Journal of Financial Risk Management, 2020, 9, 211-228
https://www.scirp.org/journal/jfrm
ISSN Online: 2167-9541
ISSN Print: 2167-9533

E-Fraud in Nigerian Banks: Why and How?

Babatunde Moses Ololade[1*], Mary Kehinde Salawu[2], Aderemi Daniel Adekanmi[3]

[1]Department of Accounting and Finance, Elizade University, Ilara-Mokin, Nigeria
[2]Department of Management and Accounting, Obafemi Awolowo University, Ile-Ife, Nigeria
[3]Department of Accounting, Federal University of Oye-Ekiti, Oye-Ekiti, Nigeria
Email: *loladebabs@gmail.com, marysalawu@yahoo.com, adekanmiaderemi2000@mail.com

How to cite this paper: 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

Received: July 14, 2020
Accepted: September 7, 2020
Published: September 10, 2020

Abstract

The advent of the internet and the adoption of e-payment platforms as a convenient means of payment have increased the extent of occurrence of e-fraud and cyber-attacks in Nigerian Banks. The study, therefore, investigated why and how e-frauds are perpetrated in the Deposits Money Banks in Nigeria by employees. The survey research design was adopted. Primary data were sourced from 120 fraud investigation officers in the Banks through the administration of structured questionnaires. Data were analysed using simple percentages. Results revealed that e-frauds were perpetrated by the employees whose employment was threatened as a result of not achieving deposit targets and using either expert or legitimate power to connive with other employees to commit e-fraud against the Banks. Furthermore, findings revealed that job losses were occasioned by disruptive technologies and economic challenges which often lead to employees' disengagement without or little compensation created fear in the mind of employees to commit e-fraud through Phishing, Pharming, and breach of internal checks. The study recommended that unachievable deposits and sales targets should be discouraged in the Banks through our labour laws. Also, the human resources department of the Banks should institute whistleblowing policy that can assist employees to get a reprieve from a supervisor that may want to influence them using any form of power to commit e-fraud. Finally, it was recommended that e-fraud consciousness of the general users of e-payment channels and employees' sensitization on negative consequences of employees' e-frauds should be heightened through frequent education and continuous training.

Keywords

E-Fraud, Cyber-Attacks, Cyber Security and E-Payment Platforms

1. Introduction

The upward swing in the occurrence of e-fraud in the Nigerian business envi-

ronment which ranges from identity theft, phishing, to online security breaches through manipulation of account holders by fraudsters has been a major concern to service providers and users of electronic payment platforms in conducting businesses including the regulators (NDIC, 2018). E-business is the use of internet facilities to connect, facilitate and empower business process activities and effective flow of communication and collaboration within an organisation and organisation with its customers, suppliers, other business stakeholders and the outside world electronically. E-businesses, which is the use of internet and technology to conduct businesses e.g. banking, insurance, brokerage services, sales of goods and service online, collections and conduct of examinations have made the conduct of businesses easy, faster and cost-effective though the fear of losing financial resources may be a reason of not fully adopting the use of e-channels (Salawu & Salawu, 2007; Elumaro & Obaniyi, 2018).

The global adoption of e-payment platforms as preferred means of payment has necessitated the upsurge of e-fraud occurrences in Nigeria. There is an increase in e-fraud occurrences by 33% between 2016 and 2018. Also, the actual amount lost to e-fraud increased by 84% between 2016 and 2018 (NDIC, 2018). The cash-less policy of the Central Bank of Nigeria (CBN) which is meant to reduce the amount of cash in circulation specifically set financial penalties for cash withdrawal above the daily cash limit withdrawal set by CBN for both individual and corporate bank customers. Individuals are meant to pay cash handling fees of 3% while corporate customers are to pay 5% on daily cash withdrawal above ₦500,000 and ₦3,000,000 respectively. Also, many of the Deposit Money Banks (DMB) discourage the withdrawal of cash less than ₦50,000 across the counter. These measures are to encourage the use of e-channels. Meanwhile, closely related with e-payment channels such as Automated Teller Machine (ATM), Point of Sales Terminals (POS), Mobile payment systems, Internet Banking, Smart TV and Electronic Fund Transfer is e-fraud which breeds lack of trust and confidence in the use of the e-payment channels (Hoffmann & Birnbrich, 2012; Tade & Adeniyi, 2017; Elumaro & Obamuyi, 2018). It is the realisations of this challenge associated with e-payment platforms that made the Central Bank of Nigeria set up Nigerian Electronic Fraud Forum (NeFF) to safeguard the integrity of the e-payment platforms and ensure seamless business transactions without fear of losing financial resources through e-fraud. However, the monster of e-fraud continues to range despite this effort. This invariably calls for more scholarly attention on strategies to tame the scourge.

According to Albrecht et al. (2008), the advent of the internet, digital technology revolution, blockchain technology and increase in technology-related products have brought about unprecedented supply of victims and potential perpetrators of e-fraud. Perpetrators of e-fraud are no longer restricted to geographical boundaries as potential perpetrators could be in the Northern part of Nigeria and defraud a victim in the South or outside the country. These potential perpetrators could be employees of Deposit Money Banks (DMB) as well who

stay within the comfort of their offices to con unsuspecting victims of e-fraud of their hard-earned money as indicated in the fraud and forgeries returns of the Deposit Money Banks to Nigeria Deposit Insurance Corporation (NDIC). The NDIC annual reports of 2018 indicated an increase in fraud cases from 26,182 in 2017 to 37,817 in 2018, representing an increase of 44.4%. Besides, the amount involved in the fraud increased significantly by 224% to ₦38.93 billion ($102.4 m at exchange rate of ₦380 to $1) in 2018 from ₦12.01 billion ($31.6 m) in 2017. Similarly, the actual amount lost to fraud incidences increased significantly in 2018 to ₦15.15 billion ($39.9 m) as against ₦2.37 billion ($6.2 m) and ₦2.4 billion ($6.3 m) in 2017 and 2016 respectively. E-payment channels driven by internet and advanced technology are drivers of these frauds and forgeries that were not only perpetrated by outsiders but also the Staff of the banks as 899 Staff were involved in frauds and forgeries in 2018 compared to 320 Staff in 2017 as noted in the NDIC annual report of 2018.

The extant literature consists of studies that have examined and investigated causes of frauds and their prevention strategies from the perspective of outsiders to financial institutions (Johnson et al., 2001; Levi, 2008; Fernandes, 2013) and the perspectives of the victims (Van Dijk & Kunst, 2010; Button et al., 2014; Hoffmann & Birnbrich, 2012; Tade & Adeniyi, 2017) and with little scholarly attention on the investigation of e-frauds from the perspectives of employees. This study intends to fill this gap by looking at why employees of Deposit Money Banks in Nigeria perpetuate e-frauds, how e-frauds are perpetuated and provide preventive measures.

2. Literature Review

2.1. Conceptual Review

Electronic Fraud (e-fraud) is any act designed to exploit others on the internet through deception, usually with an intent to dispossess others of financial resources. Various means through which e-frauds are perpetrated are:

Phishing

The fraudulent practices of sending emails or pop-up web pages purporting to be from legitimate financial institutions to stimulate individuals to provide personal or sensitive business/account information e.g. credit card numbers account information, PINs or passwords which are subsequently used to perpetuate e-frauds through the Web where physical cards are not required to transact businesses.

Pharming

This technique is used in hijacking the web address of a service provider. This occurs when a user types in a Web address and it redirects to a fraudulent Web site without his knowledge or consent. The website will look like the legitimate site to capture unsuspecting victims' cards confidential information e.g. PIN, Cards numbers and Tokens details.

Skimming

It is a fraudulent collection of payment card details using typically a small

electronic device called a skimmer. The device most times is affixed to an ATM or Point-of-Sale terminals and allows e-fraud perpetrators to capture customer's card information including PIN. The advent of wireless technology has made it easier for criminals to remotely download stolen data without physically visiting the terminals.

SIM Swap fraud

This occurs when the phone number of a customer is hijacked through fraudulent SIM replacement at a Telco outlet/agent. The perpetrator then uses the mobile line to access the account of the victim and conduct all banking services including payments for goods and services and transfer of the fund to another account usually via mobile banking.

Account takeover

This takes place when e-fraud perpetrator takes over another person's account, first by gathering personal information about the intended victim through Phishing, Pharming, Skimming or any other fraudulent means and then contact the card issuer (Financial Institutions) while impersonating the genuine cardholder, and asking for a replacement of a lost card. A new card will be issued to the fraudster and through it, the e-fraud perpetrator commits different e-frauds against the victim.

Smishing/Vishing

This takes place when e-fraud perpetrator sends text messages to defraud victims of e-fraud. Often, the text message will contain a phone number to call and once the victims call the number it would provide a ground for the e-fraud perpetrator to ask for confidential information of the unsuspecting victims. Also, it is vishing when the e-fraudsters use the hidden phone number to call the victims for sensitive information. The likely e-frauds associated with e-products of banks in Nigeria are shown in Table 1.

2.2. Theoretical Framework

Theories of Fraud Traingle, Fraud Diamond and Deception are reviewed under the theoretical review as follows:

2.2.1. Fraud Triangle Theory

Fraud Triangle Theory as propounded by Cressey (1953) stated three factors that lead to the commitment of any type of fraud by perpetrators. These are pressures, opportunities and rationalisation. According to Albrecht et al. (2008), the pressures, opportunities and rationalization are assumed but real to e-fraud perpetrators. This theory is relevant to this study because it could be applied to why employees of DMB commit e-fraud in Nigeria. There are financial pressures and non-financial pressures. While financial pressures could be the need to ride a good car, build own house, give good donations in religious organisations to be accorded a high status, provide for immediate and extended family needs, etc., the non-financial pressure could be the need to report better performance at the branch as the branch is profiled as a profit centre, frustration with work and fear

Table 1. E-Products and E-Frauds.

S/N	E-Products	Mode of operations	Likely E-fraud
1	Internet Banking	Financial services are delivered to consumers through the Internet (World Wide Web). Consumers transact their banking services (Payment to third parties for goods and services, confirmation of account balance etc.) through laptops, desktops and mobile devices connected to the internet. The banks provide login details (username, initial password) and physical tokens for transactions' authentications to the consumers.	Phishing through scam email to harvest login details and subsequent bypass of system security through expert and superior knowledge of cybersecurity infrastructure. Wrong account mapping with the intent to commit e-fraud by financial institution employees.
2	Mobile Banking Services (USSD)	These are banking services delivered to customers of DMBs through mobile phone technology. It requires the use of a registered telephone line of the banks' customers at the account opening stage. The GSM line will receive banking transaction alerts and Unstructured Supplementary Service Data (USSD) platform could be used to transfer fund, pay bills, check account balance and request for account statement.	SIM swaps either through theft or in collusion with Telcom agents which will allow the e-fraudster to take over the account from the real owner.
3.	Telephone Banking Services	Banking services are rendered to customers through pre-programmed telephone voice communication. The customers must supply Personal Identification Number (PIN) for authentication. It is mainly used for mainly inquiry on account details.	Theft of Personal Identification Number (PIN) could allow e-fraud perpetrator to gain access to account sensitive details.
4	Electronic (Smart) Card services	These are electronic purses that are preloaded by DMB's customers for making payment and settlement of bills. The card could be used on Automated Machine and Point-of-Sales (POS).	Pharming or Malware to harvest the security features of the card could be launched by e-fraud perpetrators against the victims.
5	Debit/Credit Cards	While debit cards are linked to the account of the customers in DBM, credit cards are linked to the credit account on availment of credit facilities to customers of DMB. They are secured with chip and PIN and could be used on ATM, POS and WEB to carry out banking services.	Pharming and Skimming attacks. Theft of cards and PIN by the insider e-fraud perpetrators. Unsuspecting victims of e-frauds could also be called over the phone for his security details of the cards by e-fraudsters.
6	Web Purchases Services	This is e-payment systems that allow DMB customers to pay for goods and services online through the internet without the use of the physical cards on the websites of the Merchants (Airline operators, supermarkets, Telco operators, Government agencies, Schools etc.). It requires the knowledge of the card numbers, PIN and CVV at the back of the e-cards.	Phishing, Malware, etc. There could also be Theft of cards and PIN by the insider e-fraud perpetrators. Similarly, unsuspecting victims of e-frauds could also be called over the phone for his security details of the cards by e-fraudsters.

Source: Field Survey, 2020.

of job losses because of inability to meet daily or monthly deposit targets and other financial performance indicators set by Management for each of the branch staff. Fear of job losses could also be occasioned by the disruptive technologies that are currently putting pressure on bottom lines of Nigerian banks which frequently stimulated cost reduction strategies through corporate downsizing and restructuring.

Perceived opportunities must be present before the commitment of successful e-fraud by the employees against the organisation. According to Albrecht et al. (2008), an employee or Executive with firm assurance that an act of fraud could not be hidden without the fraud being detected and the perpetrator caught would refrain from coming fraud. Meanwhile, opportunities exist to commit fraud where the perpetrator believes that he or she would not get caught and if caught the consequences is not serious. There could be opportunities to commit

e-fraud where there is weak internal control, lack of consistent job rotation, the concentration of key roles on temporary or contract employees, knowledge of customers' sensitive financial information and account balances, weak cybersecurity infrastructure from where employees can glean security codes of customers, and bypass cybersecurity infrastructure through expertise knowledge etc.

Finally, perceived rationalisation occurs when the perpetrator of fraud rationalize his fraudulent act as being acceptable. For internal e-fraud in Nigerian banks, perpetrators of fraud may rationalise the act of fraud by the thought of "we are not well paid compare to the work that we do, the need to meet our branch performance targets for us to retain our jobs, my family members are sick and they need financial help, my immediate family financial needs is more than my salary, we need to be rich through our smartness" etc.

2.2.2. Fraud Diamond Theory

This was first presented by Wolfe and Hermanson (2004) in the December CPA Journal. In this theory, a fourth dimension named capability was added to the three elements of the Fraud Triangle Theory. This is because without capability it may be seemingly impossible to commit fraud. Therefore, the potential fraud perpetrators must have the skill, be in a position of trust or have the capacity to commit fraud. The theory proposes that an individual's capability, personal trait and abilities could play a major role in determining fraud occurrence (Salawu, 2019).

Wolfe and Hermanson (2004) identified the following features that give fraud perpetrators capability to commit fraud as follows: 1) authoritative position or function within an organisation 2) ability to manipulate the weaknesses of the organisation's internal control system to perpetrate fraud 3) boldness to undertake fraudulent actions with the mind that they will not be discovered and 4) ability to cover up fraudulent activities for a long period to protect being caught.

The fraud triangle and diamond theories are relevant to the study as they provide the theoretical framework that is used to provide explanations on why and how employees of Nigerian banks engage in e-frauds.

2.2.3. Theory of Deception

Deception is often used by a con artist to dispose of a victim of financial resources and valuables in many business negotiations (Schweitzer, 1997). The theory of deception specifies seven operational tactics often used by fraud perpetrators to defraud unsuspecting victims (Grazioli & Jarvenpaa, 2003a, 2003b; Johnson et al., 2001). These tactics are Masking (Hiding or destroying critical information), Dazzling (Disguising critical information), Decoying (Distracting the victim's attention away from critical information), Mimicking (Assuming someone's identity, or impersonating someone else), Inventing (Making up information), Relabelling (Misleadingly presenting information), and Double play (Suggesting to the victim that the victim is taking advantage of the deceiver). Since e-frauds are perpetrated through the internet, con artists find it easy to use

any of the tactics of deception to fraudulently manipulate a victim. This theory is relevant to the study in the sense that internal e-fraud perpetrators will employ any of the seven tactics to either individually commit e-fraud or in collaborations with other employees most especially those with expert and legitimate power relying on his or her expertise knowledge or position of authority.

2.3. Empirical Review

Akinyomi (2012) examined the causes of fraud and its prevention in the Nigeria banking sector and found that employees of Deposit Money Banks engaged in fraud initiation, execution and concealment to enrich themselves at the expense of their customers not minding the collateral damage that such act portends to public confidence and trust in the provision of banking services. The study identified greed as the main cause of committing fraud by both internal and external fraudsters out of the six (6) causes investigated. Also, the study examined eleven (11) types of fraud in the Nigerian banks and found that computer fraud was perceived by 82% of the two hundred (200) respondents as most common with negative consequences of loss of revenue and customers' confidence. However, the study failed to evaluate the reasons and involvement of employees in e-frauds which is the main thrust of this study.

Also, Ibor (2016) investigated the involvement of employees of banks in fraud in Nigeria and the role of human resources in curtailing fraud in the banking sector. Besides, the relationship between the amount of fraud losses and the levels of employees that perpetuated fraud was determined using Ordinary Least Square (OLS) in estimating the secondary data obtained from Nigeria Deposit Insurance Corporation. The study found that 77% of the fraud cases were attributable to insiders while 23% were attributable to outsiders and that the contribution of officers to fraud losses was more than other categories of staff. Meanwhile, the study only determined the extent of involvement of employees in fraud generally without a focus on why employees of Deposit Money Banks commit e-fraud and how they perpetuate e-fraud.

Furthermore, Tade and Adeniyi (2017) examined ATM fraud in south-west Nigeria to determine the factors that are responsible for the susceptibility of victims to ATM frauds and suggesting strategies to prevent the continuous occurrence of ATM fraud. The research design was exploratory as samples of 20 respondents in Lagos and Oyo States, who were mainly victims of ATM fraud were obtained through snowballing sampling technique. The qualitative data gathered through in-depth interview were analysed using content analysis. The study found that illiteracy, ill-health and trust of relatives including children, friends, and lovers were factors that are responsible for victims falling into the victimisation strategies of the fraudsters that used swapping of ATM card, card cloning, use of physical attacks during odd hours withdrawal (gun threats) and demobilizing the victims through the seizure of their mobile phones to commit frauds. The study recommended fraud prevention strategies which are: stringent penalty

for culpable staff, continuous education and enlightenment of banks' customers and improvement in staff welfare. The study concentrated on ATM fraud without taking into consideration other e-fraud that are perpetrated in the Nigeria banks. Besides, the possible involvements of employees of the banks are not taking into consideration as the study restricted fraudsters to relatives, friends and lovers of the victims. This is a gap in the literature that this study fills.

Finally, Elumaro and Obamuyi (2018) investigated the relationship between card frauds and customers' confidence in alternative banking channels (e-channels) in Nigeria and found a negative relationship between the two. This is because e-fraud breeds uncertainty in the financial ecosystem and subsequently leads to lack of trust in the alternative banking channels. This will result in the avoidance of e-channels by the public. The study recommended collaborations among the banks and their regulatory agencies to nib at the bud card frauds occurrences. The findings of Elumaro and Obamuyi also conformed with that of Hoffmann and Birnbrich (2012) who asserted that victims of card frauds' confidence and trust in using alternative banking platforms to conduct their business transactions become shaken with a perception that the e-platforms are not safe for their financial transactions. This study is different from the study of (Elumaro & Obamuyi, 2018) in that it focuses on why and how employees of Deposit Money Banks (DBM) commit e-fraud rather than the effect of e-fraud on customers' confidence to use alternative banking channels which is the focus of Elumaro and Obamuyi (2018).

3. Methodology

The survey research design was adopted for the achievement of the objectives of the study which are to investigate why and how employees of DMBs in Nigeria perpetrated e-fraud and proffer possible e-fraud prevention measures that would curtail the scourge within the financial ecosystem. Primary data for the study was gathered through the administration of a structured questionnaire from one hundred and twenty (120) respondents who are e-fraud investigation officers of the 27 DMBs in Nigeria. The questionnaire was self-designed based on the theories of Fraud Triangle, Fraud Diamond and Deception. The researchers' general knowledge of the industry also contributed to the design of the questionnaire based on theoretical postulations of Cressey (1953), Wolfe and Hermenson (2004) and Albrecht et al. (2008). The sample of the respondents was selected through stratified and purposive sampling techniques.

One hundred respondents were taken from top ten (10) DMB where 96% of the e-fraud in the Nigerian banks were perpetrated while twenty (20) respondents were taken from the remaining seventeen (17) DMB where 4% of the e-fraud perpetrated in the Nigerian banks occurred. The questionnaires were administered through email to the respondents and one hundred and two (102) well completed questionnaires were returned and considered appropriate for analysis because they were all completed by e-fraud and cybersecurity profes-

sionals that had once carried out extensive investigation on e-fraud perpetrated by outsiders and employees. Data gathered were analysed using simple descriptive statistics.

The research instrument was reviewed for validity by cybersecurity consultants and their comments were reflected in the final draft of the questionnaire which was pre-tested on four e-fraud investigation officers in a branch of one of the Deposit Money Banks. The Cronbach result obtained was 87% which showed that the research instrument is reliable.

4. Results and Discussions

4.1. Demographic Analysis of the Respondents

The respondents are well-knowledgeable experts in e-fraud investigations, preventions and computer systems security. They are directly responsible for investigating e-frauds involving outsiders and employees in their respective banks. Table 2 shows the demographic analysis of the Respondents concerning their age, education and professional background and years of experience in e-fraud investigation.

The respondents' age group is majorly less than 25 - 45 as 78% of the respondents are in this age group. This is considered satisfactory as respondents born in the digital age are well presented. Similarly, those within the age group of 46 - 55 (12%), and above 56 years (10%) complemented the sample population. The respondents with post-graduate certification are 68% while those with first degree without any post-graduate certification are 32%. Moreso, all the respondents regardless of their academic background have different professional certifications that aided them in e-fraud investigation. In terms of years of experience in e-fraud investigation, 68% of the respondents have experience of 10 - 20 years, 10% of the respondents have between 5 - 9 years of experience while 22% have experience of more than 20 years in e-fraud investigation.

4.2. Analysis of Respondents' Responses to Why Employees of Deposit Money Banks (DMB) Engage in E-Fraud

Table 3 shows the analysis of the respondents' responses on why employees of Deposit Money Banks commit e-fraud. While 94% of the respondents agreed that financial pressures from relatives, friends and religious bodies to whom employees belong to exert pressure on them to commit e-fraud, 6% of the respondents disagreed. The general perception of many people in Nigeria is that employees of Deposit Money Banks have much money at their disposal and in a vantage position to get access to money than everyone else. This accounts for why the employees are the first point of call to relatives, friends and religious bodies for meeting their financial needs.

Fear of job losses because of the inability to meet daily deposit or financial targets set by management and frequent corporate downsizing in the industry because of disruptive technologies and dwindling economies were surveyed.

Table 2. Background information of the respondents.

	Background Characteristics	Number	%
Age Groups	<25	15	15%
	25 - 35	42	41%
	36 - 45	23	22%
	46 - 55	12	12%
	>56	10	10%
Highest Education	HND	08	8%
	B.Sc./B. A	24	24%
	HND & Masters	11	11%
	B. Sc/B. A & Masters	53	51%
	B.Sc/B. A/Masters & Ph.D.	06	06%
Professional Affiliation	ACA/ACCA	12	12%
	CISA	32	32%
	ACFE	29	28%
	CISSP	13	13%
	CRISC	16	15%
Years of experience in e-fraud investigation	5 - 9 years	10	10%
	10 - 15 years	53	51%
	16 - 20 years	17	17%
	>20 years	22	22%
	Total	**102**	**100%**

Source: Field Survey, 2020.

Table 3. Respondents' Analysis of why employees of DMB commit e-fraud.

S/N	Statements	Strongly Agree	Agreed	Disagree	Strongly disagree
1	Financial pressure from family, relatives, friends, club and religious body membership induce employees to commit e-fraud.	76 (75%)	20 (19%)	6 (6%)	
2	Employees whose Job are threatened because of inability to meet daily or monthly deposit targets and other performance indicators set by Management commit e-frauds.	66 (65%)	23 (22%)	11 (11%)	2 (2%)
3	Lack of career progression as a result of ineffective staff promotion policies which resulted in a staff spending more than six (6) years in a grade stimulate e-fraud occurrences.	45 (44%)	34 (33%)	19 (19%)	4 (4%)
4	Staff dissatisfaction arising from being a temporary or contract staff without any hope of being upgraded to permanent staff result in the commitment of e-fraud.	81 (80%)	7 (7%)	6 (6%)	8 (7%)
5	Frequent downsizing and corporate restructure which accounted for staff being relieved of their job with little or no entitlement create fear that often leads to e-fraud by employees.	56 (55%)	32 (31%)	14 (14%)	
6	Abuse of privileged position because of access to customers' sensitive information e.g. card details accounts for employees e-fraud.	78 (76%)	6 (6%)	18 (18%)	
7	Greed induces e-frauds by employees.	53 (52%)	43 (42%)	6 (6%)	

Source: Field Survey, 2020.

While 87% of the respondents agreed that fear of job losses occasioned by the inability to meet deposits targets and other performance indicators set by Management made employees commit e-fraud, 86% of the respondents agreed that fear of job losses or job insecurity arising from incessant corporate downsizing which throws employees into the job market without terminal benefits induced employees to commit e-fraud. According to Albrecht et al. (2008), this fear may not be real but very real to the perpetrator of e-fraud.

Similarly, frustration coming from staying too long on a grade (6 years and above) without progression in career path was identified as a reason why employees of Deposit Money Banks commit e-fraud as 77% of the respondents agreed to this fact while 23% of the respondents disagreed. All the Deposit Money Banks use contract or temporary staff in their operations. The contract or temporary staff have a least a year contract with the option of annual renewal subject to satisfactory performance. 87% of the respondents agreed that the use of contract or temporary staff creates employees' dissatisfaction that leads to commitment of e-fraud while 13% of the respondents disagreed.

Furthermore, 82% of the respondents agreed that abuse of privilege position of the DMBs employees as intermediaries between depositors and borrowers which enable them to have access to customers' sensitive financial information induce employees to commit e-fraud while 18% disagreed. The employees are in a fiduciary position which makes customers and potential customers divulge sensitive information to them. However, abuse of this position of trust leads to the commitment of e-fraud. The Fraud Diamond Theory as presented by Wolfe and Hermanson (2004) is very relevant here to explain that employees of banks develop the capability to commit e-fraud as a result of the fiduciary and intermediary positions they occupy in the deployment of financial resources from the deficit units to surplus units of the economy.

Finally, greed on the side of employees of Deposit Money Banks is equally identified as a reason for a commitment of e-fraud as 94% of the respondents agreed that greed to acquire unnecessary personal assets and effects make employees of DMB to engage in e-fraud while 6% of the respondents disagreed. This is in line with the findings of Akinyomi (2012) which identified greed as the main reason why employees of banks commit fraud.

4.3. Analysis of Respondents' Responses to How Employees of Deposit Money Banks (DMB) Perpetrate E-Fraud

In a bid to boost revenue, bottom lines and enhance the use of e-cards for earning e-products fees, some DMB engage in massive production of e-cards for their customers without the customers' authorisations meanwhile customers' account would have been debited for ₦1000 being the cost the cards (One of the authors received a debit alert from his bank for e-card he never requested for during this study). This resulted in an opportunity to commit e-fraud in the DMB as 95% of the respondents agreed that employees steal customers' e-cards and PIN, most especially those produced without the consent of the customers

to perpetrate e-frauds.

In the same vein, 61% of the respondents agreed that employees of the DMBs with knowledge of the sensitive financial information do call customers to obtain their account details, card numbers and PIN to commit e-fraud while 39% of the respondents disagreed. This may have been the reason one of the authors received an SMS alert from his banker during this study which states that: "Dear customer, we will never ask you for your account details, full card number, or BVN via telephone, emails or SMS. Please be cautious".

Besides, through breach of operational policies of dual custody of e-cards, PIN and physical tokens, employees of DMBs commit e-fraud as 73% of the respondents agreed that employees e-fraud were carried out because of breach of operational guidelines most especially dual custody of e-channels tools (e.g. Physical tokens, e-cards and PIN). Also, 81% of the respondents agreed that employees of DMBs engaged in sending unsolicited emails (Phishing) to unsuspecting victims of e-fraud which are often used to harvest the personal account details of customers to commit e-fraud while 19% of the respondents disagreed. These positions agreed with the findings of Akinyomi (2012) and Ibor (2016) that employees of banks are also behind e-frauds perpetrated in the banking industry in Nigeria.

Unauthorized debit to customers' accounts are carried out by employees of DMBs after gaining control of customers' accounts through (Phishing, Smishing and Vishing) or carrying out unauthorized alterations on the account set up in the system. 74% and 87% of the respondents agreed that through internal collusion, employees of DMBs do carry out unauthorised alterations and unauthorised debits respectively on customers' account to commit e-frauds. However,

Table 4. Respondents analysis of how employees of DMBs commit e-fraud.

S/N	STATEMENTS	Strongly Agree	Agreed	Disagree	Strongly disagree
1	Stealing of customers' cards and PIN that are produced without the customers' consent by the DBMs to generate more revenue.	85 (83%)	12 (12%)	5 (5%)	
2	Bank Staff personally call customers with good deposits to obtain their PINs and Card details or secret codes on the pretence of assisting them to set up their accounts properly.	39 (38%)	23 (23%)	26 (25%)	14 (14%)
3	Breach of dual custody of customers' Cards and PIN which allow the perpetrator to commit e-fraud.	56 (55%)	18 (18%)	28 (27%)	
4	The unauthorised alteration of the account details to use the account for fraudulent transaction through internal collusion. E.g. altering the mobile number to carry out authorised debit without the customer being alerted through SMS alert.	62 (61%)	13 (13%)	20 (19%)	7 (7%)
5	Sending unsolicited mails to customers to obtain their cards personal details and PIN for e-fraud.	59 (58%)	24 (23%)	19 (19%)	
6	Taking control of the customers' account after gaining access to sensitive information and thereby effect unauthorized debit transactions on customers' account.	76 (75%)	13 (12%)	10 (10%)	3 (3%)
7	Security experts in the system use their expert and legitimate power to co-opt other staff to commit e-fraud.	65 (64%)	24 (23%)	13 (13%)	

Source: Field Survey, 2020.

26% and 13% of the respondents disagreed on these assertions respectively.

Some employees in supervisory roles and with either technical or expertise knowledge do co-opt other employees to commit employees e-frauds as indicated by 87% of the respondents who agreed that there is the use of expertise and legitimate power to commit e-fraud. This often occurs when a supervisor uses his or her legitimate power to breach operational guidelines without being questioned by his or her subordinates and where employees with high Information Computer Technology (ICT) skills request co-employees to do a task in the course of discharge of his job responsibilities that eventually amount to e-frauds.

5. Conclusion and Recommendations

E-frauds in Nigerian banks are not only committed by outsiders but also by the employees of the Deposit Money Banks and this call for caution on the side of all users of e-products anytime they have dealings with their banks. The reasons employees commit e-frauds could be classified into two which are financial pressure and non-financial pressure. Financial pressure could be from relatives, friends and religious organisations the employees belong to who often demand that employees of banks should give them money to meet their personal and operational needs. Also, financial pressure could arise from the employees aspiring to acquire personal effects whose costs are above his or her income. Non-financial pressure arises from fear of job losses or job insecurity occasioned by the inability to meet unreasonable financial targets (Deposits, Credit facilities etc.) set by Management and disruptive technologies that often instigate corporate downsizing and restructuring. Besides, employees' dissatisfaction and frustration because of being used as a contract or temporary staff and staying too long on a grade without hope of career progression are non-financial pressure that becomes real to employees to commit e-frauds.

Apart from Phishing, Smishing and Vishing, employees of banks also collude together to carry out authorised debit and alternations to customers account as a means of committing e-fraud. Furthermore, legitimate and expertise power are used to co-opt other employees to commit e-frauds against the organisations and customers.

The study recommended that DMB's Management should on weekly basis sensitive the employees on negative consequence of e-frauds committed by employees as a destroyer of trust which is the foundation on which banking business and their employment stand. Also, Management of DMB should prosecute culpable employees that engage in e-frauds and do away with bogus and unreasonable financial targets often set for employees. Besides, Management of Deposit Money Banks should discontinue the use of temporary or contract employees in their operations. Employees should be treated very well even in the event of unavoidable corporate downsizing. Furthermore, internal control mechanisms should be strengthened through whistleblowing to prevent breach of operational policies and assisting junior employees from falling into the trap of le-

gitimate and expertise power of their supervisors.

Finally, National Assembly Committees on Labour and Productivity in Nigeria should introduce a bill to accommodate how employees of DMB whose employment would be terminated because of unavoidable corporate downsizing should be compensated for job losses by their employers in the 21st Century. This will ease off tension and pressure of employees that presently work under intense uncertainties of job security to participate in e-fraud in the Deposit Money Banks.

Suggestion for Further Studies

The present study only focuses on e-fraud from the perspectives of employees of banks without taking into consideration the Executive Management employees' e-frauds which also exist in the industry. Also, the strengths and weaknesses of regulatory framework to prevent e-fraud and stimulate customers' confidence and financial inclusion were not assessed.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Akinyomi, O. J. (2012). Examination of Fraud in the Nigerian Banking Sector and Its Prevention. *Asian Journal of Management Research, 3,* 184-192.

Albrecht, C., Albrecht, C. C., Wareham, J., & Fox, P. (2008). The Role of Power and Negotiation in Online Fraud. *Journal of Digital Forensics, Security and Law, 1,* 29-48.

Button, M., Lewis, C., & Tapley, J. (2014). Not a Victimless Crime: The Impact of Fraud on Individual Victims and their Families. *Security Journal, 27,* 36-54. https://doi.org/10.1057/sj.2012.11

Cressey, D. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Glencoe, IL: Free Press

Elumaro, A. J., & Obamuyi, T. M. (2018). Cards Frauds and Customers' Confidence in Alternative Banking Channels in Nigeria. *European Scientific Journal, 14,* 40-60. https://doi.org/10.19044/esj.2018.v14n16p40

Fernandes, L. (2013). Fraud in Electronic Payment Transactions: Threats and Countermeasures. *Asia Pacific Journal of Marketing and Management Review, 2,* 23-32.

Grazioli, S., & Jarvenpaa, S. L. (2003a). Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence. *International Journal of Electronic Commerce, 7,* 93-118. https://doi.org/10.1080/10864415.2003.11044283

Grazioli, S., & Jarvenpaa, S. L. (2003b). Deceived: Under Target Online. *Communications of the ACU, 46,* 196-205. https://doi.org/10.1145/953460.953500

Hoffmann, A. O., & Birnbrich, C. (2012). The Impact of Fraud Prevention on Bank-Customer Relationships: An Empirical Investigation in Retail Banking. *International Journal of Bank Marketing, 30,* 390-407. https://doi.org/10.1108/02652321211247435

Ibor, B. (2016). An Investigation of Human Resources Nexus to Frauds in the Nigerian Banking Sector. *International Journal of Scientific and Research Publications, 6,*

231-247.

Johnson, P. E., Grazioli, S., Jamal, K., & Berryman, R. G. (2001). Detecting Deception: Adversarial Problem Solving in a Low Base-Rate World. *Cognitive Science, 25,* 355-392. https://doi.org/10.1207/s15516709cog2503_2

Levi, M. (2008). Organised Fraud and Organising Fraud: Unpacking Research on Networks and Organisation. *Criminology & Criminal Justice, 8,* 389-419. https://doi.org/10.1177/1748895808096470

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

Salawu, R. O., & Salawu, M. K. (2007). The Emergence of Internet Banking in Nigeria: An Appraisal. *Information Technology Journal, 6,* 490-496. https://doi.org/10.3923/itj.2007.490.496

Salawu, R. O. (2019). Fraud Detection and Prevention: The Role of the Reporting Company and the External Auditors. In *Candido Da Rocha Memorial Lecture during the 8th Convocation Ceremonies for the Award of Postgraduate, First and Honorary Degrees of Osun State University* (pp. 1-55). Osogbo: UNIOSUN Printing Press.

Schweitzer, M. E. (1997). Omission, Friendship, and Fraud: Lies about Material Facts in Negotiation. In *Annual Meeting of Academic Management*. Boston. https://doi.org/10.1037/e683282011-011

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,* 1-7.

Van Dijk, J. J. M., & Kunst, M. J. J. (2010). E-Fraud: Exploring Its Prevalence and Victim Impact. *International Journal of Victimology, 8,* 8.

Wolfe, D., & Hermanson, D. R. (2004). The Fraud Diamond: Considering Four Elements of Fraud. *The CPA Journal, 74,* 38-42. https://doi.org/10.1016/S1361-3723(04)00065-X

Appendix 1. E-Fraud in the Nigerian Banks: How and Why

QUESTIONNAIRE

Dear Sir/Madam,

This questionnaire is designed to elicit information on why and how employees of Deposit Money Banks in Nigeria commit e-fraud against their customers. The sole purpose of the research is to support the safety of the financial ecosystem and sustainability of confidence of users of e-payment channels in Nigeria. The research is purely for academic purpose and information so gathered shall be treated confidentially in line with research code of ethics.

SECTION A: PERSONAL DETAILS

Please kindly tick (✓) the appropriate response to the statements below:

1. Sex (a) Male ( ) (b) Female ( )
2. Marital Status: (a) Married ( ) (b) Single ( ) (c) Divorced ( )
3. Age: (a) under 25 ( ) (b) 25 - 35 ( ) (c) 36 - 45 ( )
   (d) 46 - 55 ( ) (e) 56 and above ( )
4. Educational Qualification: (a) HND ( ) (b) BSc/BA/PGD ( )
   (c) MBA/MSc/MA/M.Phil. ( ) (e) Ph.D. ( )
5. Professional Qualification: (a) CISA ( ) (b) ACA/ACCA ( ) (c) ACFE ( )
   (d) CISSP ( ) (e) CRISC ( ) (f) Specify others ----------
6. Year of Experience in E-Fraud investigation
   (a) 5 - 9 years ( ) (b) 10 - 15 years ( )
   (c) 16 - 20 years ( ) (d) 21 years and above

SECTION B: Why Employee of Deposit Money Banks commit e-fraud?

S/N	STATEMENTS	Strongly Agree	Agreed	Undecided	Disagree	Strongly disagree
1	Financial pressure from family, relatives, friends, club and religious body membership.					
2	Fear of Job losses because of inability to meet daily or monthly deposit targets and other performance indicators set by Management.					
3	Lack of career progression as a result of ineffective staff promotion policies which resulted in a staff spending more than three (3) years in a grade before promotion.					
4	Staff dissatisfaction arising from being a temporary or contract staff without any hope of being upgraded to permanent staff.					
5	Frequent downsizing and corporate restructure which accounted for staff being relieved of their job with little or no entitlement.					
6	Abuse of privileged position because of access to customers' sensitive information e.g. card details.					
7	Greed induces e-frauds by employees.					

SECTION C: How Employees of Deposit Money Banks commit e-fraud?

S/N	STATEMENTS	Strongly Agree	Agreed	Undecided	Disagree	Strongly disagree
1	Stealing of customers' cards and PIN that are produced without the customers' consent by the DBMs to generate more revenue.					
2	Bank Staff personally call customers with good deposits to obtain their PINs or secret codes on the pretence of assisting them to set up their accounts properly					
3	Breach of dual custody of customers' Cards and PIN which allow the perpetrator to commit e-fraud.					
4	The unauthorised alteration of the account details to use the account for fraudulent transaction through internal collusion. E.g. altering the mobile number to carry out authorised debit without the customer being alerted through SMS alert					
5	Sending unsolicited mails to customers to obtain their cards personal details and PIN for e-fraud					
6	Taking control of the customers' account after gaining access to sensitive information and thereby effect unauthorized debit transactions on customers' account.					
7	Security experts in the system use their expert and legitimate power to co-opt other staff to commit e-fraud					

SECTION D: What are the preventive measures of employees' e-fraud.

S/N	STATEMENTS	Strongly Agree	Agreed	Undecided	Disagree	Strongly disagree
1	Cards and PIN should be produced on confirmed customers' requests					
2	Telecommunication companies should enforce SIM security through passwords					
3	Setting of unachievable targets to staff should cease.					
4	DMBs should discontinue the use of contract staff					
5	Due background check should be conducted on every employee before recruitment					
6	Staff caught should not only be dismissed but also prosecuted.					
7	Sharing of fraud investigation reports with regulatory agencies and all stakeholders.					

Section E: Others.

1. Who are mainly the victims of e-fraud in your Bank?
   (a) Illiterate customers ( ), (b) Educated and not financial literate customers ( ),
   (c) Educated and financial literate customers ( )
2. What in your opinion are the reason why employees of Financial Institutions engage in e-fraud?

3. How do the employees of financial institutions commit e-fraud judging by your experience?

---

4. In what ways do you think that the e-fraud perpetrated by employees of financial Institution of prevented?

Appendix 2. List of Top 10 Deposit Money Banks and Others

S/N	Name of Deposit Money Bank
1	Access Bank Plc
2	First Bank of Nigeria Ltd.
3	First City Monument Bank Plc
4	Fidelity Bank Plc
5	Eco Bank Nigeria Plc
6	Guaranty Trust Bank Plc
7	Stanbic IBTC Bank Plc
8	United Bank for Africa Plc
9	Union Bank Plc
10	Zenith Bank Plc
	Others
1	Citibank Nigeria Ltd.
2	Coronation Merchant Bank Ltd.
3	FSDH Merchant Bank Ltd.
4	FBN Merchant Bank Ltd.
5	Jaiz Bank Plc
6	Heritage Banking Company Ltd.
7	Keystone Bank Ltd.
8	Providus Bank Ltd.
9	Rand Merchant Bank Ltd.
10	Polaris Bank Ltd.
11	Standard Chartered Bank Ltd.
12	Globus Bank
13	Sterling Bank Plc
14	SunTrust Bank Plc
15	Unity Bank Plc
16	Wema Bank Plc
17	Nova Merchant Bank