Global Scientific JOURNALS

GSJ: Volume 7, Issue 8, August 2019, Online: ISSN 2320-9186
www.globalscientificjournal.com

ELECTRONIC BANKING FRAUD IN NIGERIA: EFFECTS AND CONTROLS

Olaleye John Olatunde PhD
Faculty of Environmental, Social and Management Sciences
Department of Accounting and Finance
Lead City University
Toll Gate Area.P.O.Box30678, Secretariat, Ibabdan, Oyo State, Nigeria
Tel. +2348023635085 /+2348035232196
E-mail address : tundelaleye@yaoo.com
&
Fashina, Abiodun Fasunle
Faculty of Environmental, Social and Management Sciences
Department of Accounting and Finance
Lead City University
Toll Gate Area.P.O.Box30678, Secretariat, Ibadan, Oyo State, Nigeria
Tel. +2348035960666
E-mail address: abiodunfashina@yahoo.co.uk;

ABSTRACT

This paper examined the nature of electronic banking related fraud on deposit money banks in Nigeria, it effects and the controls put in place to prevent financial loss. The evolution of e-banking, major channels for e-fraud, factors responsible for the high rate of fraud, nature and methods by which computer and ICT can be employed to defraud banks.

The study adopted case study research design of data collection which was based on the use of secondary. The paper focuses on Nigerian Electronic Fraud Forum (NeFF) Annual Report 2016. It was observed that the 2016 witnessed 19,531 fraud cases reported as against the 10,743 recorded in year 2015 and this represent 82% increase. However, there was a marginal reduction in attempted fraud value and actual loss. The study revealed that there is a significant relationship between e-banking practices in Nigeria and the rate of increase in the security of banking transactions. The practice of e-banking has significantly increased the volume of banking transactions. It has also improved service delivery to customers and easy. The study shows that the effect of electronic fraud would result in loss of money which belongs to either the bank or customers. It could also destroy the bank's reputation among others. The researcher concluded that despite the security problems associated with electronic banking practice in Nigeria, it has improved the operational efficiency of banks. Based on these findings, the researcher recommend that Government through CBN should provide adequate security measures for various electronic banking channels, review of BVN framework and sensitization of customers on electronic banking operations among others.

Key Words: Nigerian Electronic Fraud Forum, e-fraud, financial loss, Annual Report
Word Counts: 253

Introduction

Electronic payment systems refer to the automated processes of exchanging monetary value among parties in business transactions and transmitting this value over the Information and Communication Technology (ICT) networks. The common e-payment channels include the payment cards (debit or credit), online web portals, point of sales (POS) terminals, automated teller machines (ATM), mobile phones, automated clearing house (ACH), direct debit/deposit and real time gross settlement (RTGS) system.

With the growth in the use of electronic payments, criminals have found yet another means to increase their nefarious ways of fleecing innocent victims of their money. They employ methods such as counterfeiting, identity theft, card trapping, pharming, cloning, malware attack, BIN attack, skimming, phishing and carding to defraud and steal from users of electronic payment. Simple consumers are not the only targets of electronic payment crimes, other targets include the merchants, retailers, banking institutions, organisations that use individuals' data to transact businesses and even the government. No possible target is spared by these criminals.

The upsurge in fraudulent practices in all aspect of national life all over the world has become a source of concern and that of Nigerian banking sector has been embarrassing in recent times (Okpala & Enwefa, 2017). The major factors responsible for the high rate of fraud include the advent and extensive growth in computer technology and globalized economies supporting e-fraud, poor financial and regulatory framework, week internal control system and societal attitude to achievement at all cost.

With the advent of the Computer Age, it is common knowledge that the worldwide adoption of Information and Communication Technology (ICT) has immensely altered and enhanced human interaction and our way of life for the past three decades. Thus, the world is now a global marketplace as a result of the application of Information and Communication Technology (ICT) in business. However, the emergence of Electronic Commerce (e-Commerce) as a result of the development of the internet has brought with it a number of legal and socio-economic issues. Information and Communication Technology (ICT) is the use of scientific tools and techniques for developing, documenting and communicating information when needed especially as it concerns solving problems and providing needed services in the various areas of human endeavours. It is a term that generally covers the harnessing of electronic technology for the information needs of a business at all levels.

Nigeria has remained the fastest growing mobile phone country in Africa and the third in the world where over 60% of the populace are connected (Akwaja, 2010). Thus, Nigeria has great potential for mobile commerce implementation besides the electronic commerce that is gradually gaining momentum. The major distinction between the electronic and mobile business transaction prefixed as "e" and "m" is that the electronic medium offers "anytime access", while mobile medium offers "anytime and anywhere access" to business processes respectively. However, the success of e-payment will impact greatly on m-payment if security and usability issues are well considered. When it comes to credit and debit card

payments, several entities are required to process a transaction from start to finish: consumers and their payment cards, merchants and their point-of-sale (POS) payment devices, the card brands (i.e. Visa, MasterCard, Verve, etc), issuing banks, and card processors. Enormous amounts of electronic data and digital currency flow through this payment ecosystem as billions of transactions are processed each year.

With access to the sensitive information that enables the exchange of billions of naira in transactions each year, the payments infrastructure is a red-hot target for hackers. The electronic commerce industry has never before been at a more critical juncture in the fight against cybercrime than now. It is the good guys against the bad guys, and the good guys are determined to win. It is no secret the payment ecosystem is vulnerable. Much like the internet, the payments infrastructure was developed for connectivity, not for security. Now, in the face of serious threats and too many successful instances of hackers exploiting the vulnerabilities of the system, the industry is playing catch up to safeguard it. Despite all this importance of ICT to banking, the level of fraud in the present-day Nigeria has assumed an epidemic dimension.

Review Of Related Literature-Evolution of E-banking in Nigeria

Banking has come a long way from the time of ledger cards and other manual filling system to the computer age. Computerization in the Nigerian banking industry was introduced first in the 1970s by Society General Bank (Nigeria) Limited. Until the mid1990, few banks that were computerized adopted the Local Area Network (LAN) within the bank branches. The sophisticated ones among the banks then implemented the Wide Area Network (WAN) by linking branches within cities while one or two implemented intercity connectivity using leased lines (Salawu and Salawu, 2007)

Later on, the Scenario became different, banks have not only adopted computerization but advanced from very simple and basic retail operations of deposits and cash withdrawal as well as cheque processing, to the delivery of sophisticated products which came as a result of keen competition in view of unpresented upsurge in the number of banks and branches as well as advancement in the information technology. There was the need to innovate and modernize banking operation in the face of increased market pressure and customers demand for improved service delivery and increased convenience. The adoption of internet and electronic banking therefore become an imperative (Salawu and Salawu, 2007).

According to Sanusi (2002) as cited by Dogarawa (2005). The introduction of e-banking (e-payment) products in Nigeria commenced in 1996 when the CBN granted All States Trust Bank approval to introduce a closed system electronic purse called ESCA. This was followed in February 1997, with the introduction of a similar product called “Paycard”, by Diamond Bank. The card-based e-money products assumed an open platform with the authorization in February 1998, of Smartcard Nigeria PLC, a company floated by a consortium of 19 banks to produce and manage cards called value card and issued by the member banks. Another consortium of more than 20 banks under the auspices of Gemcard Nigeria Limited obtained

CBN approval in November 1999 to introduce the "Smartpay" Scheme (Dogarawa, 2005). The number of participating banks in each of the two schemes had been rising since then.

Furthermore, the CBN additionally granted approval to a number of banks to introduce international money transfer products, telephone banking and on-line banking via the internet, though on a limited scale (Dogarawa 2005, cite Abdulhakeem, 2002). Mention must also be made on the development of Automated Teller Machine (ATM) by some banks to facilitate cards usage and further enhance their service delivery. Today, virtually all Banks in Nigeria now have a website. The service or ordering bank drafts or certified cheque made payable to third parties has also been increasingly automated (Irechukwu, 2000).

Nature of electronic fraud in Nigeria

Computer frauds can take the form of corrupting the program(s) and even breaking into the system via a remote sensor by a computer programmer or specialist. The manipulation of computer and other Information and Communication Technology (ICT) to defraud banks gives more insight into the latent friction of technological revolution. When computer was invented, the intention of its inventors is to hasten data processing with effortless case. That, it has been doing efficiently by giving timely and accurate information.

But like other mechanical and/or electrical electronics devices, it has equally lent itself to heinous acts. What is meant to assist in daily data operations has turned out to be an undoing. While basking in the euphoria of its efficiency, banks are also grasping with its fraudulent manipulations. The liability of computer to control manipulations, frauds and forgeries continue to give the banking system nightmares.

Any type of act distinctly associated with computer or data manipulation in which victim involuntarily suffer or could have suffered losses, injuries or damage or in which perpetrator receive or could have received gain is referred to as a "Computer crime". The adoption of ICT in banking is generally referred to as electronic banking (e-banking) and the implementation strategies of banking services have become a subject of fundamental importance and concern to all banks and indeed a pre-requisite for local and global competitiveness. This is because it directly affects the management decisions, plans, and products and services to be offered by banks. The internet and indeed, the e-banking have continued to change the way banks and their corporate relationships are organised worldwide and the variety of innovations in service delivery.

In the 2003 report of the technical committee on e-banking of the Central Bank of Nigeria (CBN) defines e-banking as "a means whereby banking business is transacted using automated processes and electronic devices such as personal computers, telephones, internet, card payments and electronic channels. It further states that some banks practise electronic banking for informational purpose, some for simple transactions such as checking account balance as well as transmission of information, while others facilitate funds transfer and other financial transactions. Many systems involve a combination of these capabilities.

Types of electronic fraud in Nigeria

These are some of the types of electronic fraud in Nigeria:

Triangulation/Site cloning: Customers enter their card details on fraudulent bank sites and these details are then misused.

Hacking: Hackers/fraudsters obtain unauthorised access to the card management platform of banking system. Counterfeit cards are then issued for the purpose of money laundering.

Online fraud: Card information is stolen at the time of an online transaction. Fraudsters then use the card information to make online purchases or assume an individual's identity.

Lost/Stolen card: It refers to the use of a card lost by a legitimate account holder for unauthorised/illegal purposes.

Account takeover fraud: An individual illegally obtains personal information of valid customers and takes control of the card account.

Money laundering: Transfer of money into and out of a mobile wallet from or to a bank account is now possible. Cash-in from the bank account of an individual and cash-out to a different bank account of another individual can be used as a platform for laundering unaccounted money.

Unauthorised emails/Text messages: Asking for account information for updating bank records are sent by fraudsters. The customer information is then misused for misappropriating funds.

Unauthorised Access: This type of fraud may arise when access rights for making entries are given to unauthorised people.

Debit card skimming: A machine or camera is installed at an ATM in order to pick up card information and PIN numbers when customers use their cards.

ATM Fraud: A fraudster acquires a customer's card and/or PIN and withdraw money from the machine.

Mobile banking application against incorrect mobile number: For bank customers who do not use mobile banking, an employee of the bank could attach an associate's mobile number to the bank account and install a mobile application on his mobile devise. The customer's account is compromised by the associate and he or she does not get any notification about the same.

Creating fake and non-existent users on mobile platform: Most of the banks appoint a third-party vendor to develop a mobile application to be integrated with their core banking system. The vendor may create two unauthorised users with rights to initiate and verify transactions, and transfer funds from the organisation to his associates' wallets, effectively stealing money from the bank.

SIM Swap: means replacing the old SIM with a new one, when the old gets lost or damaged, or when one needs a differently sized SIM card. If a fraudster manages such a swap, he can carry out numerous fraudulent transactions using the mobile number of the victim. The user has no access to their account and receives no notification. The user with the other handset, on knowing the PIN, can transact in the account.

Unauthorised deduction from Mobile wallet: Employees of the mobile wallet service provider may misuse the balance stored in the wallet of a customer, especially a dormant or infrequent customer account, by making unauthorised deductions.

Major channels for electronic fraud in Nigeria

The influence of sophisticated machines like electronic fund transfer, computer manipulation on bank fraud is very significant. The majority of fraud committed in the banking sector are usually committed through electronics transfer and computer manipulation. Most of the fraud cases recorded in Bank in Nigeria are ICT and computer related through the following:

Smart Card: This is a card issued to a customer by a member bank of SMART CARD Nigeria Limited to aid them in their transactions. The card issued to the customer is usually PIN protected (Personal Identification Number), and each card holders has access/pass code or password different from any other persons. Such a pass code must be kept secret and must be changed any time it becomes known to someone else.

Electronic Fund Transfer (EFT): This is an electronic oriented payment mechanism. It allows customers accounts to be credited electronically within 24 hours (Ugwu, et al, 1999). Mark (1975) classified the basic elements of ETF system into three: Clearing network characteristics, remote service or points of sales characteristics and pre authorized debit and/or credit characteristics.

Mobile Telephone Banking: Mobile phones are increasingly being used for financial services in Nigeria. Banks are enabling the customers to conduct some banking services such as account inquiry and funds transfer through the mobile telephone. The Mobile telephone banking notifies the customer of any transaction on his/her account.

Personal Computer (PC) Banking: PC banking refers to the use of computer hardware, software and telecommunications to enables retail customers' access to both specific account and general information on bank's products and services through a personal computer.

Automated Teller Machine (ATM): This is an electronics device which allows a bank's customers to make cash withdrawals and check their account balances at any time without the need for a human teller. Many ATMs also allow people to deposit cash or cheques, transfer money between their bank accounts or even buy Mobile phone recharge cards. To withdraw cash, make deposits, or transfer funds between accounts, you generally insert an ATM card and enter your Personal Identification Number (PIN). Some ATMs impose a surcharge, or usage fee, on consumer who are not member of their institution or on transactions at remote locations.

Internet Banking Channel: Internet is a global network of computers. It is a collection of computers networks, computers and millions of users, who share a compatible means for interacting with one another to exchange information (Awe, 1998).

Methods by which computer and ICT can be employed to defraud banks

The methods are:

Computer aided fraud and embezzlement: this is automated version of the good fashion manual fraud or embezzlement that has been going on for centuries by unscrupulous employees. Skilled data processing professionals usually perpetrate this type of computer fraud.

Time (or logic) Bomb or Trap Door: Convert instruments are written and inserted into a production programs or files, or cause application software, such as a payroll to or account receivable, or the whole system to crash. A time bomb is almost impossible to detect or prevent and it is almost impossible to catch the person who devise it because a clever programmer can write the instruments so that when the bomb erases the target program application or system, it destroys itself as well.

Scavenging: This is a method of obtaining data or information by searching trash cans of banks, data processing departments, this is called physical scavenging. There are also electronics scavenging that involves searching for residual data left in a computer.

Software piracy: It involves copying or theft of proprietary computer software and/or raw data or information. Moreover, if the criminal just copied the valuable software or sensitive data, it is almost impossible to detect the crime because the original software or data remains on the disk or in the computer.

CBN Report

According to CBN reports, year 2016 experienced a lot of innovation in the electronic payment space. New products and services, well driven by cutting edge technologies came to limelight which in turn led to an increase in the adoption of e-payment and transaction volume. For example, the ease of transacting with our mobile phones took a new dimension with the introduction of USSD. As we strive daily to improve our products and services, and also make electronic payment channels simpler to use, fraudsters are also not relenting in their efforts to take advantage.

The volume of fraud reported in 2016 compared to previous years attest to the fact that fraudsters do not grow weary. The more products and services that are rolled out without proper risk and impact analysis, the easier for the "bad guys" to perpetrate more fraud effortlessly. The determination and commitment of these unscrupulous elements cannot be underrated within the financial sector. The financial industry needs to ensure that more regulations and inter-industry collaboration are put in place to curb this trend.

Over the years, technology has played a vital role in the history of Nigeria's financial space. From initiating funds transfer right from the comfort of our rooms, to paying utility bills without having to visit the service providers and uniquely identifying bank customers with biometrics, etc. Many cutting-edge products and services have been developed which in turn have changed the way we interact and transact. The ease, transparency and swiftness that technology brought to the financial ecosystem in Nigeria are noteworthy.

The directive by the Central Bank of Nigeria (CBN) for the establishment of industry fraud desks, sending of all electronic interbank transactions to the Central Anti-Fraud Solution

(HEIMDALL), introduction of biometrics to the ecosystem, and most importantly, our collaboration, have contributed to reducing fraud menace in Nigeria's financial space.

The Director, Consumer Protection Department, Central Bank of Nigeria (CBN) has said that electronic fraud losses in the banking system are projected to reach N6.1 trillion by 2021. He disclosed this at the workshop for Business Editors and Finance Correspondents, organised by Nigeria Deposit Insurance Corporation (NDIC) in Benin. According to him, the volume and value of e-transactions is projected to continue to increase nationally and globally.
The Director also said that the CBN, through its Consumer Protection Department (CPD), had resolved over 13,715 complaints which resulted in the refund of about N72.2 billion to customers by the commercial banks based on 25,043 cases of fraud in 2017. He said the amount represented a 28% increase if compared to 19,531 cases recorded in 2016. He disclosed that there was a 24% reduction in actual fraud loss value in 2017 with N1.63 billion as against the 2016bfigures.
According to the Director, the statistics provided by the CBN shows there is a significant increase in the year-on-year volume and value of transactions across all payment channels in Nigeria. Consequently, 1.4 billion transactions with a value of N97.4 trillion were processed in 2017 as against 869 million transactions with a value of N69.1 trillion recorded in 2016. He said the increase of 59.7% and 40.9% were recorded in the volume and value of transactions in 2017.

As reported by CBN, the number of recorded electronic fraud cases in the banking industry increased by 28 percent in year 2017, rising from 19,531 in 2016 to 25,043 resulting in a loss of N1.63 billion. The banking watchdog, however, noted that the number of actual losses declined by 24.0 percent relative to that of 2016 and the attempted fraud value also declined in 2017, falling to N4.03 billion from N4.37 billion in 2016. As contained in the CBN 2017 Annual report, the volume and value of electronic payments in 2017 rose by 60.0 and 39.7 percent to 1,478.5 million and N99,292.3 billion, respectively, compared with 941.8 million and N71,100.00 billion in 2016. The rise was attributed to increases consumer awareness and confidence in e-payment channels.

Methodology

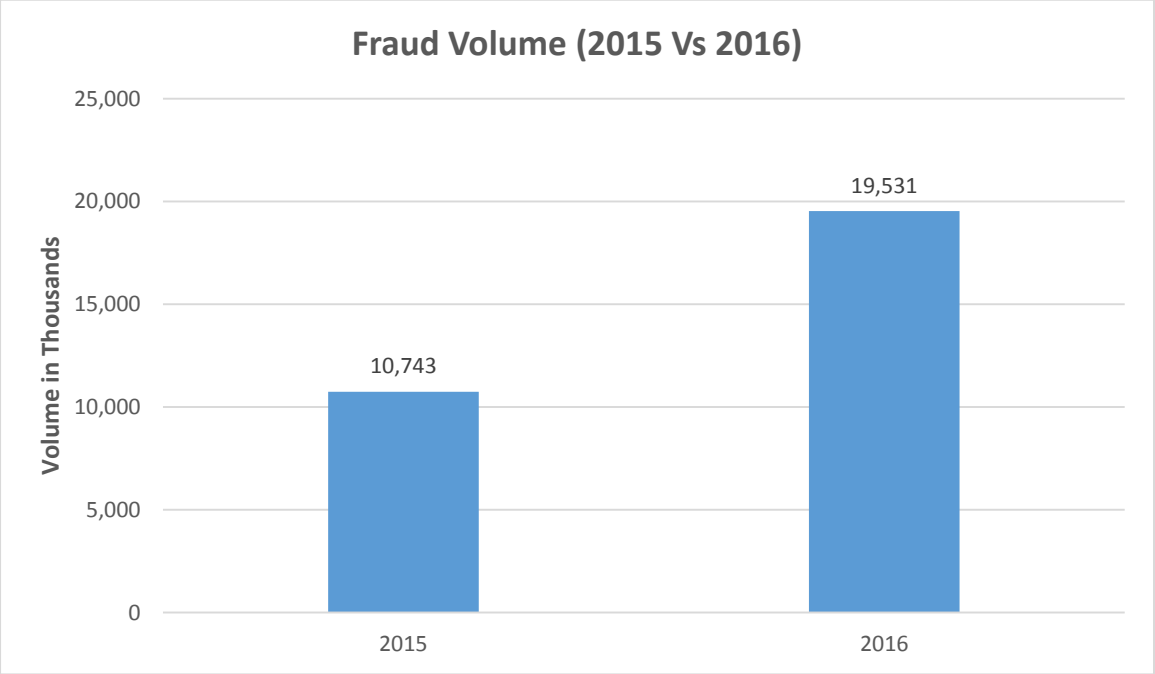
This study adopted case study research design of data collection, which was based on the use of secondary. The documentary data collection includes the number of e-banking products utilized, fraud volume, attempted fraud value and actual loss value in Nigeria for year 2016 which was compared with year 2015 figures. These were extracted from CBN: Nigeria Electronic Fraud Forum (NeFF) Annual Report, 2016 and the data were presented in tables and bar charts.

Results

The figure below shows that 19,531 fraud cases were reported for Deposit Money Banks in 2016 as against 10,743 in year 2015. Although, there was 82% increase in reported fraud cases as compared with 2015, we also witnessed marginal reduction in attempted fraud value

and actual loss is N 4,368,437,371.64 and N 2,196, 509, 038.78 respectively. Also, there was a decrease of 2.65% in actual loss due to fraud in 2016 when compared with 2015.

Year	Fraud Volume	Attempted Fraud Value (N)	Actual Loss Value (N)
2015	10,743	4,374,512,776.64	2,256,312,660.00
2016	19, 531	4,368,437,371.64	2,196,509,038.78

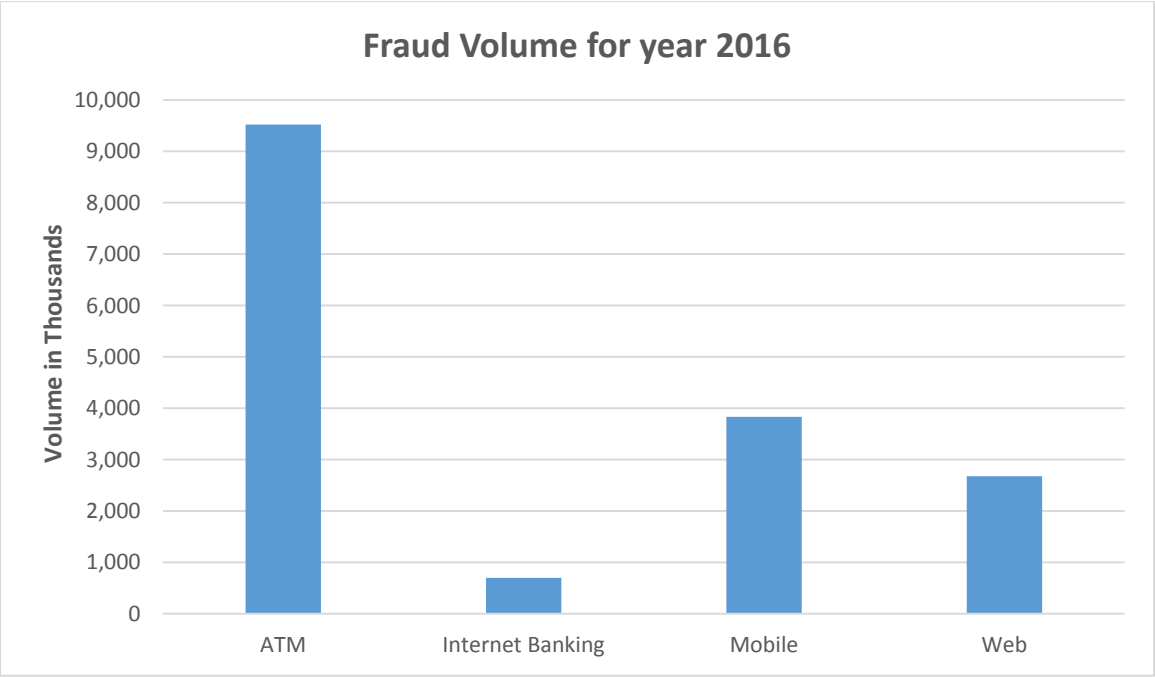


Fraud per channel

Exploring reported fraud events in the year 2016 and categorizing them according to channels, fraud perpetrated through the Automated Teller Machine (ATM) recorded the highest volume of fraud followed by Mobile. This is analogous to several emerging products and services riding on these channels which fraudsters are taking advantage of, especially mobile channel. The third most used channel to perpetrate fraud is Web.

Channel	Fraud Volume	Actual Loss Value (N)
Across Counter	325	511,072,861.29
ATM	9,522	464,514,684.27
Cheque	12	4,558,897.75
E-commerce	520	132,252,118.32
Internet Banking	698	320,665,957.87
Kiosk	3	10,198,000.00
Mobile	3,832	235,170,720.40
POS	1,658	243,321,812.67
Web	2,677	83,776,994.11
Others	284	190,976,992.10

Following the fact that we are concern with the bank electronic fraud in Nigeria, the diagram below only considered the following channels: ATM, Internet banking, Mobile and Web.



Summary of Findings

1. There is a significant relationship between e-banking practices in Nigeria and the rate of increase in the insecurity of banking transactions.
2. The practice of e-banking in Nigeria is significantly increased the volume of banking transactions.
3. The e-banking has tremendously improved the services of banks to their customers.
4. The e-banking operation has made the banking payment transactions easy and reduced the congestions in the banking all.

Effects of electronic fraud in Nigeria

Electronic fraud is fast becoming a potent threat to the Nigerian banking industry. There is as upsurge of e-fraud despite the many efforts to check cybercrime in the country. Undoubtedly, frauds lead to loss of money which belongs to either the bank or customers. This loss results in a decline of productive resources available to the bank. Adewunmi (1996), identified the under listed effects of bank frauds and forgeries:

a. It destroys the bank's reputation
b. It discourages banking habit among the banking public.
c. The bank ceases to meet up with staff welfare.
d. The trust and understanding among staff is reduced.
e. The bank will lack the ability to compete favourably with its competitors.
f. Fraud reduces bank's profitability.
g. It places emotional and psychological burdens on the fraud victims.
h. Others include: Increased operating expenses, reduced operational efficiency, damage to credibility, public criticisms, endangered bank's plans and strategies, bank's

liquidation, a decrease in foreign direct investments (FDI) and foreign investors, depletion of shareholders' funds and banks' capital base, and bad national image.

Prevention and control of electronic fraud in Nigeria

Although the incidence of fraud is neither limited to the banking industry nor peculiar to Nigeria economy, however, the high rate of fraud within the banking industry, calls for urgent attention with a view to finding solutions. Frauds in its effect reduces organizational assets and increases its liabilities. With regards to banking industry, it may engender crises of confidence among the banking public, impede the going concern status of the bank and ultimately lead to bank failure. It has become necessary to review and strengthen existing rules and enact new laws to stem the problem. Recommended solutions are:

1. **Issued of operating guidelines:** With the rapid growth in users and wider coverage of mobile phone networks, mobile banking is increasingly coming up as a significant delivery channel for extending banking services to customers. Putting the onus on banks, the Central Bank of Nigeria (CBN) should issue operative guidelines to regulate this channel, suggesting reporting of suspicious transactions to its financial intelligence unit.
2. **Deploying advanced tools and technology:** Owing to the heavy reliance on telecom operators for its services, the prevention and detection of frauds in mobile banking have become even more complex. To keep a check on frauds, banks need to incorporate a greater level of scrutiny, by deploying advanced tools and technology capable of protecting the customers against unethical activities.
3. **Deep learnings:** Internet payment companies providing alternatives to traditional money transfer methods are using deep learning, a new approach to machine learning and artificial intelligence that is good at identifying complex patterns and characteristics of cybercrime and online fraud.
4. **Internal Audit function:** This function is being altered to include fraud risk management in its scope. The changed technological landscape requires the old ways of Internal auditing to give way to new, technologically equipped audit functions. Annual audit planning may no longer be fully effective and flexible audit plans are the need of the hour, as fraud risk assessments require extensive use of forensic and data analytics solutions.
5. **Automated analysis tools:** Today, the industry is increasingly aware of the need for automated analysis tools that identify and report fraud attempts in a timely manner. Solution providers are providing real-time transaction screening, third-party screening as well as compliance solutions.
6. **CCTV Camera:** The management of the bank should install the Close Circuit Television (CCTV) camera at all the ATM locations and strategic positions within the banking hall.
7. **Networking and routine checks:** To prevent computer and ICT fraud, better networking and routine check of money transfer and transactions would frustrate the fraudsters.

8. **Effective control:** An effective control is the most potent antidote against fraud. Human supervision of ICT high waves can bring incidence of ICT manipulation to the barest minimum.
9. **High level ICT consciousness:** ICT should be subjected to a high level of security consciousness to guard against improper use, that is, posting and diversion.
10. **Regular rotation of bank staff:** The management of the bank should ensure regular rotation of duties and staff to prevent an individual from staying too long on a computer system or in a department. Also, there should be inter-branch and intra-bank regular rotation of bank staff.
11. **Relevant laws:** The National Assembly should propose relevant bills that can curb the electronic frauds in Nigeria. For example:
    - Cyber security and Information Protection Bill.
    - Electronic Transactions Protection Bill.
    - Computer Security and Protection Bill.

Conclusion and Recommendation

In view of the fact that the security problem may have seen to be a crucial issue in the practice of e-banking in Nigeria but that could not imply that the operational efficiency of e-banking is impaired. This is because the core banking operations of accepting deposits, granting credit facilities and facilitating cash withdrawal have empirically proved to have improved with the introduction of e-banking in Nigeria. Woherem (2000) opined that only banks that overhaul the whole of their payment and delivery system and apply ICT to their operations are likely to survive and prosper in the new millennium. Therefore, it can be concluded that e-banking introduction in Nigeria had aid to enhance Nigerian banking operations vis-a-vis banks employees' productivity cum general performance. Consequent upon this, the researcher recommended the following:

a. Government through CBN should provide adequate security measures towards the various e-banking products in Nigeria.
b. Banks should regularly train their workers who in turn will educate their customers on e-banking system and its products.
c. The CBN should organize seminars, workshops, symposia and public lectures to bank customers and general public on the application of information and technology cum e-banking system.
d. Banks should in addition to the storage of information in the computer, maintain the manual filing of all the relevant documentary evidence of information in their financial statement in order to avoid loss of audit trail, with an understanding that e-banking in Nigeria is an "add process" and not an "or process".
e. The banking industry should review the existing BVN framework with the introduction of BVN Watchlist in the framework.

REFERENCES

Adewunmi, W. (1996). Fraud in banks. Nigerian institute of bankers, Land mark Publication, Lagos.

Adeyemi Adesanya-Daniel (November, 2018). CBN Journal on "Central bank: Electronic Fraud will hit N6.1 trillion by 2021".

Aluko-Olokun (1990). Nigeria Banks and Computer.

Central Bank of Nigeria (2017) Annual report Page 38.

Chike, O. (2018). "Banks loss N1.63 BN to E-fraud". Nigeria Communications week Journal. August 18.

Dogarawa, A. B. (2005). The impact of E-banking on consumer satisfaction. Department of Accounting, Ahmadu Bello University, Zaria.

Ekwueme, C. M., Egbunike, P. A., & Amara, O. "An Empirical assessment of the Operational efficiency of electronic banking: Evidence of Nigerian banks". Review of Public Administration and Management paper. Vol.1 No. 2 Page 108-133.

Folami, O. M. (2000). Crime in the Banking Sector. M.Sc. thesis, Department of Sociology, OAU.

Irechukwu, G. (2000). "Enhancing the performance of banking operations through appropriate Information Technology". Information Technology in Nigeria Banking Industry, Ibadan, Spectrum Books.

Journal of Forensic Accounting and Fraud Investigation (JFAFI) ISSN 2659-1138 (Print): ISSN 2659-1146 (Online) volume 4. Issue 1, January-March, 2019. P. 49.

Nwankwo, G. O. (2005). Bank management, principles and practice.

Okpala, K. E. & Enwefa, C. (2017). War against corruption in Nigerian public sector: An analysis of stakeholders' role. FUNAI journal of Accounting, Business and Finance, 1 (1), Page 204-218.

PWC India publication (June 2015). Current Fraud trends in the Financial Sector.

Salawu, R. O. & Salawu, M. K. (2007). The emergence of internet banking in Nigeria.

The Nigeria Electronic Fraud Forum (NeFF) Annual Report (2016). A changing

payments Ecosystem: The Security challenge.

Tughgba A. (2017). Katsina-Ala Multidisciplinary Journal. The challenges of Information and Communication Technology in the Nigerian Banking Industry in the 21st Century: The way out.