is also my school father kind of introduced me to cyber fraud because my dad was unable to pay my school fees and I have to hustle by myself (IDI/ Female Undergraduate Cyber Fraudster /Christianity/Igbo/OOU/300L/21years).

Another respondent had this to say:

> My boyfriend introduced me to it (cyber fraud); and seeing how they (other people involved in cyber fraud) do it and get money, nobody wants to live without having money. Looking at them, and seeing the way they are doing stuffs, and at the end they usually come up with money, there is no way one would not have interest in it (IDI/ Female Undergraduate Cyber Fraudster /Christianity/Yoruba/OOU/300L/22years).

A respondent also mentioned:

> I have always been doing it (cyber fraud). The first time I tried it myself, I made money. So, I was encouraged to do more. Actually, I never learnt from any group of people. I got to learn it from a particular person and that person is my boyfriend. Any issue I am having on my scheme, I usually discuss it

> with him. Whenever I need any information, I always ask him (IDI/ Female Undergraduate Cyber Fraudster /Christianity/Yoruba/OOU/300L/22years).

From the above submissions, it is clear that the involvement of female undergraduates in cyber fraud was strongly influenced by their significant others, who could either be a boyfriend or a boyfriend or a godfather. A major deduction that can be made from this finding is that female students were initiated into cyber fraud perpetration by their male relatives and associates. The implication of this finding is that the risk for female undergraduates to be receptive to cyber fraud is higher if their brothers or boyfriends were involved in it. Also, this result is similar to the findings of Ige's (2008) study which discovered that secondary school students in Oyo and Ondo States, Nigeria were being initiated into Internet crime by their friends in the universities, polytechnics, and colleges of education. Equally, it validates a major proposition of social learning theory which submits that deviant behaviour is more likely to result when an individual associates more with individuals who engage in, and approve of deviant than with people who do not. Furthermore, this result is in tandem with the outcome of Miller and Morris 's (2014) study which discovered that associations with delinquent peers who have records of cyberbullying appeared to have a significant effect on people's tendencies towards such new deviant behaviour.

2. Motivating Factors for Female Undergraduates' Involvement in Cyber Fraud

Information was also sought on the motivating factors for female undergraduates' involvement in cyber fraud as a way of understanding the situational and contextual indices informing their decisions to take to this form of crime. Findings revealed that different push and pull factors accounted for respondents' involvement in the perpetration of cyber fraud. Nearly all the female cyber fraudsters interviewed ascribed their motivation for indulging in online fraud to financial need and peer pressure, only few of them attributed their involvement in the criminal act to the desire for fun and entertainment. For instance, in one of the interviews conducted in LAUTECH, a respondent opined thus:

> My brother who engages in cyber fraud is my junior. I am his elder sister. I just thought that if what my brother is doing (cyber fraud perpetration) could fetch him money why can't I also do same and earn money for the family? At least, what a man can do a woman can do better, that was just what actually motivated me to engage in it (IDI/ Female Undergraduate Cyber Fraudster/ Islam/Yoruba/LAUTECH/300L/24years).

A respondent also stated:

> What actually motivated me is that I needed money. Whenever I saw my friends buying something I could not afford, I always feel so bad. That was why I decided to go into cyber fraud. I prefer engaging in cyber fraud to becoming an *olosho* or a runs-girl (sex-worker) (IDI/ Female Undergraduate Cyber Fraudster /Christianity/Yoruba/OOU/400L/22years).

In the words of another respondent:

> I was a teacher before I gained admission into this University. I was teaching in a primary school where I was receiving a salary as low as four thousand five hundred naira (₦4, 500) per month. Then, luckily enough I was able to gain admission to study in OOU, so I had difficult time after my verification and registration. I almost gave up until my Godfather, who was then my school father, showed me the way (cyber fraud) (IDI/ Female Undergraduate Cyber Fraudster/Christianity/Igbo/ OOU/300L/21years).

However, a respondent asserted:

> Nothing actually motivated me to engage in it (cyber fraud). It is just something I decided to do to while away time, have some fun and probably to make some money (IDI/Female Undergraduate Cyber Fraudster /Christianity/Yoruba/OOU/200L/20years).

It can be inferred from these narratives that financial gain and peer pressure were the dominant factors encouraging female undergraduates' involvement in cyber fraud in Nigeria. Most of the respondents claimed they were pushed into engaging in cyber fraud to meet some financial demands such as payment of their tuition fee, augmenting the inadequate monthly allowance received from their parents, and procuring some materials needed in school. Indeed, engaging in cyber fraud was considered by the respondents as a better alternative to taking to prostitution. Although most of the respondents were motivated to engage in cyber fraud, few of them took to the act out of the desire for fun and entertainment. This outcome is in tandem with the result of Ojedokun's (2010) research which found the desire for monetary gain and peer pressure to be the major factors predisposing university undergraduates in south-west Nigeria to cybercrime.

3. Mode of Operation of Female Undergraduates Involved in Cyber Fraud

The success or failure of a crime is often influenced by the method(s) employed by its perpetrator(s) (Schamelleger & Volk, 2018; Brown, Geis, & Esbensen, 2010). Therefore, the mode of operation usually adopted by female undergraduates for facilitating cyber fraud was investigated as a way of understanding their levels sophistication and dexterity regarding this form of crime. Generally, female undergraduate cyber fraudsters relied on the utilisation of social media platforms and social engineering for enticing and swindling their victims. Some of the methods commonly employed involved selling fictitious goods on social media platforms, engaging in romance scam, engaging in identity theft, and soliciting money from donors through false pretense and deception. In one of the interviews conducted at LAUTECT, an interviewee described her method of operation this way:

> Everything is done online. If you message them (potential victims) and they are falling for you, they do not block you (Facebook account) or report you to Facebook administrator. Then, I will continue chatting with them until a

> form of relationship is established (IDI/ Female Undergraduate Cyber Fraudster /Christianity/Yoruba/ LAUTECH/400L/23years).

In the words of another:

> It is just a matter of opening a new account (social media). The truth is that cyber fraud will not be possible without them (victims); this is because they are the ones making it easier for us. Imagine, you as a female opened a Facebook account, and in the next three minutes your inbox is already filled-up with messages of people trying to know more about you. We just make use of this kind of opportunity to get what we want (IDI/ Female Undergraduate Cyber Fraudster /Islam/Yoruba/OOU /400L/24years).

Also, a respondent stated:

> Dating (online) is deeper. There are some females that do *legit*, and when it comes to *legit,* they usually use their own real picture. Some of them are lucky enough to meet a man that would tell them, I really want to marry you, if it is for me to bring you down here (Europe or America). They are easily trusted because they engage in video calls with them. But for someone like me, I am using someone else's picture. Really, the trust is not easy to build because some of them usually ask me to make video call with them. You know, one would not be able to make a video call because of the fake identity. This kind of thing can be discouraging, but if you know how to turn someone's brain (to manipulate) by bringing up lies, then you can be lucky (IDI/ Female Undergraduate Cyber Fraudster /Islam/Yoruba/OOU/300L/24years).

Another had this to say:

> We usually go online and pretend as if we sell different things like body cream, bathing soap, bags, shoes, watches, children wear etc. What we usually do is that we normally open a page for what we do on Facebook or Instagram and we get a new sim card. On the page, we usually advertise what we sell and include our phone contact(s). When you call the number with the Truecaller application, it would display the name of the business we use the sim card to register, but we usually ensure that the location icon is put off. When we are engaging in local scam, we get new sim-card, a new Facebook or Instagram page, write a new name which is mostly the name that goes with whatever we are selling, they cannot even trace us or detect us with the Truecaller application. The only source through which we can be successfully traced is through our bank. Whenever I am browsing, I always make sure that the location icon is off so that people will not be able to detect where I am and trace me. I can even be in Ogun State and write online that I am in Taraba State, and that the goods will take some days before it could get delivered (IDI/ Female Undergraduate Cyber Fraudster /Christianity/Yoruba/OOU/400L/23years).

An interviewee also mentioned this:

> I normally send a passionate message to someone online that I am suffering from cancer, and that I have raised a certain amount of money. I will then indicate that my spirit asked me to request for your financial assistance in order for me to get enough money so as to be able to treat myself. If the person believes my story, he or she person would send me some money (IDI/ Female Undergraduate Cyber Fraudster /Islam/Yoruba/OOU/300L/21years).

It can be deduced from these submissions that female undergraduates involved in cyber fraud employed a wide range of methods for perpetrating the crime. Some of the major ones mentioned were advertising fictitious goods on the social media platforms, especially Facebook and Instagram, engaging in fake online dating, relying on female charms and wits to attract victims, and requesting for financial assistance to treat terminal illnesses from anonymous donors. This finding indicates that female undergraduate cyber-fraudsters like their male counterparts are ingenious people who have carefully devised different means of ripping-off their victims both locally and internationally. Kunz and Wilson (2004) have also observed that computer fraudsters are using electronic resources to present fraudulent or misrepresented information as a means of deception. Another major deduction that can be gleaned from this finding is that female undergraduates involved in cyber fraud are maximising the wider interconnectivity and interactive advantages presented by the ubiquity of social media platforms in Nigeria for their criminal activities. Akor (2017) and Aileru (2016) have also affirmed that undergraduate students in Nigeria are employing social media platforms to victimise their unsuspecting their targets. In addition, this outcome validates a tenet of social learning theory which states that if one associates disproportionately with groups that expressed, accepted and involved in deviant behaviour, one is more likely to engage in that same behaviour because these groups are likely to provide reinforcement and serve as models to imitate (Akers, 2000).

4. Female Undergraduates' Sources of Cyber Fraud Techniques

Attention was also devoted to female undergraduates' sources of information on techniques for perpetrating cyber fraud. Generally, findings revealed that female undergraduate cyberfraudsters usually gather information for facilitating their criminal act from different sources. Although all the respondents identified their male relatives and friends who were also cyber fraudsters as the primary source(s) of information for cyber fraud techniques. Nevertheless, they were not solely dependent on a single source, as they normally cross-fertilize ideas with different sources. Also, they usually do conduct their own private research on the Internet to determine new result-oriented techniques. One of the students interviewed at the Olabisi Onabanjo University, Ago-Iwoye stated thus:

> To an extent doing it (cyber fraud) with my boyfriend has helped me a lot. For instance, there was a time I got a client I was talking to, it was my boyfriend that realised that we could make a lot of money from him. In fact, I did not realise this potential initially. When he helped me to handle him,

> the client paid a lot of money (IDI/Female Undergraduate Cyber Fraudster /Christianity/Igbo/OOU/300L/23years).

A respondent also said:

> I have guys that do give me formats (ideas) of what to ask my clients. They will always ask me if I am making progress in the scheme. Whenever I tell them that hit is slow or not moving, they usually give me advice as per new tricks that I can use on clients. This usually works, but sometimes it does not work as expected. So, I always ensure I Google everything they told me before using it on my *clients*. So, if it is not possible, I will tell them and say, let us do something else. I do not want to run into debt. For instance, there was a time my friend told me about the basic travelling allowance (BTA) format which I Googled, and realised that it is only members of staff in a company that can ask for that kind of money, so I told the person who gave me the format not to try it (IDI/FemaleUndergraduate/CyberFraudster/Christianity/Yoruba/OOU/300L/20years).

Another interviewee stated:

> I use to sit with the guys in my hall whenever they are doing it (cyber fraud perpetration). I will be looking at them and be asking question. From there I will be helping them to clone accounts for lotto. In the process, I will be practicing on my own through that. But for online dating, one will just need to open an account on a dating site and one would just be acting normal as if one is chatting with one's boyfriend (IDI/Female Undergraduate Cyber Fraudster /Islam/Yoruba/OOU/300L/21years).

In the words of another:

> We are in the computer age, so things are really easy to learn and understand. Even using one's mobile phone without any person teaching one how to go about it (cyber fraud perpetration), one can easily browse different techniques online. I do stay with those that have already know it and grab what they are doing, and whenever I am on my own, I do try it (IDI/Female Undergraduate Cyber Fraudster /Christianity/Yoruba/LAUTECH/400L/23years).

A respondent also claimed:

> I use to read and go through the format they (other friends perpetrating cyber fraud) normally give to me. If I meet a client for the first time, the suitable question I can ask him or her is contained in the format I already collected. For example, I can ask the client the kind of music he or she likes to listen to or the type of food he or she likes to eat etc. (IDI/Female Undergraduate Cyber Fraudster /Christianity/Yoruba/OOU/400L/24years).

These narratives indicate that female undergraduates involved in cyber fraud mostly learned the techniques for perpetrating the crime from their friends and associates. Equally, some of them also do combine the techniques learned from others with information generated on the Internet. The implication of this finding is that female undergraduates have realised that cyber fraud requires constant creativity and elements of ingenuity to be successfully perpetrated. Therefore, they are usually actively making efforts to be able to succeed in the criminal act by learning from their male counterparts who are already well-established in the illegal business. Adeniran (2008) has equally posited that youths of both sexes are functionally involved in Internet fraud in Nigeria with varying specialised functions. Furthermore, this finding brings to bear the relevance of social learning theory which views imitation or modelling to be central to the learning process which essentially involves observing the behaviour of others.

5. Female Undergraduates' Use of Cyber Fraud Proceeds

Previous studies have indicated that male undergraduates involved in cyber fraud in Nigeria are spendthrifts who are generally wasteful to the extent that they have been widely recognised to be maintaining distinct social lifestyles which conferred on them the status of *big boys* among their peers (Ojedokun & Eraye, 2012; Aransiola & Asindemade, 2011; Tade & Aliyu, 2011). Thus, respondents were questioned on how they usually utilise the proceeds realised from cyber fraud. The study established that female undergraduate cyber fraudsters were generally using the financial gains of their fraudulent activities for two major things. Apart from using the illicit gains for their upkeep and for meeting some of the needs of their immediate family members, they are also saving and investing their proceeds in some legitimate businesses.

One of the respondents submitted:

> I usually settle (give money) my family members and make sure they are okay. I do provide for my family needs, and I have another savings account where I do keep my money (IDI/ Female Undergraduate Cyber Fraudster/Islam/Yoruba/OOU/300L/24years).

Another respondent declared:

> I get most of the things that I need. My monthly stipend is nothing. So, calling my parents for money is like making them feel bad. My elder sister is not into cyber fraud so at times I do send stuffs to her. Also, at times, I even do send money to my brother and my parents, especially when my mum wants to get something for herself (IDI/ Female Undergraduate Cyber Fraudster /Islam/Yoruba/LAUTECH/200L/18years).

In the words of another respondent:

> From this *yahoo-yahoo* (cyber fraud) thing, I have gotten myself an oven because I am also into baking. I have gotten all my baking equipment which also fetches me some additional money (IDI/ Female Undergraduate Cyber Fraudster /Christianity/Yoruba/OOU/400L/22years).

Also, a new entrant into this crime said:

> I do not have any asset now because I just started it (cyber fraud). However, people use to say that if you made money, you will spend it anyhow. It depends on the individual. If you have plans you will know what you are doing. Okay, for me that I decided to get involved in *Gee* (cyber fraud), I know what I want to use the money for when I make a hit. But there are some people that are just engaging in *Gee*, they do not have plans. If I see one big money now why would I not invest? I will invest in something that will be bringing me money every time (IDI/Female Undergraduate Cyber Fraudster/Yoruba/OOU/300L/22years).

These responses indicate that female undergraduates involved in cyber fraud, unlike their male counterparts who are reputed to be extravagant and generally careless with their criminal proceeds, see the crime as a source of income for meeting their own personal and their relatives' financial needs. Also, they viewed cyber fraud as a means of generating the initial capital for which they are planning to invest in a legitimate business. This finding negates the position of Idehen et al. (2013) that females are more likely to have a negative attitude towards Internet fraud, and would rather not engage in it. Another deduction that can also be made from these finding is that the relatives, including parents of some of these female students may be indirectly encouraging them to continue to perpetrate the crime as a result of their financial dependence on them. Moreover, social learning theory opines that individuals' behaviours and attitudes develop in response to the reinforcement and encouragement from the people around them.

Conclusion

This paper has examined the pathways and motivations for cyber fraud involvement among female undergraduates of two universities, Ladoke Akintola University of Technology (LAUTECH) and Olabisi Onabanjo University (OOU) in south-west Nigeria. Generally, female undergraduates involved in cyber fraud got initiated into the crime by their male relatives and associates. The need for financial gain was the dominant factor encouraging their involvement in the criminal act. Also, the methods commonly employed by the female students for perpetrating cyber fraud included: advertising fictitious goods on the social media, especially Facebook and Instagram, engaging in online dating, relying on female charms and wits to attract potential victims, and requesting for financial assistance to treat terminal diseases from anonymous donors. Friends constituted the major source of information for the respondents on the techniques

employed for perpetrating cyber fraud. Female undergraduates saw cyber fraud as a source of income for meeting their own personal and their relatives' financial needs, and as a means of generating the initial capital for investing in a legitimate business. Cyber fraud is not only having devastating effects on the victims, but it is also negatively impacting the economy and international image of Nigeria as a nation. Therefore, the following recommendations are suggested as way of addressing the problem:

Relevant security agencies, particularly the Economic and Financial Crimes Commission (EFCC) should intensify their efforts at tackling cyber fraud by developing strategies for identifying, arresting, and prosecuting female undergraduates involved in it. Indeed, the nearly exclusive ascription of cyber fraud perpetration in Nigeria to male youths (*yahoo boys*) has over time deflected attention away from female undergraduates perpetrating the crime. Although female students involved in this crime typically maintain a low profile which usually make them difficult to identify, nevertheless security personnel can infiltrate their networks by through the assistance of their arrested male counterparts. Similarly, the Student Affairs Department in Nigerian tertiary institutions in collaboration with their school managements should design a framework through which cyber fraud perpetration can be effectively discouraged among their students. This step can be achieved by setting up of anti-cyber fraud campus committee that would be charged with the responsibility of detecting and penalising students engaging in cyber fraud. Also, the whistle blowing policy newly created by the Federal Government of Nigeria to discourage corruption among Nigerians should be expanded to cover cyber fraud perpetration among tertiary institution students. In this instance, a form of reward system should be created to encourage students to provide information that can be useful for the identification and arrest of their colleagues perpetrating cyber fraud. Finally, there is a need to embark upon massive reorientation regarding cyber fraud perpetration. Indeed, the '*get quick rich*' mentality that is pervasive among the youths in Nigeria should be discouraged. This step requires a multi-level approach that will essentially involve relevant stakeholders including the family and religious institutions, the media, and officials of the National Orientation Agency (NOA).

References

Adeniran, A. I. (2008). The internet and emergence of yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2*(2), 368–381.

Aderinto, A. A., & Ojedokun, U. A. (2017). Cyber underground economy in Nigeria.In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 219-226). Zaria, Nigeria: Ahmadu Bello University Press.

Aghatise, E. J. (2006, June). Cybercrime definition. *Computer Research Centre*. Retrieved from http://www.crime-research.org/articles/joseph06/2.

Aileru, M. M. (2016). *Social media and cyber victimization experience of University of Ibadan undergraduate students* (Unpublished master's thesis). African Centre for Information Science (ARCIS), University of Ibadan, Ibadan, Nigeria.

Akers, R. L. (1985). *Deviant behaviour: A social learning approach*. Belmont, CA: Wadsworth.

Akers, R. L. (1998). *Social learning and social structures: A general theory of crime and deviance*. Boston, MA: Northeastern University Press.

Akers, R. L. (2000). *Social learning theory*. USA: Roxbury Publishing Company.

Akinkuotu, E. (2018, November). EFCC arrests 23 OOU students, 12 others for internet fraud. *The Punch*. Retrieved from https://punchng.com/efcc-arrests-23-oou-students-12-others- for-internet-fraud.

Akor, L. (2017). The social media, deviance and youths in Nigeria. In P. N. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 47–64). Zaria, Nigeria: Ahmadu Bello University Press.

Amosun, P. A., & Ige, O. A. (2009). Internet crime: A new breed of crime among in-school aged children in Nigeria. *The African Symposium: An Online Journal of African Educational Research Network, 9*(2), 90–98.

Anyanwu, J., Oforegbu, T., Igbo, J., & Obiyo, N. (2012). Application of E-learning as a conduit for computer crime among deviant university undergraduates in Nigeria: Psychological and counselling implications. *US-China Education Review,11*, 979–985.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 759-763.

Arowosaiye, Y. I. (2008, November). *The new phenomenon of phishing, credit card fraud, identity theft, internet piracy and Nigeria criminal law*. Paper presented at 3rd Conference on Law and Technology, Faculty of Law, University Kebangsaan, Malaysia and Faculty of Law, University of Tasmania, Australia.

Babatunde, M. M., & Olanrewaju, M. K. (2015). Peer pressure, parental socioeconomic status, and cybercrime habit among university undergraduates in Southwestern Nigeria. *International Journal of Technology in Teaching & Learning,11* (1), 50–59.

Brown, S. E., Esbensen, F., & Geis, G. (2010). *Criminology: Explaining crime and its context (Seventh Edition)*. Mathew Bender & Company, Inc.

Button, M., & Cross, C. (2017). Technology and fraud: The 'fraudogenic' consequences of the Internet Revolution. In M. R. McGuire and T. J. Holt (Ed.), The *Routledge handbook of technology, crime and justice* (pp.78- 93). Routledge.

Chantler, A. N. (1995). Risk: *The profile of the computer hacker* (unpublished thesis). Curtin University, Australia.

Cross, C. (2018). Marginalised voices: The absence of Nigerian scholars in global examinations of online fraud. In K. Carrington, R. Hogg, J. Scott & M. Sozzo (Eds.), *The Palgrave Handbook of Criminology and the Global South* (pp 261-280). Gewerbestrasse: The Palgrave Macmillan.

Duffield, G., & Grabosky, P. (2001). *The psychology of fraud*. Canberra: Australian Institute of Criminology Trends and Issues in Crime and Criminal Justice, No. 199.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance & Control: Financial Markets & Institution, 4*(2), 16-26.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and unauthorised account access. *Security Journal, 4*, 2-12.

Hutchings, A., & Chua, Y. (2017). Gendering cybercrime. In T.J. Holt (Ed.), *Cybercrime through an interdisciplinary lens* (pp. 167-188). Oxon: Routledge.

Idehen, E. E., Ojewumi, A. K., & Olasupo, M. O. (2013). Influence of self-esteem and self-monitoring on attitudes towards internet fraud among undergraduate students of Obafemi Awolowo University, Ile-Ife. *African Research Review, 7*(2), 294-305.

Ige, O. A. (2008). *Secondary school students' perceptions of incidences of internet crimes among school age children in Oyo and Ondo States, Nigeria* (Unpublished master's thesis). Department of Teacher Education, University of Ibadan, Ibadan, Nigeria.

Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I., & Olorunyomi, B. R. (2016). Gendered alternative to cyber fraud participation: An assessment of technological driven crime in Lagos State. *Nigeria Gender & Behaviour, 14*(3), 7 67 27 692.

Jegede, A. E. Oyesomi, K. O., & Olorunyomi, B. R. (2016). Youth crime and the organised attributes of cyber fraud in the modern technological age: A thematic review. *International Journal of Social Sciences and Humanities*, 6(1), 153-164.

Koong, K. S., Liu, L. C., & Wei, J. (2006). An examination of internet fraud occurrences. *International Journal of Cyber Criminology, 5*(2),441-449.

Kunz, M., & Wilson, P. (2004). *Computer crime and computer fraud.* Report Submitted to the Montgomery County Criminal Justice Coordinating Commission, in part as fulfilment for the professional Master Degree in the Department of Criminology and Criminal Justice, University of Maryland, United State.

Lee, W. A. (2003). *Progress report from BITS* on *fraud prevention effort*. The American Banker, 1.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *British Journal of Criminology, 48*, 293-318.

Miller, J. (2001). *One of the guys: Girls, gangs, and gender*. New York: Oxford University Press.

Miller, B., & Morris, R. G. (2014). Virtual peer effects in social learning theory. *Crime & Delinquency*. doi: 10.1177/0011128714526499.

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001–1013.

Ojedokun, U. A. (2010). *Cybercrime and changing lifestyle among students of some selected universities in south western Nigeria* (Unpublished master's thesis). Department of Sociology, University of Ibadan, Ibadan, Nigeria.

Okeshola, F. B., & Adeta, A. K. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American International Journal of Contemporary Research, 3*(9), 98–114.

Onah, N. G., & Nche, G. C. (2014). The moral implication of social media phenomenon in Nigeria. *Mediterranean Journal of Social Sciences, 5*(20), 2231–2237.

Schmalleger, F., & Volk, R. (2018). *Canadian criminology today: Theories and applications* (6th ed.). Ontario: Pearson.

Singleton, T. W., & Singleton, A. J. (2010). Fraud auditing and forensic accounting, Fourth Edition, New Jersey: John Wiley & Sons, Inc.

Skinner, B. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*, 495-518.

Smyth, S. M., & Carleton, R. (2011). *Measuring the extent of cyber fraud: A discussion paper on potential methods and data sources*. Public Safety Canada.

Steffenmeiser, D. J., Schwartz, J., & Roche, M. (2013). Gender and twenty-first-century corporate crime: female involvement and the gender gap in Enron-era corporate frauds. *American Sociological Review, 78*(3), 448-476.

Tade, O., & Aliyu, A. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860-875.

Taylor, P. A. (1999). *Hackers*, London: Routledge.

This Day. (2016, April). Nigeria loses over ₦127bn annually through cybercrime. Retrieved from www.thisdaylive.com/index.php/2016/04/18/cyber-security-nigeria-loses-over-n127bn-annually-through-cybercrime/amp.

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY_210213.pdf.

Whitty, M. T. (2018). 419 –It's just a game: Pathways to cyber-fraud criminality emanating from West Africa. *International Journal of Cyber Criminology*, 12(1), 97-114.

Zhang, S. X., Chin, Ko-Lin., & Miller Jody. (2007). Women's participation in Chinese transnational human smuggling: A gendered market perspective. *Criminology, 45*, 699–733.