Journal of Psychology and Behavioural Disciplines, COOU, Vol. 2, No 3, December 2022.
Published by Psychology Department, Chukwuemeka Odumegwu Ojukwu University (COOU), Anambra State, Nigeria.
ISSN (PRINT): 2814-3183: e-ISSN (ONLINE): 2955-0572

COPING WITH ORGANIZATIONAL DIGITAL FRAUD: THE NIGERIAN EXPERIENCE

Udeme Offiong
Unity Bank Plc,
Abakaliki, Ebonyi State, Nigeria
Email: uoffiong3@gmail.com; Phone: +2348036437383

ABSTRACT: *Digital fraud is ravaging organizations world over and Nigerian financial organizations are no exception. Nigeria has evolved from the days of cheque transactions to electronic payment plat forms, this gave rise to the maladaptive behavior (Digital fraud). The collected its Data its data from the Nigerian Interbank settlement system Plc (NIBSS). The study sought to know which channel digital fraud is more perpetuated and also sought to know how digital fraud could be reduced to its barest level. At the end of reviewing the Secondary data, it was discovered that WEB based digital fraud was most prevalent in Nigeria from 2019 to Q3 2020, this was as result of the Covid 19 pandemic that ravaged countries world over and company resorted to Web based transactions more. The researcher recommended users education, deployment of fraud solutions, introduction of biometric identification system, complete and accurate reporting of fraud, strengthening the international gateway.*

KEYWORDS: Coping, Organizational, Digital Fraud

INTRODUCTION

Corruption and fraud are menace all around the world with the increase in the use of internet web technologies in carrying out financial transactions; this has also heightened fraudulent practices around financial organizations around the globe. Big organizations have been crumbled by activities of fraudsters. The activities of fraudsters rubbish the work of auditors as it is expected that auditors should see and report the activities of fraudsters before it occurs (NDIC, 2018). Showed that the upward swing in the occurrence of fraud in Nigeria business environment which ranges from identity theft, phishing, to online security breaches through manipulations of account holders by fraudster has been a major concern to service providers and users of electronic payment platforms in conducting businesses including the regulators.

The acceptance, globally of e-payments platforms as the preferred means of financial transactions (payments and purchases) in Nigeria has therefore increased the incidences of e-fraud in Nigeria. The actual amount lost to e-fraud increased by 84% between 2016 and 2018 (NDIC, 2018).

The introduction of the CBN (Central Bank of Nigeria) cashless policy where individuals are meant to pay as penalty of 3% while corporate customers pay 5% on withdrawals daily above ₦500, 000 and ₦3, 000,000 respectively has suffered some setbacks due to lack of confidence that customers have to pull transactions through platforms such as ATM, POS, (Point of Sale) and other mediums. This reason necessitated the establishment of NEFF (Nigerian Electronic fraud forum) by the central Bank of Nigeria to safeguard the integrity of e-payment platforms in Nigeria.

Ademiyi (2004) and Ican (2006) defined fraud as an international act by one or more individuals among management employees or third parties, which results in a misrepresentation of financial statements. Fraud can be seen as the intentional misrepresentation, concealment or omission of the truth for the purpose of deception or manipulation to the financial detriment of an individual or an organization.

According to Albrecht et al (2008), the advent of the internet, digital technology revolution, block chain 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 geo graphical 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

ISSN (PRINT): 2814-3183: e-ISSN (ONLINE): 2955-0572

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.

As banking procedures and processes evolves, fraudsters also evolve changing their own mode of operation. The most affected person in the fraud situation is the person that loses his or her funds (customers). The introduction of Technology based payment systems has done a lot to increase security, the convenience of bank customers, staff as well as the society at large (Kelvin, 2012). Recently paying and getting money between buyers and sellers are not necessarily transacted trough raw cash, transactions have increased in volumes and profitable. Nigeria economy has also been projected to the world through this adoption of online real-time transactions through ATM (Automated Teller Machine), internet or web, point of sale (POS) terminal.

All these have made Nigeria key into Electronic transaction. Electronic transactions refer to financial transaction that are often initiated through the use of a computer terminals, online banking automated phone system or other methods of electronic funds transfer. According to (Amaefule, 2012) the term electronic transaction refers to the application of information and communication technologies, online and computerized based sector in business transactions.

As electronic transactions grow and more banking activity extends to the ATM, internet which also includes embezzlement, theft or any attempt to steal or unlawfully obtain misuse or harms the asset of the organization, (Adeduro, 1998).Or web, POS, mobile devices the ability to detect and prevent financial crimes reduce fraud risk exposure therefore becomes critical. 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; Fernandez, 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 how e- fraud grew in Nigeria preventive measures.

Statement of Problem

Due to the prevalence of e-fraud in Nigerian financial organizations in Nigeria amidst effort by Central Bank of Nigeria in curbing this menace by setting up NEFF (Nigerian Electronic fraud forum) to check the integrity of electronic platforms, this monster or menace still exist greatly. It is on this backdrop that this study is embarked by the researcher to finding out improved ways in checkmating e-fraud in Nigeria and educating the general public on E- fraud strategies.

Purpose of Research

Owing to the alarming rate of e-fraud and the importance that e-platform play in our day to day financial transactions. The following purposes:

1. To help in educating financial organization on new measures used in combating e-fraud.
2. To unearth the impact e-fraud has to individuals, organizations and the country at large.

Research Question

This study is carried out to answer the following research questions:

1. What e-channels do fraudsters perpetrate fraud through more in Nigeria?
2. What are the impacts that e-fraud has on customers and organizations in Nigeria?

Significance of Study

A wide array of literatures shows studies that have investigated causes of fraud and their preventive ways without stressing security measures deployed by financial organizations in curbing digital fraud. This solution is artificial intelligent driven. With this study financial organizations will learn to secure payment platforms in Nigeria.

LITERATURE REVIEW

Theoretical Framework

Fraud Triangle Theory: An American Criminologist by name Cressey Donald 1953

ISSN (PRINT): 2814-3183: e-ISSN (ONLINE): 2955-0572

developed the fraud triangle theory model where he explained that in most incidences of framed. These three factors are always present hence the need for this postulation. Below are the three characteristics behind most frauds.

1. Perceived financial need (Greed-motivation)
2. Perceived Opportunity
3. Rationalization/Justification

Decomposed Theory of Planned Behavior: This theory shows that fraud is the intentional theft, diversion or misappropriation of assets. These assets include, but are not limited to cash, equipment, supplies, salvage and software intellectual property. The theory assumes that a person's behavior is determined by the person's behavioral intention to perform it and the intention itself is determined by the person's attitudes and his or her subjective norm towards the behavior.

Theory of Reasoned Action (TRA): This theory originates from social psychology developed by Ajzen and Fashbein (1975). This theory was developed to establish the link between beliefs, attitudes, norms, intentions and behaviors of individuals in their intentions to use ICT. The theory suggests that human behavior is controlled by personal attitudes, but also by social pressure and a sense of control. Experts agree that any type of frauds and other unethical behaviors often occur due to an individual's lack of personal integrity or other moral reasoning (Aorminey, Fleming, Kranacher & Riley, 2012); (Rae & Subramaniam, 2008), as moral and ethical norms play an essential role in an individual's decision and judgement. But environmental circumstances that provides opportunities for exploitation is also a contributory factor.

Conceptual Review

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

Overview of fraud/e-payment frauds Digital frauds are frauds committed on the digital/e-payment space. They are internet or web based. The global adoption of e-payments 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).

Digital fraud (e-fraud) is any act designed to exploit others on the internet through the act of deception, usually with the intent to dispose other people of financial resources this is achieved through different means.

Phishing: This is the fraudulent practice of sending emails or pop up web pages pretending to be from legitimate financial institution to arouse the individual interest in providing personal or sensitive business information/account information e.g. credit card information, PINS, passwords, which are used to perpetrate digital or e-frauds through the web were you don't need physical curds to transact business e.g. payment platforms.

Pharming: This fraud technique involves hacking the web address of a service provider. In this fraud, a web user types a web address and he or she will be directed to a fraudulent who site without his or her knowledge. When victims do not suspect, they release confidential information such as PIN, cards, numbers and token details.

Skimming: This is a fraudulent collection of payment card details using typically a small electronic device called a skimmer. In most cases this device is fixed to an ATM or point of sale terminals. This allows fraudsters the opportunities to capture customer's card information including pin. This information will now download this information through

wireless means and then use it for fraudulent transactions.

SIM Swap Frauds: This occurs when the phone number of a customer is taken unauthorizing through telecommunication outlet or agent. When this is done, the fraudster uses the mobile line to access the account of the victim and begins to conduct banking transaction without the knowledge of the victim. In some cases, pays for goods and services. Also, transfers will also be made to other accounts.

Account Takeover: This is the fraudulent process an e-fraudster takes over another person's account by gathering information about the person through the other fraud means such as phishing, pharming, skimming impersonating the original card holder by asking for another card from the financial institution requesting for card replacement. When a new card is issued, he uses it to commit fraud against his victims. This usually comes with insider in the financial institution.

Smishing/Vishing: This technique involves the fraudsters sending text messages to victims including a phone number to call, when such calls are made the victim now divulges all the sensitive information about his or her account information to the fraudster and this is used in turn to defraud the victim.

METHOD

Participants: Information from this study is derived from secondary data. The primary data source was from Nigerian Interbank Settlement system (NIBSS).

Instrument: The researcher used NIBSS holistic bank fraud report from 2018 to Q3 of 2020.

Procedure: The procedure used in this research was to get NIBSS report of 2018 up to Q3 2020. It was downloaded from NIBSS website. Based on this report the researcher was able to put the data on bar and pie charts as represented in the discussion section.

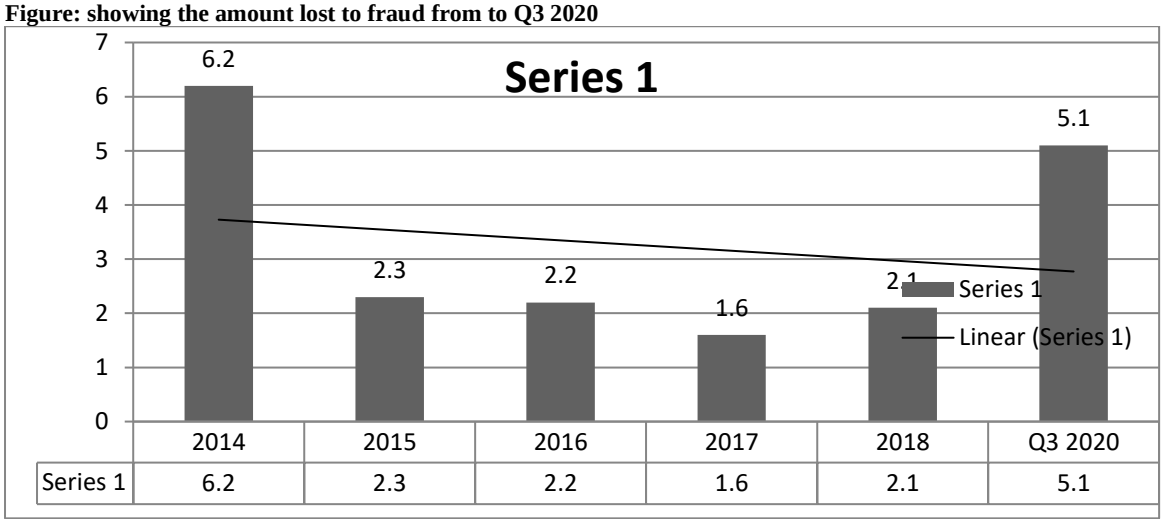
Design/ Statistics: The research adopted descriptive design. This research is a narrative research data gotten from the NIBSS (Nigerian Interbank Settlement System) report. The data were represented on the bar chart, pie chart and tables. This makes descriptive statistics the appropriate statistics for the study.

RESULT

There is a need to pay attention to the growth in online fraud which could threaten digital banking success, as Nigeria continues to embrace electronic transactions and push for financial inclusion. According to the Nigeria Inter-Bank Settlement System Plc (NIBSS), in the first nine months of 2020, fraudsters attempted 46,126 attacks, and they were successful on 41,979 occasions, 91 percent of the time.

These numbers show that internet penetration, mobile phone usage, and agency banking activities are all increasing but the country's financial fraud rate peaked as well.

Figure: showing the amount lost to fraud from to Q3 2020



Data not available for 2019 and full year 2020; Source: Nigeria Interbank Settlement System plc (NIBSS)

According to NIBSS, the spike in 2020 was as a result of the pandemic which caused people, businesses, and the government to take their businesses and social connections online.56% of the fraud attempts were carried out using social engineering techniques

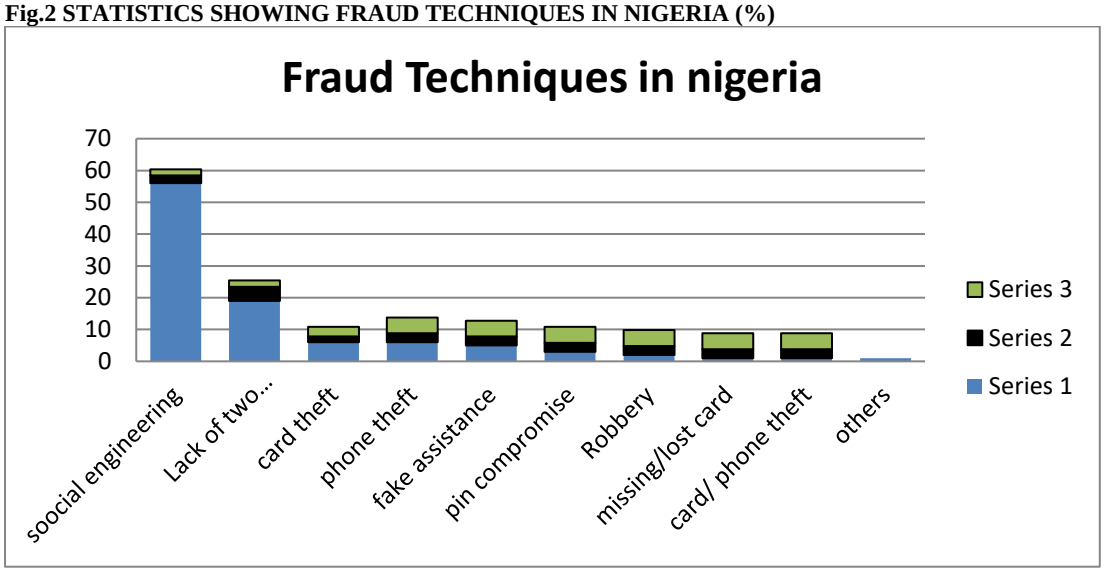
ISSN (PRINT): 2814-3183: e-ISSN (ONLINE): 2955-0572

The NIBSS identified social engineering, no 2-factor authentication, PIN compromise, card/phone theft, fake assistance, and several others as the major methods for fraudulent activities. The most common was social engineering which involves manipulating

people to give out confidential information and bank details. The most common is receiving text messages or emails from fraudsters pretending to be bank personnel.

The next big targets were those who did not have two-factor authentication systems set up at 19 percent. Others include card theft (6 percent), phone theft (6 percent), fake assistance (5 percent), pin compromise (3 percent), Robbery (1 percent) and others.

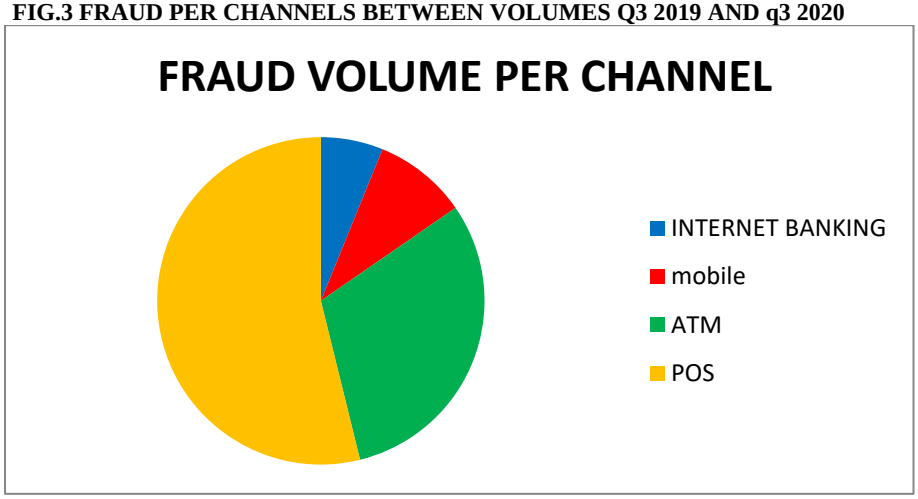
Fig.2 STATISTICS SHOWING FRAUD TECHNIQUES IN NIGERIA (%)



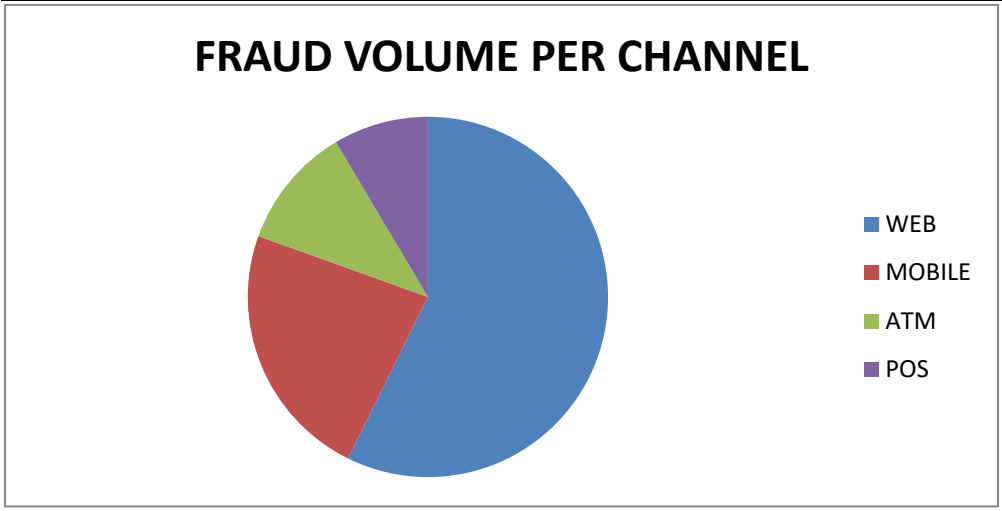
SOURCE: Nigeria Interbank settlement system Plc (NIBSS)

Online, Mobile and ATM were the most channels through which people were defrauded: Fraudsters carried out their acts through the web, mobile transaction and ATM machines. In 2019 fraudulent activities were carried out mostly through the web (51 percent), mobile transactions (35 percent) and ATM (20 percent.) Also, in 2020 many Nigerians were defrauded through the web (47 percent), mobile transactions (19 percent) and ATMs (9 percent). Below chart shows fraud chart per channel between Q3 2019 and Q3 2020.

FIG.3 FRAUD PER CHANNELS BETWEEN VOLUMES Q3 2019 AND q3 2020



Q3 2019: Source: Nigerian interbank settlement system (NIBSS).



Q3 2020: Source: Nigerian interbank settlement system (NIBSS).

Fig.4 SHOWS THAT NGERIA IS THE WORST HIT AMONG COUNTRIES OF THE WORLD.

While fraud is not peculiar to Nigeria alone but it appears to be the worst hit by a wide margin. Most countries recorded almost no case of fraud but Nigeria saw a total fraud value of N3.3 billion in Q3'2020 compared to 499 million in the same period of 2019, according to NIBSS.

STATISTICS OF DIGITAL FRAUD IN FINANCIAL ORGINISATION BETWEEN Q3 2019 AND Q3 2020.

COUNTRIES	Q32019	Q3 2014
UNITED STATES	39	18
CHINA	0	0
TURKEY	0	0
SOUTH AFRICA	0	0
INDIA	0	0
CANADA	0	0
GERMANY	0	0
CYPRUS	0	0
ARGENTINA	0	0
NIGERIA	499	3340

Source: Nigerian Interbank Settlement system NIBSS.

DISCUSSION

Negative Effects of Financial E-Fraud in Nigeria

The negative effect of e-fraud in this study is divided into:

Human Impact: Fraud against public organizations is not a victimless crime. Fraud usually can be very traumatic. The experience often causes real and irreversible on victims, their families, careers and even the communities. Those who rely heavily on government services such as pensioners are the ones harmed directly or indirectly and this increases the disadvantage in the society, vulnerability and inequality. Fraud could lead to lasting mental health and physical trauma for victims.

Impact on Governance: When frauds are committed against the government according to the International Public Sector fraud forum February, 2020 fraud against public bodies compromises the government ability to deliver services and achieve intended targets and the services delivered can be substandard or unsafe. This can lead to program failure. It also leads to opportunities for individuals and businesses.

Impact on Nigeria Reputation: When fraud happens industries and government tend to lose their reputations if it is not handled well. International agencies and journals will not want to relate with organizations that have suffered huge loss due to fraud unless their security is strengthened.

Impact on Nigerian Industrialization: Fraud against public bodies can result in distorted markets where fraudsters obtain a competitive advantage and drive legitimate business out. It can affect services delivered by business and expose other sectors to further instances of fraud.

ISSN (PRINT): 2814-3183: e-ISSN (ONLINE): 2955-0572

Impact on Trust on Nigeria Financial Institution: Fraud in the Nigerian financial institutions breed mistrust. Investors avoid the Nigerian financial institution because of fraudulent practices and financial insecurity therein

Curbing Actions Against Fraud

Users Education: As the Industry Continues to improve its business, there is a need for continuous innovations. As the Fraudsters continue to innovate, the financial industry must continue to adopt and develop outstanding strategies to beat and combat practice, this is why developing strategies militants should be key to everyone in this business.

User education is one key way to deal with fraudulent activities. Social engine ring is a large range of changing a victims Psyche by educating customers and Users on the need and dedication not to give out Sensitive information to Strangers who they are not sure either by plusing, Farming and other Sources. In every Situation to be solved, Customers must have physical presence in financial institutions; talk with qualified and approved Staff or agent to be sure information emanated from the bank. User Education should be adopted by financial institutions sternly for insiders and external customers to educate to reduce fraud incidents.

Development of Fraud Solutions: Institutions are currently investing in State-of-the-art facilities (anti-fraud) Solutions that takes advantage of the latest advancement in Artificial intelligence to provide Suitable protection against fraudulent activities. Also, Data mining tools that are artificial intelligence driven are used basically by credit search bureaus such as CRC, CRMS to check for serial credit defaulters in the financial system and when these debtors are discovered by these Data Mining tools, they are denied loans and other financial benefits.

Introduction of Biometric Identification System: NIBSS (Nigerian Interbank Settlement System) has participated in the establishment of an industry Biometric Identification System by deploying, the e-passport portal to verify Customer's International passport (Driver's License is still on the way). NIBSS has also deployed the e-reference Submission among and between banks. All these measures put in place is to ensure that the case of account take over is reduced or eliminated totally in the Nigerian financial institutions. An effective Know Your Customer (KYC) is what the banks have adopted to curb the menace of fraud among financial Institution in Nigeria.

Complete and Accurate Reporting of Fraud: Banks in Nigeria have been tasked by the NIBSS CBN, NDIC on the timely rendition of fraud reports to these regulatory bodies, this is to help in the education of new fraud Strategies and techniques that are new to the System to forestall future occurrences.

Also, the System will keep the record and data of fraudsters to discount people from dealing with such fraudsters. An example of the reporting link is to log on to http://efraud nibs-plc.com: 8082/ to make such reports.

Strengthening the International Gateway: NIBSS has ensured that all international gateways have been given opportunity for all to pass their switches and integrate then through the Nigeria payment for proper regulation and audit trial.

Recommendations

Owing to the importance of digital financial Services, it is pertinent to note that many financial organizations still create loop holes for this detriment of its customer who may suffer Psychological disorders and even physical wellbeing issues. It is on this premise that financial organizations need to initiate a well round Strategy involving sensitization, investment in well-suited technologies with adequate Securities in places. Most financial Institutions fall prey to software's that are not adequately secured, this pave way to fraudulent practice.

Services level Agreements between financial institutions and ICT companies should be taken seriously and any threat found should be directed to the company for immediate resolution. Risk management, effective governance and industry-wide collaboration with relevant stakeholders.

Conclusion

Based on the aforementioned no financial organization should operate without educating its customers on how to conceal password, manage their ATM cards and be sure of WEB transactions they are carrying out. Employees of financial should be profiled so as to ensure they don't have previous cases of fraud involvement before recruitments.

ISSN (PRINT): 2814-3183: e-ISSN (ONLINE): 2955-0572

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. 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 counter measures. *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, 2*31-247.

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). Organized fraud and organizing fraud: unpacking research on networks and organization. *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 Nigeria: An appraisal. *Information Technology Journal, 6*, 490496.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). 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, victimization strategies and fraud prevention. *Journal 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