African Journal of Business and Economic Research (AJBER)
(Online) ISSN 1750-4562 (Print) ISSN 1750-4554
Published consistently since 2006
Indexed by SCOPUS, UGC CARE List, IBSS, EBSCO, ProQuest, ABDC, SAJE, COPERNICUS, ERIH PLUS, CABELL, Sabinet and J-Gate

Vol. 19, (Issue 3), September 2024

Pp483–500

Collaborative Bank E-Fraud and Customers' Reactions in Ado-Ekiti Metropolis, Ekiti State, Nigeria

DOI: https://doi.org/10.31920/1750-4562/2024/v19n3a22

ABRIFOR Chiedu Akporaro[1], EGBO Amechi Ken[2], OJO, Odunayo Tolulope[3], OJIZIELE, Monday Oriabure[4], AKAN, Kevin Akpanke[5], ATINUKE Titilope Babalola[6], POPOOLA Sikiru Solagbade[7] and Adebayo Anthony Abayomi[8]

[1-5,7]*Department of Criminology and Security Studies, Federal University Oye Ekiti, Nigeria.*
[6]*Department of Guidance and Counseling, Federal University Oye Ekiti, Nigeria.*
[8]*Department of Sociology, Federal University Oye Ekiti, Nigeria*
**Corresponding author: ABRIFOR Chiedu Akporaro*
**Email: chiedu.abrifor@fuoye.edu.ng*

Abstract

The high prevalent rate of banks e-frauds that is enthralling customers' finance and bank integrity will soon begin to retard public trust and banks' developmental purposes in Nigeria generally and specifically, Ekiti State if prompt actions are not taken against its effect. This paper examined the collaborative banks' e-fraud and customers' reactions in Ado-Ekiti Metropolis, Ekiti State. The paper was anchored in the fraud triangle theory to explain e-fraud, using three important elements (pressure, opportunity, and rationalisation). The qualitative data were generated from the respondents (bank staff, customers, and victims) respectively, using a purposive sampling technique. Thirty (30) key informant participants with adequate and information about collaborative banking e-fraud and customers' reactions were selected for

the study. Key informant interviews were conducted, transcribed, and reported verbatim to complement the secondary data. The findings revealed that all the participants 30 (100%) had e-fraud awareness through various means ranging from 20 (66.7%) as victims of e-fraud to 6 (20%) through various social media platforms, and 4 (13.3%) as bank staff. The paper also revealed that some bank officials are culprits in bank e-fraud and that banks are not held liable for e-fraud committed against the customers and other related frauds. The study concluded that the effects of banking e-fraud on bank victims are immeasurable; therefore, timely intervention is highly required to reduce and curb the prevalence of e-fraud in the banking sector. The study recommended that banks should trained their employees to improve internal oversight mechanisms to identify and stop fraudulent activities, including e-fraud on the customer assets, while customers should be orientated on how to detect e-fraud tricks and report to relevant authorities for prompt actions.

Keywords: *Fraudulent, Monetary, Opportunity, Pressure, Rationalisation, Victims.*

1.1 Introduction

The prevailing monetary fraud in most Nigerian financial institutions makes many banks more of monetary crime havens for fraudulent acts (Ololade, Salawu, & Adekanmi, 2020; Kingsley, 2012). It is so normalised to the extent that banking fraud cases made most news headlines on all social and print media platforms at intervals (Nigerian Deposit Insurance Corporation [NDIC], 2018). Hence, NDIC (2018), in its annual report, categorically listed 10 Nigerian banks and staff with the highest involvement in monetary fraud, costing the nation and its citizenry about ₦10.53 billion. Undoubtedly, these alarming fraudulent acts drastically reduce most customer trust and public trust and also retard the developmental purposes for which banking services were created and promoted in Nigeria.

Nonetheless, the introduction of the cutting-edge Internet and the uptake of electronic payment systems have made cyber-attacks and e-frauds more common in banks in Nigeria (Ololade, Salawu, & Adekanmi, 2020). The perpetrators of most fraudulent acts in the banking sector are not exactly anonymous as it seems, as many of the monetary fraudulent

acts and other e-frauds are perpetrated collaboratively by both bank staff and professional fraudsters (Ololade et al., 2020). This buttresses the fact that the internal mechanisms of most banks are weakly designed, thereby making it difficult to detect frauds through early warning accountability indicators.

Popoola, Fakunle, Omole and Oyedeji, (2018) opine that the banking electronic payment (e-payment) scheme, a modern and innovative means of cashless payment globally through information and communications technology (ICT), has altered the characteristics and mode of banking operations and upsurge in the activities of fraudsters in Nigeria. However, fraudsters collaborate with unscrupulous bank staff and other Internet fraudsters in many developing countries including Nigeria. For instance, NDIC (2018; 2021) reported a 33% and 45% rise in electronic frauds in 2016 and 2018 respectively, and between 2019 and 2021 respectively. The report stated that the actual amount lost to e-frauds from 2016 to 2018 and from 2019 to 2021 increased from 84% to 86%. Surprisingly, the Central Bank of Nigeria's (CBN) cashless policy initiative, which aims to decrease the quantity of money flow and equally promote customers' use of e-payment for banking activities and transactions, is being frustrated, and Nigerians and others resident in Nigeria get discouraged by the alarming rate of e-frauds perpetrated in the country.

Therefore, the growing fraud epidemic in most Nigerian financial organisations during the last few years undoubtedly poses numerous risks to the survival and stability of customers' finances and performance of banking institutions. Therefore, almost every area of the nation's economy is prone to financial frauds affecting business organisations, individual consumers' finances, and the nation's economy at large (Agwu, 2014). Consequently, Orji (2019) asserts that consumer protection right under the Nigeria's Cybercrime Act of 2015 is inadequate, as customers lack the obligatory right to litigate banks and their staff who are in possession of customers' personal financial information and supposed to safeguard customers' personal financial information against unauthorised access or identity theft as the case may be. Thus, this makes the Act inefficient in fulfilling its main goal of protecting customers' finances against bank frauds. The incessant fraudulent activities taking place in most banks needs timely intervention so as to erase customer disappointments and victims' doubt, and to promote bank performance (Muritala, Ijaiya, Afolabi, &Yinus, 2020; Jegede, 2014).

More scholarly studies need to be conducted on collaborative monetary bank fraud and customer reactions. The few scholars that have researched into this area are Popoola et al. (2018) in a study titled "Bank Fraud and Its Effect on Nigerian Economy". The study investigated some banking institutions and concluded that ICT has increased both banking operations and financial crimes against banks and customers. Nwaimo (2020) explored the perpetration of fraud in banks in Nigeria, with specific emphasis on its implication on the performance of deposit money banks (DMBs). Nwaimo (2020) concluded that all concerned authority in the banking sectors should initiate viable cyber security controls and internal control measures to strengthen fraud checking. Tade and Adeniyi (2017) looked into the frauds perpetrated in the banking sector in South West Nigeria's on automated teller machines (ATMs), laying emphasis on victim typologies, victimisation strategies, and fraud prevention in Lagos and Oyo, and how ATM e-frauds affect victims. Their study found illiteracy, ill-health, and unreliable relatives as major factors giving rise to the high number of ATM fraud victims. The study recommended the following: improved staff welfare; harsh penalties for negligent employees; and continuous education and awareness campaigns for bank clients.

Moreover, Iyodo, Agbaji and Abu (2016) beamed their searchlight on the consequences of bank frauds on the growth of the Nigerian economy and found that fraud has led to many banks' failure and reforms in the banking sector. The study recommended a comprehensive fraud management scheme of factors involved in bank frauds to prevent and control the milieu. Ololade et al. (2020) study on "E-Fraud in Nigerian Banks: Why and How" found that banks employees with threatened employment from low deposit targets, job losses from disruptive technologies and economic challenges connive with other employees to commit E-Fraud against the Banks. The study recommends discouragement of unreachable sales and deposit goals in the banking industry with whistleblowing policy against negative influences from senior colleague.

While the aforementioned studies are valuable and informative, there are still large gaps on collaborative monetary banking fraud and customer reaction in Nigeria. Therefore, these studies cannot be used to generalise the collaborative monetary banking fraud and customer reaction. Hence, it is of great importance to conduct a study on Collaborative Banks E-Fraud and Customers' Reactions

1.2 Statement of Problem

Financial sector fraud is an expanding industry for criminals who use ever-more-creative and inventive methods to target any suspected vulnerabilities in banking institutions and credit-givng systems. Murital et al. (2020) opined that bank performance declines as fraud in the banking industry rises by linking Granger fraud variables to establish the casual relationship between bank performance and fraud. They reported that frauds affects banks performance and customers trust in the bank. Similarly, Idolor (2010) argued that unauthorised lending and foreign exchange (FOREX) fraud are prevalent types of fraudulent activity by banks and yet not perceived as fraudulent activities due to employee participation in fraud planning, execution, and hiding eventually. Other factors such as organisational factors include not enough employees, lax oversight, inadequate training, and unfavourable conditions at work; individual factors include avarice, unfaithfulness, and impoverishment among others are factors helping the propagation of frauds in banks. Agwu (2014) argued that the lack of appropriate legislation and policy frameworks to adequately protect creditors and borrowers is a key player in fraud activities. Customers' heavy reliance on the Internet for financial services has increased the volume of electronic deals, according to Berney (2008) observations. According to Gates, Jacob, and Malphrus (2009), there are greater chances for fraudsters to target clients who have no physical presence on the Internet in order to carry out authenticating transactions. There continues to be increasing worry about fraudulent activities and other illicit conducts in the Nigerian banks, despite fact that the Nigeria Deposit Insurance Corporation (NDIC), the Chartered Institute of Bankers of Nigeria (CIBN), and the CBN oversee and regulate the banking industry. This study aims at examining the collaborative bank e-frauds and customers' reactions in Ado-Ekiti Metropolis, Ekiti State.

2. Literature Review

2.1 Theoretical Framework

The core finding of Donald Cressey's 1919 to 1987 theory of the fraud triangle revealed the dependence of fraud's occurrence on these three factors coming together: pressure (motivation), opportunity, and rationalisation. Thus, someone with a trustworthy reputation starts to bet

ray others' trust when they believe they have a private financial issue, realise that this issue can be solved covertly by betraying financial confidence, and can use their behavioural expressions in the circumstances that allow perception modification of status as trusted individuals with personal perceptions granted funds or property's users. An opportunity is a set of conditions that make fraudulent activity possible. It is the only element in the circle of fraud that a business has a complete influence over. Some of the examples of situations where fraud can be committed are cited here. The procedures and techniques referred to as feeble internal oversights are implemented to ensure the precision of finances and accounting information. Fraudulent activities' chances occur as a result of failing internal oversights, including insufficient task segregation, oversight, and procedure documentation. An organisation with a poor managerial tone is more vulnerable to fraudulent activity. Poor fiscal procedures relate to the way commodities on the accounting records are documented. Managerial tone signifies the management team and the board of directors' (BOD) dedication to ethics, truthfulness, and honesty. Lackluster accounting procedures may allow employees to manipulate the data. Another name for motivation is pressure, and it describes how a worker feels about perpetrating fraudulent activities.
The following are some of the instances that encourage fraud. Profits and net revenue are two monetary indicators that are used to evaluate the work of a worker and determine incentives.

Financial metric-based bonuses put stress on workers to hit desired outcomes, which may lead them to engage in fraudulent activities in order to reach the goal. Requirements from analysts and investors to keep or raise stock prices can also put stress on workers to engage in fraud. Similarly, personal motivations could include having to cover one's own expenses, the desire to make more cash, an addiction to gambling, etc.

A person's rationalisation is their explanation for defrauding others. The typical rationales fraudulent people use to justify their dishonest acts include the following: ill-treatment accompanied by fury to their supervisors or employers; belief in using fraud as retaliation; staff deriving motivation from the upper management staff committing fraud; staff perceiving fraud to be a sure way to wealth should they lose their jobs; and the feeling of being on a safer side as they involve in fraudulent activities (Abdullahi & Mansor, 2015). Essentially, whether motivation, opportunity, and rationalisation are enough or not, the possibility of group action or culture stands at the Centre of the circle, criminality

cannot be exempted. Further, most fraud cases within the Nigerian banks are perpetrated by insiders or insiders-outsiders from the circle of fraudsters. An employee who knows the weaknesses and internal workings of a particular bank will be compelled through internal or external pressures to defraud the bank or share information with others externally (outsiders) to carry out nefarious tasks as joint forces.

2.2 Empirical Review

The banking industry has grown more complicated as information and communications technology (ICT) has advanced, which has not only changed the nature and mode of operations of the banks in Nigeria but also changed the nature of fraud practices (Popoola et al., 2018). There are several factors responsible for banking frauds in Nigeria. One of such factors is the weak internal control mechanism which allows employees-fraudsters to lodge undocumented money through money laundry, grant loans without proper documentation, or illegally invest customers' money. Another factor is failure of the external control mechanism – the inefficiency and inadequacy of the government policy and legal framework – to curb frauds in the banking industry due to implementation problems. Moreover, no organisation is exactly immune to fraud in any society, meaning that fraud is inevitable due to crime rates and criminal tendencies among citizens who feed on the weaknesses of the internal and external control mechanisms, and lack of personal ethics (Idolor, 2010; Kingsley, 2012; Iyodo et al., 2016; Ololade et al., 2020).

The effects of fraud on banks are numerous but more significantly, it causes significant financial hardship for banks and clients (Popoola et al., 2018). Also, Olongo (2013) argued that bank frauds hurts both banks and their customers. Similarly, reimbursing clients' cash losses results in significant operational expenses for banks, causing significant time and emotional losses for the clients of banks. Customers need to identify and report fraudulent transactions to their bank. They should take steps to restrict access to their cards or accounts, have them reissued or opened, and press for the reimbursement of their financial losses reimbursed (Gate & Jacob, 2019; Idolor, 2010). Experiencing fraud can also affect a client's sense of security and protection when they bank there, such that fraud may damage the bank-customer relationship and raise discontent due to a perceived breakdown in the service, leading to conflicts more often. This damages banks' standing and makes it more difficult for them to attract new clients. The absence of a proactive mechanism to combat

fraud, and the ability to gain and maintain customer loyalty are almost nonexistent. An organisation's single immediate problem with not addressing fraud preemptively is loss of revenue. Revenue loss in the long run is caused by the absence of customer trust and lack of perception of safety. To effectively and proactively track and regulate deposit money banks (DMBs), and to stop various forms of fraud and avert the collapse of banking institutions, the NDIC and the CBN must work closely together (NDIC; Iyodo et al., 2016; Popoola et al., 2018).

Fraudulent activities were a major factor in the collapse of banks, which prompted changes in Nigeria's banking industry. This points to a serious issue with the handling and inquiry into fraudulent activities in Nigerian banks. Therefore, a thorough fraud management plan is required to allow one to acquire an in-depth knowledge about every aspect of the development of fraudulent activities and provide a mechanism to checkmate bank e-frauds (Iyodo et al., 2016). However, the appropriate legislative and policy framework to logically protect creditors and debtors is yet to be working efficiently in a way to guard against bank e-frauds. It is, therefore, essential to design control measures within all financial organisations, and the government should also pass appropriate legislation that will allow the stoppage of these obscene incidents. Nonetheless, if stakeholders in financial or banking institutions, especially deposit money banks, CBN, and NDIC, are to ascertain a level of control, there may be a need for cyber-security controls and internal control measures to strengthen them towards checkmating e-frauds (Nwaimo, 2020). Furthermore, instead of continuing to report the instances of fraud in a reactive manner, regulatory organisations such as the NDIC ought to take proactive steps to protect depositor funds in DMBs. The study, therefore, investigated the causes and effects of frauds on banks in Ado-Ekiti metropolis of Ekiti State.

Fraudulent activities in the banking sector are fast becoming more attractive for criminals who use ever-more-creative and inventive methods to take advantage of suspected vulnerabilities in banking institutions and credit-giving systems. Muritala et al. (2020) opined that bank performance declines as frauds in the industry rise by linking Granger fraud variables to establish the casual relationship between bank performance and fraud. They reported that frauds affect bank performance and customers trust in banks. Similarly, Idolor (2010) argued that unauthorised lending and FOREX fraud are prevalent types of bank fraud, but yet they are not perceived as fraudulent activities due

to employee participation in fraud planning, execution, and hiding eventually. Additional elements include personal ones like avarice, cheating, and destitution, as well as organisational ones such as understaffing, shoddy internal oversight, poor training, unfavourable workplace circumstances, etc. These are some of the factors helping the propagation of frauds in banks.

To identify the variables that contribute to victims' vulnerability to ATM frauds and to propose preventative measures, Tade and Adeniyi (2017) investigated ATM frauds in southwest Nigeria. Using the snowball sampling method, 20 respondents — most of whom were victims of ATM frauds — in Lagos and Oyo states were used in this exploratory study design. Using content analysis, the qualitative information obtained from in-depth interviews was examined. The study discovered that factors such as illiteracy, poor health, and mistrust of family members, friends, and lovers contributed to the victimisation tactics used by dishonest individuals. These tactics included ATM card exchanging, card cloning, physical assaults at odd hours (including threats of gunfire), and demobilising those who were attacked by seizing their cell phones. The study suggested three methods for preventing fraud: improving employee welfare; enforcing strict penalties for negligent employees; and providing ongoing education and awareness to bank clients. The focus of the research was ATM fraud, with no attention given to other forms of electronic frauds that occur in Nigerian banks. Furthermore, since the research only included friends, family, and romantic partners of the victims as fraudulent individuals, the potential participation of bank workers is not taken into account. This study closes a gap in the body of literature (Ololade et al., 2020).

Since unscrupulous individuals are now increasingly skilled, fraudulent activity prevention strategies must constantly advance to stay up to date and effectively combat the risk that they pose. For financial services companies, the battle against fraudulent activities is vital. Fraudulent activities have an enormous effect on consumers particularly, the economic system as a whole, and people's businesses. Agwu (2014) argued that the lack of appropriate legislation and policy frameworks to adequately protect borrowers and lenders contributes to the preponderance of fraud activities.

Since evolution, banks have been the target of fraudulent activities, and this has a negative impact on their efficiency and financial performance and could potentially result in trouble. To gain confidence from consumers and goodwill, they must fulfil their obligations with

honesty of intent and unwavering integrity regarding how they operate. The general public expects banking institutions to be more accountable, fair, and transparent, and to provide effective mediation. With advancement in ICT, which has altered the nature of bank fraud, the banking industry has grown more complex. Clients' heavy reliance on the Internet for their banking needs has increased the volume of electronic dealings, according to Berney (2008). According to Gate, Jacob, and Malphrus in 2009, fraudulent individuals have greater chances to target online shoppers who are not physically there to verify online deals. Increasing worries regarding Nigerian bank's fraudulent activities and unethical activities still exist despite the CBN regulating and inspecting banks, the NDIC, and the Chartered Institute of Bankers of Nigeria (CIBN) supervising the sector.

Thus, to guarantee the accuracy of electronic payments and other smooth financial transactions that guarantee the adequate protection of customers' financial resources from fraudulent bank staff and e-fraudsters, the CBN set up the Nigerian E-Fraud Forum (NEFF). Despite several interventions to closely monitor these banking procedures pertaining to electronic payment channels, including mobile payment systems, Internet banking, Smart TVs, ATMs, Point of Sales Terminals (POS), etc., cybercrime has remained a locust eating deep into the strategies to tame it (Tade & Adeniyi, 2017; Ololade et al., 2020). The study assessed the relationship between collaborative bank electronic frauds and customers' reactions in Ado-Ekiti metropolis, Ekiti State, Nigeria. The hypothesis was formulated as:

> Ho1: A significant relationship exists between collaborative bank e-fraud and customers' reactions in Ado-Ekiti metropolis, Ekiti State, Nigeria.

3. Research Methodology

The study adopted the descriptive cross sectional survey. Primary and secondary data were collected, using quantitative and qualitative methods and information from bank staff, customers, and victims selected from Ado Ekiti metropolis. A sample size of 30 respondents with adequate and informed knowledge about collaborative bank e-fraud and customers' reactions were selected for the study using the snowballing sampling techniques. The study employed the purposive sampling technique to select banks, and the selected banks were WEMA Bank Plc,

First City Monument Bank (FCMB) Plc, Zenith Bank Plc, Guaranty Trust Bank Plc, and Access Bank Plc. The data collected were analysed, using both quantitative and qualitative techniques of data analysis. The quantitative data were analysed using percentage and frequency distribution, while the qualitative data were transcribed verbatim and typed into a computer using a word processor using a descriptive method to interpret the findings.

4.Data Analysis and Discussion of Findings

4.1 Background Information of Respondents

The socio-demographic and economic characteristics such as sex, age, education, occupation and designation of the participants were analysed. First, gender shows that, of the 30 participants selected during the interview, 18 (60.0%) of the participants are males, while 12 (40.0%) are females. Hence, the difference between the male and female participants in this study was due to the availability of the female respondents during data gathering as a result of the snowballing approach to ensure the research meets the timeframe. Second, the ages of the participants range from 20-29 years 6 (20%), 30-39 years 10 (33.3%), and 40years above 14 (46.7%). Participants' educational level indicates that 7 (23.3%) had primary education, 11 (36.7%) had secondary education, while 12 (40%) had tertiary education respectively. Occupation type indicates that 8 (26.7%) were private employees, 9 (30%) were civil servants, while 13 (43.3%) were self-employed. All the participants live within the study area and currently operate a minimum of one bank account. The selection criteria were based on recent report of the most affected victims and banks with highest fraud cases in Nigeria, according to FITC Quarter 2, 2021. The participants, however, consist of some bank officers, customers, and fraud victims who were interviewed to understand their reactions.

4.2 Views on Collaborative Electronic Bank Frauds in Ekiti State

Key informants were asked during the interview section if they are aware of e-banking fraud. Overwhelmingly, all the participants 30 (100%) confirmed they had the awareness of e-fraud through various means; 20 (66.7%) became aware as victims of e-banking fraud and had lost huge but undisclosed amounts of money; 6 (20%) became aware through

various social media platforms, while 4 (13.3%) got awareness of e-banking fraud as bank staff. These were the views of some of the key informants interviewed.

A female interviewee says:

> I got e-fraud awareness when I received a debit alert of [a] huge sum of money from my bank, two days after using my Mastercard at a public ATM machine. I became sceptical and confused. I have [had] to immediately visit my bank and lodge a complaint about the received alert since I never withdrew such a sum. After several checking and cross-checking in the bank, I was told that someone else had access and has [had] taken-over my account to withdrew such a huge sum. I almost fainted and all the bank did was to block the account to forestall further occurrence without recovering my money. The experience was gruesome and unimaginable. (KII Female participant, Civil servant, Aged 45)

Another female interviewee adds:

> My experience with e-fraud was when I suddenly heard a call from a number claiming to be a staff of my bank. The person in question mention my name, account detail, and other vital personal information to show it was from my bank. At this point, I was convinced that the call is [was] from my bank. The voice continued that they are [were] upgrading the banking systems and will [would] equally need to do same to customers' accounts. Hence, customer needs to send the password as soon as possible to enable proper upgrading of the e-payment account, then I was naïve of the situation. So, I immediately complied and few minutes later, I received a debit alert. I tried to call back the number and it was switched off. I was perplexed as I rushed to my bank and narrated my ordeal. I was told that the caller is [was] a fraudster who had phished my account as a result of the information given on the phone, though they immediately blocked the account to prevent another fraud. However, my question is, how did the fraudster got my information without the bank's official knowledge? (KII Female participant, Private employee, Aged 35)

A male interviewee supports:

> I went to the bank to make some withdrawals across the counter but I was directed to use the ATM machine by the cashier. Getting to the machines, there few customers on the queue. Suddenly, a young lad

> offered to be of help, claiming he is [was] next to use the machine. I gave him my detail not knowing that he had ulterior intention within. He truly did help and I appreciated his gesture. Only for me to receive a debit alert a day later. I never imagined such coming from him until proven at the bank that someone had used my account for online transactions and may continue in such act if not immediately blocked. However, my question is that how did the fraudster have such orientation if not from the banks who introduced the e-payment system? (KII male participant, Self-employed, Aged 55)

The key informants were also asked during the interview session to air their views on e-fraud and their responses on collaborative bank e-fraud in Ado Ekiti are presented below where majority of them maintained that some bank officials are not absolutely innocent of e-fraud in Nigerian banks.

A male interviewee supports:

> When my wife account was fraud [sic] due to her careless response to a call claiming to be from her bank. I have no doubt that some dubious bank officials are connected with the [sic] fraudsters to defraud customers, or how do we explain the fact that all customer's financial information kept within the bank got leak to a fraudster? How can the fraudster be that smart in the operation without the bank detecting its operation? At this point, we need to speak out against the financial mishaps going on in many banks as it is affecting the customers a lot. Banks need to monitor the account officers and deny some transact except it is properly ordered by the genuine account holder. (KII Male participant, Self-employed, Aged 50)

Some participants add additional pieces of information on e-fraud perpetrated in banks that lighten the views.

A male interviewee maintains:

> Most times, customer thinks e-fraud is perpetrated by the bank's [sic] staff, since they have access to their banking details. However, most of the customers need to pay more attention to how they use the ATM cards, who they gave it to, how they disseminate their personal banking details, etc. The not too recent reports of e-fraud on customers' show they are most times at fault. One of the victim was fraud [sic] by a relation living with her, another by his son's friend who got the

> information from his innocent son while the last yield to dubious media message that almost took away her life savings. This is not to deny that some culprits may be insiders, but customers need to be very careful. (KII Male participant, Bank employee, Aged 48)

Another male interviewee maintains:

> Banks through media messages and calls should keep orientating their customers on better ways to handle and use the ATM machines and cards. Personal banking information should be kept secret and never be released to anyone even to the bank official on the media and in the banking hall. No bank officer needs to or should have access to your card's password and thus, make it a little bit difficult for any bank officers to defraud a customer once kept properly. However, any dubious person can defraud a customer as soon as they have access to his/her vital financial details. Hence, customers must be very careful on how to hand their information, most especially the card passwords. (KII Male participant, Bank employee, Aged 42).

The key informants were also asked during the interview session to air their views on why banks are not liable for e-fraud committed on the customers' accounts. The participants' responses are captured below:

A female interviewee maintains:

> Banks cannot be liable for any customer's lapses. What the bank can do is to promptly and swiftly respond to stopping and prevent E-Fraud occurrences is to first block the customer E-payment account and later reopen it with customer's new password. However, further investigation may be carried out depending on the gravity to the customer and organisation's interest. All customers need to adhere to banking instruction on e-payment in order not to be a victim let alone think of prevention. (KII Female participant, Bank employee, Aged 42).

Another female interviewee maintains:

> Customer information can be gotten through online surfing, through careless utterances at public and private places, from unreliable relatives, etc. Those that phished customers account are not necessarily bank officials. They may claim to be calling from your bank and give some vital account details gotten through illegal means to carry out their fraudulent acts. However, after subjecting you to being a victim, the numbers can hardly be reached; switched off or not reachable.

> These mobile number calls and messages are in no way connected to the banks. So, customers need to be very aware and be careful about their financial personal details to safeguard their finances because no bank will be liable for their inadequacies. (KII Female participant, Bank employee, Aged 42).

4.3 Views on How to Eliminate or Reduce E-Fraud in Banks in Ekiti State

The participants were asked on how to reduce the prevalence of e-banking frauds in Ekiti State? The participants' views are captured below:

A male interviewee affirms:

> To reduce e-fraud in banks, customers need to adhere to vital instructions about the financial information and never let loose or share with anybody irrespective of the closeness. Banks on the other hand should promptly inform customers through text messages and calls on vital and necessary means on how to curb the ever-increasing fraudulent activities. The bank ICT unit can in turn use their innovative capacity to tackle any noticed fraudulent transactions from all fronts. (KII Male participant, Bank employee, Aged 47)

A female interviewee says:

> The Internet appeals to all ages, ethnics, races and countries…so there's need to embrace the Internet, especially the social media networks, by all customers and bank account operators to reduce their naivety from the widespread attack of the e-fraudsters. Many users are unfortunately unaware of the different threats and dangers associated with the use of the Internet. So, bank staff must be constantly trained while information [should] be passed to the customers on how to identify and prevent e-frauds in banking. (KII Female participant, Civil servant, Aged 47)

A female interviewee reveals:

> Most customers often fall prey to some deceptive adverts, uncensored messages, crafty mails, and unauthorised caller claiming to be from the banks and we end up given [giving] out our vita personal financial details to the delight of e-fraudsters. The banks need to keep orientating customers on how to detect such tricks and create

awareness on how consumers can communicate with relevant authorities in case of any suspected and fraudulent activities. The banks should also maintain good relationship with customers in information dissemination. (KII Female participant, Self-employed, Aged 40)

5. Conclusion

The study concludes that e-banking frauds could be both collaborative and non-collaborative depending on situation and case. Also, the effects on victims are immeasurable; therefore, e-banking frauds need to be tackled timely to reduce and curbed them. Thus, the interests of customers and the banks need to be protected from the claws of e-fraudsters to keep banks in operation and customers in business in Ekiti State, Nigeria.

6. Recommendations

The study recommends the following:

i. Appropriate banks' authority in charge of internal oversight systems must be strengthened in order to identify and stop fraudulent activities including electronic ones on customer assets.
ii. Bank employees should be trained to maintain consumer protection and tighten other e-avenues that could be used by e-fraudsters to swindle bank customers.
iii. Banks should keep orientating customers on how to detect e-fraud tricks and also create awareness on how to communicate with relevant authorities against any suspected fraud.
iv. Customers should adhere to banks' vital financial information and never let loose or share sensitive information with anybody irrespective of their closeness.
v. Banks should use their innovative capacity to tackle and reduce any noticed fraudulent transactions within their domains.

References

Abdullahi, R., & Mansor, N. (2015). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent For Future Research. *International Journal of Academic Research in Accounting, Finance and Management Sciences, 5*. 10.6007/IJARAFMS/v5-i4/1823.

Agwu, M. E. (2014). Reputational Risk Impact of Internal Frauds on Bank Customers in Nigeria. *International Journal of Development and Management Review (INJODEMAR), 9*(1).

Berney, L. (2008). For online merchants, fraud prevention can be a balancing act. *Cards & Payments, 21*(2), 22-7.

Gate and Jacob (2019). Important Drivers for Customer Satisfaction from Product Focus to Image and Service Quality. *Total Quality Management and Business Excellence, 32*(5-6), Pp 1-10. DOI10.1080/14783363.2019.1594756

Idolor, E. J. (2010). Bank Frauds in Nigeria: Underlying Causes, Effects and Possible Remedies. *African Journal of Accounting, Economics, Finance and Banking Research, 6*(6).

Iyodo, B. Y, Agbaji, J. S., & Abu, A. S. (2016). *Consequences of Bank Frauds on the Growth of Nigerian Economy*.

Jegede, A. E. (2014). Cyber Fraud, Global Trade and Youth Crime Burden: Nigerian Experience. *Afro Asian Journal of Social Sciences, 5*(4), Quarter IVV.

Kingsley, A. (2012). Frauds in Nigerian banks: Nature, deep-seated causes, aftermaths and probable remedies. *Mediterranean Journal of Social Sciences, 3*(2), 279-289. 10.5901/mjss. 2012.v3n2.279.

Malphrus Steve. (2009). Perspectives on Retail Payments Fraud *Economic Perspectives, Vol. XXXIII, No. 1*, 2009, p. 6.

Muritala, T. A., Ijaiya, M. A., Afolabi, O. H., & Yinus, A. B. (2020). Fraud and Bank Performance in Nigeria – Var Granger Causality Analysis. *Financial Internet Quarterly, 16*(1).

NDIC (2018). *Nigeria Deposit Insurance Corporation Annual Report of 2018*. https://ndic.gov.ng/wp-content/uploads/2019/09/NDIC-2018-ANNUAL-REPORT.pdf

Nigerian Cybercrimes Act of 2015, Federal Republic of Nigeria.

Nwaimo, S. C. (2020). *Fraudulent Practices in Nigerian Banks: Implications on the Performance of Deposit Money Banks, 1994 -2015*.

Ololade, B. M., Salawu, M. K., & Adekanmi, A. D. (2020). E-Fraud in Nigerian Banks: Why and How? *Journal of Financial Risk Management, 9*, 211-228. https://doi.org/10.4236/jfrm.2020.93012

Olongo, F. O. (2013). *The Effects of Financial Fraud and Liquidity on Financial Performance of Commercial Banks in Kenya*. Published by University of Nairobi School of Business. http://erepository.uonbi.ac.ke:8080/xmlui/handle/123456789/58568

Orji, U. J. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria.

Tilburg Law Review, 24(1), 105–124. DOI: https://doi.org/10.5334/tilr.137

Popoola, A. F., Fakunle, I. O., Omole, I. I., & Oyedeji, O. (2018). Bank Fraud and Its Effect on Nigerian Economy- A Study of Selected Quoted Banks. *European Journal of Accounting, Auditing and Finance Research, 6*(8), 104-120.

Tade, O., & Adeniyi, O. (2017). Automated Teller Machine Fraud in South-West Nigeria: Victims Typologies, Victimisation Strategies and Fraud Prevention. *Journal of Payment Strategy and Systems, 11*(1), 86-92.