Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) DOI: 10.7176/JLPG
Vol.88, 2019

From Revolution of Payments System to Perpetration of Cybercrimes in Nigerian Banks and Against Customers: Is the Nigerian Cybercrimes Act 2015 Relevant?

Felix, Emeakpore Eboibi * Ebizi, Blessing Eradiri
Faculty of Law, Niger Delta University, Wilberforce Island, Yenagoa, Bayelsa State, Nigeria

Abstract
The evolving nature of the information and communication technology and its effect on the global lives of individuals have consequently revolutionized the manner payments system is currently being undertaken. The difficulties and hardship constituted by the traditional payments system whereby for any cash transaction to be executed, a bank customer was mandated to visit the bank premises and where it has to do with the purchase of goods and services, parties would have to meet physically to transact, partly triggered the payments system in Nigeria from over dependence on cash to adoption of modern electronic alternatives for payments by the Central Bank of Nigeria. Questions have been asked about the legality or otherwise of this transformation from the traditional payments system to the present modern payments system. What nature of challenges has been faced by the introduction of the modern payments system? Unfortunately, these laudable modern payments initiatives in the Nigerian banking industry have been abused by perpetrators of crimes through the instrumentality of the computer and information and communication technology infrastructures. Prevailing crimes like hacking, identity theft, BVN scam, phishing and spamming, card theft, computer related fraud, electronic cards related fraud, email fraud and system interference are presently being perpetrated against the Nigerian banks and their customers. In the light of these, how is the Nigerian Cybercrimes Act 2015 relevant towards the protection of victims of these crimes?
Keywords: Cybercrime Law, Payments system, Bank customers, Cybercriminals, Nigerian Cybercrimes Act 2015, Strategies of cybercriminals.
DOI: 10.7176/JLPG/88-06
Publication date: August 31st 2019

1. Introduction

The existence of payments system is key to every economy and the role of payments system cannot be undermined, as it determines how money is to be transferred, accepted or circulated. Prior to the modern payments system, we had the traditional payment system which involved cash transactions basically where customers visit banks to send and receive money, buyers had to go to physical shops for purchases or shopping, buyers had to meet with sellers as well for receipt of consideration and goods and services, *inter alia.*

The drawback of this system of payment was that for bank transactions, they had to be done within the limited banking hours and banking halls were usually crowded which made conducting even basic transactions time-consuming. Buyers also had to leave the convenience of their homes and business places to shops and offices with cash to purchase goods within business hours which also involved cost of transportation, risk of losing cash to thieves, armed robbers, and loss of considerable time to get to the physical shop or office, among others.

In recent times, our society is increasingly relying on the internet and other Information and Communication Technology (ICT) tools to engage in personal communication and conduct business activities among other several benefits.[1] With the advent of modern payment system, transactions can be done online and many services are available 24/7 which cuts the hurdle of trying to transact within banking hours and business hours, business can even be done across borders at ease. More so, one need not move around with cash and face the many risks accompanied with cash and payments can even be made with just few clicks or dialling some short code.

As a matter of fact, this is reflected in the banking industry where many facilities are provided for clients and customers. Some of these facilities include mobile banking, internet banking, credit card, debit card, online transfer, the use of ATMs and online banking. Commendably, bank customers can use bank facilities 24 hours a day, 7 days a week and 365 days each year, and interestingly accounts can be operated easily and transactions can be concluded from any place in the world with the aid of the internet and mobile gadgets.[2]

Unfortunately, the innovative policies and technologies in the banking industry aimed towards a safer, efficient, effective and more reliable system have been abused and as a matter of fact have become a platform for

[1] Omodunbi B. A., Odiase P. O., Olaniyan O. M and Esan, A. O. (2016) "Cybercrimes in Nigeria: Analysis, Detection and Prevention" *Federal University Oye Ekiti Journal of Engineering and Technology,* (1)1, 1,1.
[2] Rathore D. S. H. and Marwaha, K (2015) "Cyber Crime In Banking Sector" *International Monthly Journal*, (2)7, 1,1.

cybercriminals to perpetrate more cybercrimes. In what way is the Nigerian Cybercrimes Act 2015 relevant to cybercrimes currently being perpetrated in the Nigerian banks? There are number of cybercrimes witnessed in the banking sector, like ATM frauds, Cyber Money Laundering and Credit Card Frauds. However, in general all the frauds in the banking industry are executed with the ultimate goal of gaining access to users' bank account, steal funds and transfer it to some other bank account.[1]

With the number of incidents of theft, phishing, computer viruses, hacking, on the rise, many customers have lost funds and different banks and financial institutions have obviously suffered from the surge. These have left many bank customers with little or no confidence in the system due to the high risk of loss of funds through mobile and internet banking, etc. In fact, some bank customers avoid the modern way of payments and go through the rigours of making payments through traditional methods.

In addition, cybercrimes can also incur untold hardship in the banking industry because there would be increased loss of income, rapid fall in investment in banks as a result of reduced confidence. As a matter of fact, it can crash the banking industry depending on the extent of the cyber-attack, which would cause much more losses which are better imagined than experienced.

Consequently, this paper discusses in detail the revolution of the payments system which has transcended from the traditional system of payment to the modern system of payment, with emphatic reference to the electronic system which is a major development in the Nigerian Payment System, initiated and implemented by the CBN in collaboration with the Bankers' Committee. It is in this light that this paper takes into consideration the concept of payments system, as well as the CBN being a body in charge of the Nigerian Payments System. The legality or otherwise of the migration of the traditional payments system to modern payments system is determined. It thereafter examines the cybercrimes that are perpetrated in Nigerian Banks with particular recourse to the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 and it further discusses the strategies adopted by cybercriminals in the perpetration of cybercrimes. It notes from a comparative perspective, what should be done to eradicate the perpetration of cybercrimes.

2. The concept of payments system

Factually, the need for functional and efficient payments system in any modern society is vital. Due to the sophistication in economic activities, modern economies have developed or are developing multilateral payments systems. This permits the settlement of financial obligations for economic operators, irrespective of where such transactions are made.[2]

According to the CBN, payments system development, just like currency management has direct linkage implications for the conduct of monetary policy.[3] Payments system here refers to the system of exchange established for the facilitation of transactions in an economy.[4] More so, the Bank for International Settlements has defined payments system as a specific set of instruments, banking procedures and inter-bank funds transfer system that ensures the circulation of money.[5] In addition, payments system refer to the established infrastructures (comprising institutions, people, set of instruments, rules, procedures, standards and computer networks) through which financial obligations are discharged by economic agents.[6]

Simply put, payments system mean an arrangement in the financial system which supports the transfer of funds from suppliers/savers to the users/borrowers, and from payers to the payees, usually through exchange of debits and credits among financial institutions.[7] It consists of a paper-based mechanism for handling cheques and drafts, and a paperless mechanism (such as electronic funds transfer) for handling electronic commerce transactions.[8] This leads us to the two eras of payments system.

2.1 Traditional payments system

Primarily, there are types of payments system available through different platforms and broadly categorised into two, namely the Retail/Small Value Payments system and Wholesale/Large Value Payments Systems.[9] The former involves relatively small payments among consumers and businesses and are used primarily by non-bank public for making and receiving payments,[10] while the latter depicts a system that typically processes high value

[1] Raghavan A.R. and Latha Parthiban, (February-2014) "The Effect of Cybercrime on a Bank's Finances" *International Journal of Current Research and Academic Review*, 2(2), pp.173-178. Available at <http://www.ijcrar.com/vol-2-2/A.R.%20Raghavan%20and%20Latha%20Parthiban.pdf> Last accessed 16 June 2019.
[2] Central Bank of Nigeria, "The Nigerian Payments System" (2011) Series No. 6, *Understanding Monetary Policy Series,* 1
[3] Jimoh, L. S. (2012) "The Mandate of the Central Bank of Nigeria," *Understanding Monetary Policy Series*, Series No. 19, 1, 5
[4] *Ibid.*
[5] *Ibid.*
[6] Central Bank of Nigeria, (2011) "The Nigerian Payments System" *Understanding Monetary Policy Series,* Series No. 6, 3
[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid* at 5
[10] *Ibid*

payments and it is used for corporate financial transactions, which is privately run by the Nigeria Inter Bank Settlement System (NIBSS).[1] The traditional and modern payments system fall under these types. The traditional payments system reflects the payments system in practice before the advent of ICT in the banking industry and modern means of payment. For the retail payments system, there are four instruments, out of which, three are traditional payments system. They are:[2]

i. **Currency or cash**: This instrument takes the form of bank notes and coins, and it is the most preferred method for small payments in Nigeria because it is without credit risk.
ii. **Paper based instruments**: These include cheques, bank drafts and travellers' cheques. In spite of the obvious advantage of these instruments over cash, their use is still very limited in Nigeria due to the low level of trust and acceptability of the instruments in settlement for business transactions, predominance of peasantry in the real sector and informality in the trade sub-sector of the economy.
iii. **Other payments instruments**: This includes postal order, money orders, vouchers and pre-paid cards. The use of these instruments are diminishing over time due to poor postal system, preferred use of banking services especially bank drafts or certified cheque and increased use of electronic payments instruments in the country.[3]

2.2 Modern payments system

Modern Payments System refers to the payments system which is birth out of the employment of ICT in the banking industry. Moreover, both the retail and wholesale payments system come under modern payments system.

2.2.1 Modern instruments of retail payments

The modern retail instruments are paperless instruments. Essentially, these are non-paper computer-based technology payments instruments and the electronic payment is one.[4] The electronic payments system is made possible by the existence of electronic money (e-money) which can be defined as a stored-value product in which a record of the funds or value available to the consumer for multipurpose use is stored in an electronic device held by the consumer. The electronic payments system is amenable to electronic platforms such as automated teller machines (ATM), point-of-sale (PoS) terminals, internet payment, plastic money, mobile payment and wire transfers, *inter alia.*[5]

The Nigerian electronic payments systems are discussed under the following heads:[6]

2.2.1.1 Electronic cards: these are physical plastic cards that uniquely identify the holder and carries monetary value that could be used as a means of settling financial obligations. Its basic types are:

a. **E-purse** – This is also called electronic wallet. An E-purse carries a pre-loaded monetary value and can be used as a means of payment for multiple small value purchases. E-purse (for example ValueCard and SmartPay) are the most predominant types of plastic money in use in Nigeria.

b. **Credit cards** – A credit card indicates that the holder has been given line of credit by the card issuers. Credit cards are used to facilitate transactions without the movement of currency or cash. This allows the holder to make purchases or make withdrawals of cash, up to the pre-arranged credit limit. The credit is settled either in part or in full within a specified period.

c. **Debit cards** – Debit cards enable the holders to have purchases and withdrawals charged directly to funds in their accounts. In Nigeria, the only example of debit cards is the ATM card being issued by banks on the Inter-Switch network.[7]

2.2.1.2 Internet banking: Internet banking involves conducting banking transactions such as account enquiry, printing of statement of account, funds transfer, payments for goods and services, among others, on the internet, using electronic tools such as the computer without visiting the banking hall. E-commerce is greatly facilitated by internet banking and is mostly used to effect payments. Internet banking also uses the electronic card infrastructure for executing payment instructions and for final settlement of goods and services between the merchant and the consumer.[8]

2.2.1.3 Telephone banking: These are banking services which a customer of a financial institution can access using a telephone line as a link to the financial institution's computer centre. Services rendered through telephone banking include account balance, fund transfer, change of pin and bills payment.[9]

[1] *Ibid* at 6
[2] *Ibid* at 5
[3] *Ibid*
[4] *Ibid* at 12
[5] *Ibid* at 5, 12
[6] *Ibid* at 13-14
[7] *Ibid* at 13
[8] *Ibid* at 13-14
[9] *Ibid* at 14

2.2.1.4 Mobile banking: This involves the use of the mobile phone for settlement of financial transactions. It supports person-to-person transfers with immediate availability of funds to the beneficiary. Mobile payments use card infrastructure for funds transfer as well as secure Short Message Service (SMS) messaging for confirmation of receipts (to beneficiaries) and payments (to account holders who have given payment instructions) of funds. It is used for low value transactions where speed of completing the transaction is important. The services covered under this product include account inquiry, fund transfer, recharging phones, changing passwords and bills payment which are offered by few financial institutions.[1]

2.2.2 Modern instruments of wholesale payments

On the part of wholesale, the instruments include the Real Time Gross Settlement System (RTGs) and Society for Worldwide Inter-bank Financial Telecommunications (SWIFT) for the modern payments system.[2] In the first vein, RTGs are large-value funds transfer services that operate continuously during the business day to provide irrevocable settlement of payments obligations *via* the Central Bank. This was commenced by the CBN on 18 December 2006 to increase the efficiency of payments and it was named the CBN Inter-bank Funds Transfer System (CIFT).[3]

The system interfaces with the Bank's core banking application (the T24 System) and has all the Deposit Money Banks (DMBs) and discount houses as direct participants. The System allows participants to perform electronically a number of transactions from their offices, using the Terminal Access Device. Notably, transactions that can be effected are inter-bank transfer, third party fund transfer (transfer on behalf of Bank A's customer to the account of Bank B's customer), account balance inquiries, queue management, report generation and reconciliation.[4]

Benefits offered by RTGs include a reduction of systemic risk, the elimination of settlement risks due to irrevocability of payment messages and enhanced efficiency of the monetary policy implementation process. The system is also capable of providing Delivery Versus Payments (DVP) for securities settlement and Payments Versus Payments (PVP) for foreign exchange settlements to reduce their risks.[5]

In the second vein, SWIFT is designed for international payments using messaging system. It facilitates international trade for example, Letters of Credit; and its transfers are characterised by high transaction costs denominated in US dollars because the network is not domiciled in Nigeria.[6]

3. The legal cadre for the revolutionised payments system in Nigeria

The legal basis for the developments in the Nigerian payments system stems from the power conferred on the CBN by the enabling Act, the CBN Act 2007, particularly Sections 2(d), 47(2), and (3). While it is evident in Section 2(d) that the CBN is to promote a sound financial system in Nigeria, Section 47(2) further buttresses that in the discharge of this particular object, the CBN shall continue to promote and facilitate the development of efficient and effective systems and this is with the inclusion of the development of electronic payment systems.

More so, Section 47(3) of the CBN Act empowers the CBN to prescribe rules and regulations for the efficient operation of all clearing and settlement systems. These sectional provisions put together validate the rules and regulations prescribed by the CBN which has revolutionised the Nigerian payments system from the traditional means to a more ICT compliant and convenient way.

Applying this to the modern payments system in Nigeria, it is an undeniable fact that these means of payments as endorsed by the CBN are promoting and facilitating an efficient and effective payment system for the settlement of transactions, even though they are not without their encumbrances.

4. Challenges of the Nigerian payments system

Despite the fact that remarkable strides have been made in the country to improve and develop a viable, secure and reliable payments system, the system is bedevilled with several problems which have continued to militate against optimal operations, growth and development. Some identifiable challenges include:[7]

4.1 Cash transactions, infrastructural deficiency and sharp practices

Considering the huge reliance on cash by bank customers, inherent dangers like armed robbery attacks, counterfeiting of currency notes and coins, inconvenience of carrying large amount of currency are still prevalent coupled with the fact that cash transactions increase the cost of currency management and it encourages money laundering and leakages. The poor state of infrastructural facilities for electronic communication and electric

[1] *Ibid*
[2] *Ibid* at 6
[3] *Ibid*
[4] *Ibid*
[5] *Ibid* at 6-7
[6] *Ibid* at 7
[7] Central Bank of Nigeria, *op.cit.,* at 15

power supply hinder the growth of electronic payments. Thus, financial institutions are compelled to incur high costs due to unreliable power supply and insecure wide area networks. The wide prevalence of sharp practices and fraudulent schemes in Nigeria undermine payment arrangements. The sharp practices include deliberate misdirection and wrong delivery of clearing instruments as well as presentation of spurious and cloned cheques to paying banks. These are associated with cases of insiders' complicity in cheques and bank draft frauds.

4.2 Distress in the financial sector, low level of literacy and large scale fraud

The recurrence of distress in the banking system negatively influences public confidence in banks and constitutes a serious threat to the smooth operations of the payments system. E-payments are a recent development in Nigeria and people find it difficult to operate because it is largely driven by knowledge-based information technology which they are not familiar with.[1] Under the e-payment platform, users are prone to fraud and loss of funds especially from system security breach by criminals.

4.3 High charges and Low level of banking habit

Withdrawing from ATMs other than that of the card issuing bank attracts additional charges of about ₦63 (Sixty Three Naira) which is deducted upon the third withdrawal in each month. There are also associated charges like VAT and commission incurred using internet banking for settlement of bills. For most people to use the e-payment platform, they must be bank account holders. Non-ownership of accounts hinders the effective use of e-payment.[2]

4.4 Poor service delivery, lack of accessibility and difficulty in accessibility to e-payment platforms

As one of the major challenges of e-payment in Nigeria, there are issues of insufficient funds in ATMs; network problem; dispensing error; some ATMs are not user friendly and old notes loaded in them make withdrawal difficult; poor human relations and very long response time when attending to customers' complaints. Some people do not have access to ATM services due to the locality and they may have to go to a major town before they are able to transact with the ATM. At times, a whole town may have just one ATM point, which makes accessibility to the ATM difficult and tiring.[3]

5.Cybercrimes perpetrated in Nigerian Banks, strategies adopted by cybercriminals and the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

The life wire of the banking sector is the internet, and currently, banks all over the world are taking advantage and incorporating opportunities brought about by e-banking. However, as the security level in this sector becomes stronger, the strength and tactics of these fraudsters increases also. Various lucrative attacks have been launched and unfortunately, many have succeeded.[4]

In general, cybercriminals execute fraudulent activities with the ultimate goal of accessing a user's bank account to either steal or transfer funds to another bank account without rightful authorisation. However, in some rare cases in Nigeria, the intention of cyber-criminals is to cause damage to the reputation of the bank by denying service to users and sabotaging data in computer networks of organizations.[5]

Significantly, the Central Bank of Nigeria (CBN) reported that 70 percent of attempted or successful fraud/forgery cases in the Nigerian banking system were perpetrated *via* electronic channels. Between 2000 and 2013, banks in the country lost ₦159 billion ($440,430,000.00) to electronic frauds and cybercrime. In 2014, bank customers lost about ₦6 billion ($16,620,000.00) in Nigeria. Indeed, security experts in the 2016 Cybersecurity Awareness Month in Lagos stated that financial losses to cybercrime may rise to $6 trillion (₦ 2,163,651,420,000,000.00) globally by 2021.[6] In the light of the above, cybercrimes perpetrated in Nigerian banks, coupled with the strategies of the cybercriminals and the implication of the Nigerian Cybercrimes Act would now be discussed.

5.1 Hacking

This is commonly known as unauthorised access and sometimes referred to as unlawful access to computers and networks.[7] This occurs where an individual without having the necessary authority, logs into and gains entry into

[1] *Ibid.*
[2] *Ibid*
[3] *Ibid*
[4] Omodunbi, B. A. , Odiase, P. O., Olaniyan O. M and. Esan, A. O, *op.cit.*, at 2
[5] *Ibid*
[6] Thisday, "Curbing Cybercrime in Nigeria"
available at <https://www.thisdaylive.com/index.php/2016/11/07/curbing-cybercrime-in-nigeria/> Last accessed 14 July 2017.
[7] See generally Eboibi, F. E., (2017) "A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015" *Computer Law & Security Review*, 33(5), pp.581 – 750 @ p. 705

computers and networks.[1] Emphatically, unlawful access can be obtained by merely logging on without permission. This may involve the use of networks to gain remote access through computers in some jurisdictions. Hackers can even use software tools to break into computers to steal data, plant viruses or carryout mischief.[2]

The perpetrators of this crime can be seen from two perspectives: persons who attack from outside the network and wrongfully access a computer without authorisation; and persons who are insiders and thus have authorisation to specific portions of the network but intrude into other parts of it by exceeding authorised access.[3]

Imperatively, these can be done by breaking the password of password-protected websites;[4] circumventing password protection on a computer; use of faulty hardware or software implementation to illegally obtain a password to enter a computer system;[5] setting up "spoofing" websites to make users disclose their passwords;[6] and installing hardware and software based key logging methods (e.g."keyloggers") that record every keystroke – and consequently any passwords used on the computer and/or device.[7] However, the Nigerian Cybercrimes Act punishes persons who indulge in the offence of unlawful access to computers in four different categories:

- By virtue of section 6(1) of the Act, where a person intentionally accesses in whole or in part, a computer system or network without authorization, for fraudulent purposes and obtains data that are vital to national security, such person is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦5,000,000.00 ($16,380.01) or both;
- But where the intent of obtaining computer data, securing access to any program, commercial or industrial secrets or classified information, section 6(2) of the Act provides the punishment to be imprisonment for a term of not more than 7 years or a fine of not more than₦7,000,000.00 ($22,932.02) or both;
- Where the person uses any device to avoid detection or otherwise prevent identification or attribution with act or omission, he shall be liable on conviction to imprisonment for a term of not more than 7 years or to a fine of not more than ₦7,000,000.00 ($22,932.02) or both such in accordance with section 6(3) of the Act, and
- Finally where a person or organization knowingly and intentionally traffics in any password or similar information through which a computer may be accessed without lawful authority, if such trafficking affects public, private or individual interest within or outside the Federation of Nigeria, by virtue of section 6(4) of the Act, liability on conviction is to a fine of not more than ₦7,000,000.00 ($22,932.02) or imprisonment for a term of not more than 3 years or both.

A major strategy utilised by cybercriminals in perpetrating hacking is data theft. Hackers' access secure or non-secure sites, then they get the data they want, use it themselves or sell it.[8] Other strategies include shoulder surfing, the use of key logger software and underground websites. Shoulder surfing involves using direct observational techniques, such as looking over someone's shoulder, to get personal information such as PIN, password, etc.[9] Key logger software involves the use of malicious software to steal sensitive information such as password, card information, etc,[10] while underground websites are used by Fraudsters to purchase personal information such as PIN, PAN, etc.

Other strategies are social media hacking, web application vulnerability, sniffing, Google hacking, session hijacking and man in the middle attack.[11] Social media hijacking has to do with obtaining personal information such as date of birth, telephone number, address, etc, from social media sites for fraudulent purposes. During web application vulnerability, attackers gain unauthorised access to critical systems by exploiting weaknesses on web applications. Sniffing on the other hand involves viewing and intercepting sensitive information as it passes through a network, while in Google hijacking, Google techniques are used to obtain sensitive information about a potential victim with the aim of using such information to defraud. Session hijacking is an unauthorised control of communication session in order to steal data or compromise the system in some manner, and man in the

[1]Barrie Gordon, Internet Criminal Law,
available at <http://www .cyberlawsa.co.za/cyberlaw/cybertext/chapter15.htm> Last accessed 10 October 2016 in Eboibi, F. E., *Ibid.*
[2]See generally Eboibi, F. E., *Ibid*
[3]Ahmad Kamal, (2005), *The Law of Cyberspace*, 1st edn., United Nations Institute for Training and Research, 17 available at www.un.int/ kamal/thelawofcyberspace, last accessed 10 October 2016, in Eboibi, F. E., *Ibid.*
[4]Sieber, Council of Europe Organized Crime Report 2004, 65 in Eboibi, F. E., *Ibid.*
[5]Mustgrove, Net Attack Aimed at Banking Data,Washington Post, 30 June, 2004 in Eboibi, F. E., *Ibid.*
[6]Sieber, Council of Europe Organized Crime Report 2004, 66 in Eboibi, F. E., *Ibid.*
[7]Sieber, Council of Europe Organized Crime Report 2004, 65 in Eboibi, F. E., *Ibid.*
[8]Nwanu, O, (2015) "E-Fraud in Nigeria: Growing or Dying Trend" *CBN NeFF 2015 Annual Report: Improving and Securing the Cyber-Environment,*18,19
[9]*Ibid.*
[10]*Ibid.*
[11]*Ibid*

middle attack involves sniffing into a bank network and capturing data so when there is a bank instruction, it can be edited to the favourable banks and accounts.[1]

Furthermore, ransomware is another strategy and it is one of the detestable malware-based attacks. Ransomware enters the computer network and encrypts the files using public-key encryption, and unlike other malware this encryption key remains on the hacker's server. Attacked users are then asked to pay huge ransoms to receive this private key.[2] Distributed denial of service (DDoS) attacks is another strategy adopted by cybercriminals. DDoS attacks entail making an online service unavailable in order to bring it down, by bombarding or overwhelming it with traffic from multiple locations and sources. Large networks of infected computers, called Botnets are developed by planting malware on the victim computers. The idea is normally to draw attention to the DDoS attack, and allow the hacker to hack into a system.[3]

5.2 Identity theft

Section 22 of the Act prohibits identity theft and impersonation. Identity theft refers to "the stealing of somebody else personal information to obtain goods and services through electronic based transactions."[4] Subsection 1 makes it an offence for any person under the employment of any financial institution and based on his special knowledge indulges in identity theft of the employer, staff, service providers and consultants with the intent to defraud is liable on conviction to imprisonment for a term of 7 years or a fine of ₦5,000,000.00 ($16,380.01) or both.[5]

Other instances of identity theft and impersonation have been expressly provided for in subsection 2. These include where a person fraudulently or dishonestly;[6]

• makes use of electronic signature, password or any other unique identification feature of any other person or fraudulently impersonates another entity or person, living or dead with the intent to; gain advantage for himself or another person;
• obtains any property or an interest in any property;
• causes disadvantage to the entity or person being impersonated or another person or avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice.[7]

In this regard, the person is liable on conviction to imprisonment for a term of 5 years or a fine of not more than ₦7,000,000.00 ($22,932.02) or both.[8] Moreover, where a person directly or indirectly makes or causes to be made, any false statement as to the material fact in writing, knowing it to be false and with the intent that it be relied upon in respect to his identity or that of any other person or his financial condition or that of any other person for the purpose of procuring the issuance of a card or other instrument to himself or another person contravenes section 22(3) of the Act and is liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than ₦7,000,000.00 ($22,932.02) or both.[9]

5.3 Phishing and Spamming

Section 32(1) of the Nigerian Cybercrimes Act criminalizes computer phishing, and it is defined as the "criminal and fraudulent process of attempting to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication…"[10] This takes place through e-mails or instant messaging, in the form of an e-mail, what appears to be one's bank, asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user.[11]

Phishing alludes to the receipt of spontaneous messages by customers of financial institutions, asking them to enter their username, secret word or other individual data to access their accounts for some reason by cybercriminals disguising as the financial institution. Customers are directed to give a response to a mail and also directed to click on the link mentioned in the mail. When they click on the given link and consequently enter the information, which were asked for in the mail received from the fraudulent institutions or banking website, unknown to the customer, the details given would be used to perpetrate fraudulent activities. By implication, the cybercriminal has admittance to the client's online financial balance available in the bank account and to the

[1]Interview with Dr. B. Nurudeen, Head, Forensic Unit, EFCC Headquarters, Wuse II, Abuja, 6 November 2017.
[2] Leadership Nigeria Newspapers, "Business Cybercrime: Nigeria's Losing Battle Against Unrelenting Enemies" available at http://leadership.ng/2017/09/30/cybercrime-nigerias-losing-battle-unrelenting-enemies/> Last accessed 20 March 2018.
[3]*Ibid.*
[4]Cybercrimes (Prohibition, Prevention, etc) Act 2015, s. 58
[5]See generally Eboibi, F.E., *(2017), op.cit*
[6]*Ibid*
[7] *Ibid*
[8] *Ibid.*
[9] *Ibid.*
[10] Cybercrime (Prohibition, Prevention, etc) Act 2015, s. 58.
[11] Cybercrimes (Prohibition, Prevention, etc) Act, 2015, s.58

funds contained in that account by making the misuse of the details received from the customer fraudulently.[1] In this regard, a cybercrime perpetrator who knowingly or intentionally engages in computer phishing is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 ($3,276.00) or both.[2]

Spamming, on the other hand, is "an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations."[3] Spamming applies to media in internet forums, instant messaging, and mobile text messaging, social networking spam, junk fax transmissions, television advertising and sharing network spam.[4]

Section 32(2) of the Nigerian Cybercrimes Act criminalizes the conduct of engaging in spamming by any person with the intent to disrupt the operations of a computer, be it public or private financial institutions. Such a cybercriminal is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 ($3,276.00) or both.[5]

A major strategy of perpetrators in phishing and spamming is the spreading of viruses, adwares, etc.[6] Subsection 3 punishes a person who is involved in malicious or deliberate spread of viruses or any malware, thereby causing damage to critical information in public, private or financial institution's computers. In this respect, such a person is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 ($3,276.00) or both.[7]

5.4 Bank Verification Number (BVN) scam

The BVN Scam is not contained in the Nigerian Cybercrimes Act 2015. However, it is a scam done through fake and unauthorised text messages, emails and calls, which is aimed at getting the BVN and other bank account details of bank customers. This is used to extort money and carry out other fraudulent activities birth out of the implementation of the BVN Policy. In addition, phishing sites were created to acquire such information for insalubrious activities on the bank account.[8]

Most times, in the text messages, there would be a number to call, and in emails, a link to follow leading to an online form where sensitive details of the Bank Account Holder would be disclosed. They usually do this in the disguise of the targeted victim's bank requiring the account holder to follow the instructions in order to activate the person's account or deactivate transaction limits due to incomplete BVN Registration.[9]

At times, the messages threaten that one would not be able to withdraw from the account, and some other times the language used is that the account has been blocked until the targeted victim calls the number contained in the text or follow the link sent. When the details are gotten, the implication is that they hack into the targeted victim's system and clear the account.[10]

Interestingly, the Economic and Financial Crimes Commission (EFCC), arraigned and secured the conviction of one Ayomide Olamide before Justice. H. O Eya of the Enugu State High Court, Enugu on a one-count charge bordering on conspiracy, impersonation, obtaining money under false pretences and ATM fraud. This was on 13 September 2017.[11] Olamide belongs to a syndicate of fraudster that specialises in tricking members of the public to disclose their Personal Identification Numbers (PIN) to avoid being deactivated from using their Automated Teller Machine (ATM) Cards.[12] The petitioner alleged that he received a text message on his phone sometime in December 2016 purportedly from United Bank for Africa (UBA) customer Care department claiming that his ATM card would be stopped from operations, due to incomplete BVN registration unless he called the bank's customer care number given as 09032578084, to update his details which he nervously did.[13] He further added that shortly after disclosing his bank details, his account was subsequently debited to the tune of ₦75,900.00 (Seventy Five Thousand Naira Only)($207.75). Investigation carried out on the matter revealed that the convict actually sent out SMS messages and used monies realised from his nefarious act to buy mobile phone airtime online. Justice Eya thereafter sentenced him to five months imprisonment

[1] Rathore and Marwaha, *op.sit at 3*
[2] Cybercrime (Prohibition, Prevention, etc) Act 2015, s.32(1); see also Eboibi, F. E., *(2017), op.cit*
[3] *Ibid*
[4] Technopedia, "Spamming" available at <https://www.techopedia.com/definition/23763/spamming> Last accessed 20 March 2018.
[5] See also Eboibi, F. E., *(2017), op.cit*
[6] Technopedia, "Spamming" available at <https://www.techopedia.com/definition/23763/spamming> Last accessed 20 March 2018.
[7] See also Eboibi, F. E., *(2017), op.cit*
[8] Omodunbi, Odiase, Olaniyan and Esan, *(2017), op.cit* at 12
[9] Bella Naija, "Oma: Beware, Scammers are on the Prowl Trying to Use a BVN Related Email" Available at <https://www.bellanaija.com/2015/11/oma-beware-scammers-are-on-the-prowl-trying-to-use-a-bvn-related-email/> Last accessed 8 November, 2018.
[10] *Ibid*
[11] EFCC, "EFCC Secures Conviction of ATM Fraudster" available at <https://efccnigeria.org/efcc/news/2741-efcc-secures-conviction-of-atm-fraudster> Last accessed 21 March 2018.
[12] *Ibid*
[13] *Ibid*

commencing from the date of arrest and detention.[1]

Imperatively, a classic BVN scam case is *FRN v. Innocent Clinton and Another*,[2] where the EFCC secured the conviction of Innocent Uche Clinton and Emmanuel Okanni before Justice Sa'ad Muhammad of the Gombe State High Court on a two count charge bordering on conspiracy and theft. The convicts specialised in duping innocent people by obtaining their bank verification numbers using the trick that their accounts had been closed due to BVN issues. They were arrested by Operatives of the Gombe Zonal office of the EFCC in Imo State following a petition by one Ibrahim Bala Gwamna, alleging that on 7 December, 2016 he received a call from one Kingsley who presented himself as a staff of Diamond Bank and asked him whether his mobile banking is working to which he answered in the negative. Later, he received a text message purportedly from Diamond Bank instructing him to call a particular phone number as customer care in order to lodge his complaint. Few minutes after complying, he received an alert that the sum of ₦864,000.00 ($2,393.28) was transferred from his account into the convicts' accounts. Upon arraignment, they pleaded guilty to the charge and were accordingly convicted and sentenced to six months imprisonment each. They however received the option of ₦30,000 ($83.10) fine.[3]

The common strategy used by cybercriminals to perpetrate BVN Scam is phishing and social engineering. Social engineering is a method where the cyber criminals make a direct contact with a target using emails or phones – mostly the latter. They try to gain the target's confidence and once they succeed at it, they get the information they need. This information can be about the target's money, company where he works or anything that can be of interest to the cyber criminals.[4]

5.5 Theft of bank cards

The theft of bank cards has evolved from the physical theft of the card to simply the theft of the numbers. Today, bank card hackers do not need to be in the same country to steal other people's identities.[5] Bank Card in this context means any instrument, token, device, or card whether known as a bank service card, banking card, cheque guarantee card, or debit card or by any other similar name, issued with or without a fee by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value or for the use in automated banking device to obtain money or any of the services offered through the device.[6] Section 34 of the Nigerian Cybercrimes Act provides that any person, other than the issuer, who receives and retains possession of two or more cards issued in the name or names of different cardholders, which cards he knows were taken or retained under circumstances which constitute a card theft commits an offence and is liable on summary conviction to 3 years imprisonment or to a fine of N1,000,000 ($3,276.00) and shall further be liable to repayment in monetary terms the value of loss sustained by the cardholder or forfeiture of the assets or goods acquired with the funds from the account of the cardholder.

Furthermore, section 35 of the Nigerian Cybercrimes Act creates criminal liability for acts constituting purchase or sale of card of another. This occurs where a person, other than an issuer or his authorized agent, either sells a card to or buys a card from a person other than an issuer or his authorized agent. That person is liable on summary conviction to a fine of ₦500,000.00 ($1,638.00) and is further liable to pay, in monetary terms, the values of loss sustained by the card holder or forfeit the assets or goods acquired with the funds from the account of the cardholder.[7] Cybercriminals make use of hidden cameras to record ATM card pins and numbers in distinct places such as an eatery payment using POS, or at the ATM to perpetrate this crime.[8]

5.6 Cyber-theft / banking fraud/ Computer Related Fraud

By virtue of Section 14(1) of the Nigerian Cybercrimes Act, any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits on himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less that ₦7,000,000 ($22,932.02) or both fine and imprisonment.

More so, subsection 2 provides to the effect that any person who with intent to defraud sends electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and shall be liable on conviction to imprisonment for a term of not less than 5 years and to a fine of not less than ₦10,000,000 ($27,700.00) or to both fine and

[1] *Ibid*
[2] EFCC, "Court Jails Two for N.8m BVN Scam" available at <https://efccnigeria.org/efcc/news/2410-court-jails-two-for-n-8m-bvn-scam> Last accessed 21 March 2018.
[3] *Ibid.*
[4] Leadership Nigeria Newspapers, *op.cit*.
[5] Omodunbi, Odiase, Olaniyan and Esan, *supra, note* 1 at 12
[6] Cybercrimes (Prohibition, Prevention, etc) Act 2015, s. 58
[7] Cybercrimes (Prohibition, Prevention, etc) Act 2015, s.35; see also Eboibi, F. E., *(2017), op.cit*.
[8] Omodunbi, Odiase, Olaniyan and Esan, *op.cit* at 12

imprisonment.

Some of the strategies adopted in the perpetration of this crime include franking electronic messages and instructions; super scribing electronic messages and instructions; short paying or over paying employees either by themselves or conniving with an employee of a financial institution. Emphatically, hackers target the vulnerabilities in the security of various bank systems and transfer money from innumerable accounts to theirs. Most cyber-criminals transfer bantam amounts like 5 naira which are sometimes overlooked by the user without questions raised by the users who assumes this was deducted for either SMS or ATM withdrawal charges. Doing this for over a million accounts enriches most cybercriminals.[1]

As a matter of fact, all of these strategies are criminalised in subsections 3, 4 and 5 respectively: imprisonment for a term of not more than 3 years or a fine of not more than N5,000,000 ($16,380.01) or to both such fine and imprisonment; imprisonment for a term of not more than 7 years and forfeiture of proprietary interest in the stolen money or property to the bank, financial institution or the customer; imprisonment of not more than 5 years or a fine of not more than N7,000,000 ($22,932.02) or to both fine and imprisonment.

In *FRN v. Solomon Uchendu and 2 Ors*,[2] the Economic and Financial Crimes Commission (EFCC), on Wednesday, February 3, 2015 arraigned the trio of Solomon Uchendu, Ndubisi Agu and Uchendo Chikwadu before Justice D. V. Agishir of the Federal High Court sitting in Enugu, Enugu State for cybercrimes bordering on obtaining by false pretence and Advanced Fee Fraud. Furthermore, another practical cybercrime case is that of *FRN v. Uchenna Nwako and 4 Ors.*[3] The EFCC, on Monday, May 11, 2015 arraigned Uchenna Nwako, Ejikeme Oluchukwu, Nnamani Ikechukwu, Ibeh kodili Martins and Nwako Victoria Ifeoma before Justice D.V. Agishir of the Federal High Court, Enugu, on a 16-count charge bordering on intent to defraud and obtaining ₦26,338,000 ($72,956.26) by false pretence. The five accused persons were picked up by EFCC operatives on February 27, 2013 after intelligence reports indicated that they were involved in fraudulent activities bordering on cybercrime.

Other strategies include shoulder surfing, the use of key logger software and underground websites. Shoulder surfing involves using direct observational techniques, such as looking over someone's shoulder, to get personal information such as PIN, password, etc.[4] Key logger software involves the use of malicious software to steal sensitive information such as password, card information, etc,[5] while underground websites are used by cybercriminals to purchase personal information such as PIN, PAN, etc.

Disgruntled employee is another strategy used by cybercriminals. This entails using banking staff who act as insiders to certain cybercrimes. Due to the fact that they are aggrieved, they form alliance with cybercriminals to make extra money.[6]

5.7 Electronic cards related fraud

Electronic cards which this cybercrime apply to are: debit cards; credit cards; charge cards; loyalty cards; magnetic stripe based cards; smart chip based cards; EMV cards; passwords; personal identification number (PIN); electronic plate; electronic serial number; code number; mobile identification number; any account number or other telecommunications service, equipment, or instrument identifier, or other means of account access including telephones, PDAs, etc; Automatic Teller Machines; Point of Sales Terminals; other vending machines.[7]

Section 33 of the Act creates criminal liabilities for electronic cards related fraud. Subsection1 prohibits the use of any access device including credit, debit, charge, loyalty and other types of financial cards, to obtain cash, credit, goods or service by any person with the intent to defraud. Liability for such a person is on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 ($16,380.01) or to both fine and imprisonment and also liable to pay, in monetary terms, the value of loss sustained by the owner of the credit card.[8] Subsection 2 concerns a situation where a counterfeit access device, an unauthorized access device, or an access device issued to another person is used by a person that results in a loss or gain. Here, the person is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 ($16,380.01) and forfeiture of the advantage or value derived from his act.[9]

Moreover, by virtue of subsection 3, circumstances which permit the stealing of an electronic card by a

[1] *Ibid* at 3
[2] EFCC, available at <https://efccnigeria.org/efcc/news/1160-efcc-arraigns-youth-corps-member-two-others-for-cybercrime> Last accessed 21 March 2018.
[3] EFCC, available at <https://efccnigeria.org/efcc/news/1330-efcc-arraigns-five-suspected-internet-fraudsters> Last accessed 21 March 2018.
[4] Nwanu, O, (2015) "E-Fraud in Nigeria: Growing or Dying Trend"*CBN NeFF 2015 Annual Report: Improving and Securing the Cyber-Environment,*18,19
[5] *Ibid*
[6] *Ibid*
[7] Cybercrime (Prohibition, Prevention, etc) Act 2015, s.58; see also Eboibi, F.E, *(2017), op.cit*.
[8] Cybercrime (Prohibition, Prevention, etc) Act 2015, s.33(1); see also Eboibi, F. E., *(2017), op.cit*.
[9] See generally Eboibi, F. E., *supra, note* 35.

person, creates liability on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00 ($3,276.00) and also liability to repay in monetary terms the value of the loss sustained by the card holder or forfeit the assets or goods acquired with the funds from the account of the cardholder.[1]

Subsection 4 is in respect to the receiver of a card who knowingly, or who ought to have known, that the card is lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder and who retains possession with the intent to use, sell or to traffic it to a person other than the issuer or the cardholder. Here, the person is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00 ($3,276.00) and further liable to pay, in monetary terms, the value of loss sustained by the cardholder.[2] Subsection 5 relates to a situation where a person obtains control over a card as security for a debt with the intent to defraud the issuer, a creditor, or any other person. Liability is on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦3,000,000.00 ($9,828.00) or both and further liable to pay, in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.[3]

By virtue of subsection 6, a person who signs a card other than the cardholder or a person authorized by him with the intent to defraud the issuer or a creditor is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00 ($3,276.00).[4]

In accordance with subsection 7, a person is possessed with the intent to defraud the issuer or a creditor where they use, for the purpose of obtaining money, goods, services or anything else of value, a card obtained or retained fraudulently or a card which the perpetrator knows is (i) forged or expired, or (ii) who obtains money, goods, services, or anything else of value by representing, without the consent or authorization of the cardholder, that he is the holder of a specified card, or (iii) by representing that he is the holder of a card and such card has been validly issued.[5] Upon conviction the person is liable on to imprisonment for a term of not more than 3 years and a fine of not more than ₦1,000,000.00 ($3,276.00).[6]

Subsection 8 relates to circumstances where a creditor, with the intent to defraud the issuer or the cardholder (i) thereby furnishes goods, services, or anything else of value upon penetration of a card, which within his knowledge is obtained or retained fraudulently or illegally, or (ii) a card that within his knowledge is forged, expired, or revoked. That person is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00 ($3,276.00) or to both fine and imprisonment.[7]

Subsection 9 concerns a situation where a creditor who, with the intent to defraud the issuer or the card holder, fails to furnish goods, services, or anything of value which he represents in writing to the issuer or the cardholder that he has furnished. That person is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000.000.00 ($3,276.00) or both.[8]

Subsection 10 involves a person who is authorized by a creditor to furnish goods, services, or anything else of value upon presentation of a card or card account number by a cardholder, or any agent or employee of such person, who, with intent to defraud the issuer or the cardholder, presents to the issuer or the cardholder, for payment, a card transaction record of sale, which sale was not made by such person or his agent or employee. That person is liable on summary conviction to a fine of not more than ₦500,000.00 ($1,638.00) and to imprisonment for a term of 3 years.[9]

Subsection 11 deals with a person who, without the creditor's authorization, employs, solicits or otherwise causes a person who is authorized by the creditor to (i) furnish goods, services, or anything else of value upon presentation of card account number by the cardholder, or (ii) employs, solicits or otherwise causes an agent or employee of such authorized person, to remit to the creditor a card transaction record of a sale that was not made by such authorized person or his agent or employee. That person is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00 ($3,276.00) or both.[10]

Subsection 12 pertains to anyone who is found to be in possession of counterfeit cards, invoices, vouchers, sales drafts, or other representations or manifestations of counterfeit cards, or card account numbers of another person with intend to defraud. Such person is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦3,000,000.00 ($9,828.00) or both. Subsection 13 deals with a receiver, possessor, buyer, seller, controller or anyone who is in custody of any card-making equipment with the intention that such equipment be used in the manufacture of counterfeit cards. Such a person is liable on conviction to

[1] *Ibid*
[2] *Ibid*
[3] *Ibid.*
[4] *Ibid*
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid.*

imprisonment for a term of not more than 5 years or to a fine of not more than ₦7,000,000.00 ($22,932.02) or both.[1]

Subsection 14 deals with anyone who falsely alters an invoice for money, goods, services, or anything else of value obtained by use of a card after that invoice has been signed by the cardholder or a person authorized by him, with the intention to defraud. That person is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦5,000,000.00 ($16,380.01) or both. Where, without the prior written consent of the cardholder, an institution makes available, lends, donates, or sells any list or portion of a list of cardholders and their addresses and account numbers to any person, by virtue of subsection 15 the institution is liable on conviction to a fine of ₦10,000,000.00 ($32,760.03).[2]

However, by virtue of subsection 16, an institution may make available to the Central Bank of Nigeria or a licensed credit bureau, which seeks to determine only the cardholders' rating, any list or portion of a list of any cardholder and their addresses without the permission of the cardholder. However, they shall, within 7 working days, give notice in writing of the disclosure to the cardholder. An institution which fails to comply with the requirement to notify the cardholder is liable on conviction to a fine of not more than ₦1,000,000.00 ($3,276.00).[3]

Accordingly, if any person steals an ATM, such person commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than N10,000,000 ($32,760.03) or to both fine and imprisonment, and forfeiture applies.[4] Meanwhile, for attempts to steal an ATM, upon conviction the perpetrator shall be liable to imprisonment for a term of not more than 1 year or a fine of not more than N1,000,000 ($3,276.00) or both fine and imprisonment.

Additionally, any person who manipulates an ATM machine or Point of Sales terminals with the intention to defraud shall be guilty of an offence and upon conviction be sentenced to five years imprisonment or N5,000,000 ($16,380.01) fine or both.[5] Where any employee of a financial institution is found to have connived with another person or group of persons to perpetrate fraud using an ATM or POS device, such person shall be guilty of an offence and upon conviction sentenced to seven years imprisonment without an option of fine. A classical example is the case of *FRN v. Abdulhakeem Daudu,*[6] Justice Kuewumi Babs of the Federal High Court sitting in Lagos convicted and sentenced Abdulhakeem Daudu to three years imprisonment for credit card fraud. The convict was arraigned for 3.8 million naira ($10,526.00) scam on a two-count charge bordering on possession and fraudulent use of credit card.

Notably, one of the strategies adopted by cybercriminals in the perpetration of electronic card related fraud is cross channel fraud. This is a situation whereby customer information is obtained from one channel, (for instance a call centre) and is used to carry out fraud in another channel, for example, the ATM.[7] Sometimes cybercriminals use phone calls to solicit personal information from their victims. This is known as vishing.[8] Other strategies include shoulder surfing, the use of key logger software and underground websites. Shoulder surfing involves using direct observational techniques, such as looking over someone's shoulder, to get personal information such as PIN, password, etc.[9] Key logger software involves the use of malicious software to steal sensitive information such as password, card information, etc,[10] while underground websites are used by Fraudsters to purchase personal information such as PIN, PAN, etc.

Moreover, ATM skimming is another strategy cybercriminals use**.** It is a method that involves placing an electronic device on an ATM that scoops information from a bank card's magnetic strip whenever a customer uses the machine. Also, another cybercrime carried out via this means in Nigeria includes internet order fraud. Internet order fraud involves fraudsters inputting stolen cards numbers on online commercial sites to order goods. Credit card numbers or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction. Different applications can be used to retrieve this information such as key loggers at cybercafés or cloned websites.[11]

5.8 Email fraud

Section 36 of the Act prohibits the use of fraudulent device or attached e-mails and websites. This occurs where

[1] *Ibid.*
[2] *Ibid.*
[3] *Ibid.*
[4] Cybercrimes (Prohibition, Prevention, etc) Act 2015, s.15(c)
[5] Cybercrimes (Prohibition, Prevention, etc) Act 2015, s.30(1)
[6] EFCC, available at <https://efccnigeria.org/efcc/news/1840-n3-8m-scam-court-jails-credit-card-fraudster-3-years> Last accessed 21 March 2018.
[7] Nwanu, O, (2015) "E-Fraud in Nigeria: Growing or Dying Trend" *CBN NeFF 2015 Annual Report: Improving and Securing the Cyber-Environment,*18,19
[8] *Ibid.*
[9] *Ibid.*
[10] *Ibid*
[11] Omodunbi, Odiase, Olaniyan and Esan, *op.cit* at 12

a cybercrime perpetrator uses any device or attachment, e-mail or fraudulent website to obtain information with the intention to defraud. That person is liable on conviction to imprisonment for a term of 3 years or to a fine of ₦1,000,000.00 ($3,276.00) or both by virtue of subsection 1.[1]

Subsection 2 relates to a situation where a person fraudulently re-directs funds transfer instructions during transmissions over any authorized communications path or device and then re-directs funds transferred electronically within an authorized account. That person is liable on conviction to imprisonment for a term of 3 years or to a fine of ₦1,000,000.00 ($3,276.00) and is further liable to pay, in monetary terms, the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.[2]

A common strategy used in perpetrating email fraud by hackers or evil organizations, is that they send email to bank customers attaching a link through which unsuspecting bank customers would fill in their account details.[3] The implication of this is loss of funds from the disclosed account details.

In the case of a person who perpetrates the electronic fraud or online fraud using a cybercafé, he shall be guilty of an offence and shall be sentenced to three years imprisonment or a fine of ₦1,000,000 ($3,276.00) or both.[4] In the event of proven connivance by the owners of the cybercafé, such owners shall be guilty of an offence and shall be liable to a fine of ₦2,000,000 ($6,552.00) or a 3 years jail term or both.[5]

A strategy these cybercriminals adopt is email spoofing. In this instance, the header information is changed in an email message in order to hide identity and then, they make the email appear to have originated from a trusted authority.[6]

5.9 System interference

Flowing from section 8 of the Nigerian Cybercrimes Act 2015, system interference is said to have occurred where without lawful authority, a cybercriminal intentionally or for fraudulent purposes does an act that causes directly or indirectly the serious hindering of the functioning of a computer system. This is by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose.

Resultantly, financial losses become what victims are faced with. This is made possible by physical attacks on the computer system and it includes strategies like inserting metal objects in computer devices to cause electrical shorts or blowing hairspray into sensitive devices or cutting cables.[7] Web-based frauds pose many difficulties for cyber citizens and legal systems. Instances of theses remote attacks against computer systems include: computer worms or denial-of-service (DoS) attacks.[8]

Section 8 of the Nigerian Cybercrimes Act 2015 imposes a punishment for imprisonment for a term of not more than 2 years or to a fine of not more than ₦5,000,000.00 ($16,380.01) or both against person(s) who engages in acts resulting to system interference. This offence is also repeated in section 16(3) of the Act with the same punishment attached therein.[9]

Furthermore, it has been noted that the CBN itself can be a victim of cyber-attack which can compromise its system and paralyse its activities in the course of dispensing its responsibilities. Instances may include an attack on a central bank operated Real Time Gross Settlement (RTGs) system which may disrupt the settlement of inter-bank transactions.[10] The compromise of network for submission of financial data to the central bank can lead to manipulation of figures which may produce misrepresentation of the financial position of supervised financial institutions.[11] Additionally, other attacks may include diversion of funds through the transfer system, concealment and integration of laundered money, uncontrolled money creation activities, etc are possibilities through cyber-attacks.[12]

6. International dimensions to cybercrime

It is feasible to use the advanced methods applicable in the countries fighting cybercrime for long and

[1] see also Eboibi, F. E. *(2017), op.cit*.
[2] Cybercrime (Prohibition, Prevention, etc) Act 2015, s.36(1) & (2); see also Eboibi, F. E., *ibid.*
[3] *Ibid*
[4] Cybercrimes (Prohibition, Prevention, etc) Act 2015, s.7(2)
[5] *Ibid*, s.7(3)
[6] Nwanu, O, (2015) "E-Fraud in Nigeria: Growing or Dying Trend" *CBN NeFF 2015 Annual Report: Improving and Securing the Cyber-Environment,*18,19
[7] Sieber, Council of Europe Organized Crime Report 2004, 107 in Eboibi, F. E., *(2017), op.cit.*
[8] See generally Eboibi, F. E., *supra, note* 7 at 706.
[9] *Ibid.*
[10] kinwunmi, A.O., (2012) "Central Banking and Cyber Threats: Implications and Management of Emerging Risks" *Central Bank of Nigeria Bullion*,(36(1), 31,33
[11] *Ibid*.
[12] *Ibid* at 34

successfully. Mainly, those are that of Advanced Economies like the United Kingdom(UK), the United States of America(US), Canada and Germany. However, lessons can also be drawn from Emerging Economies like South Africa, Malaysia, Indonesia and Brazil, as well as Developing Economies like Kenya, Uganda, Ghana, Botswana, *inter alia.*

Using the US as a case study, the Department of Homeland Security (DHS) works with other federal agencies to conduct high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools. Criminal investigators and network security experts with deep understanding of the technologies malicious actors are using and the specific vulnerabilities they are targeting work to effectively respond to and investigate cyber incidents.[1]

More so, the U.S. Secret Service and U.S. Immigration and Customs Enforcement (ICE) have special divisions dedicated to combating cybercrime. To add to this is the Social Security Number (SSN) Policy in the US which contains comprehensive data of each citizen thereby assisting in tracking suspects in any event of cybercrime, *inter alia.*[2]

Furthermore, in the UK, the National Cyber Crime Unit (NCCU) leads the UK's response to cybercrime, supports partners with specialist capabilities and coordinates the national response to the most serious of cybercrime threats.[3] Working closely with the Regional Organised Crime Units (ROCUs), the MPCCU (Metropolitan Police Cyber Crime Unit), partners within Industry, Government and International Law Enforcement, the NCCU has the capability to respond rapidly to changing threats. The NCCU has the capability to respond in fast time to rapidly changing threats and collaborates with partners to reduce cybercrime.[4]

Similarly, other Advanced Economies like Germany and Austria have adopted quite a number of strategies to combat cybercrime and it will be a whole lot better if Nigeria can adopt vital strategies from Advanced Economies in order to aid the country achieve her goal of minimising the perpetration of cybercrime to the barest minimum. Some of these strategies adopted by Germany include national data protection laws, the launch of a new Cyber and Information Space Command (CIS) to tackle attacks from hackers and foreign spy agencies,[5] the strategic policies on Cyber defense and Cybersecurity which do not just tackle present cybercrimes but future cyber-attacks, with the monitoring of foreign social media.[6]

On the part of Australia, Australia embraces a comprehensive strategy of strong cyber defences, regional capacity building and national law enforcement efforts in its fight against cybercrime. They are into collaboration at different levels efforts to protect Australians from the harm of cybercriminals. The 2016 Cyber Security Strategy committed the Government to enhance Australia's ability to respond to cyber security threats, including cybercrime. In 2017, the Government directed the Australian Signals Directorate (ASD) to use its offensive cyber capabilities to disrupt, degrade, deny and deter organised offshore cybercriminals. This capability is subject to stringent oversight, and consistent with domestic law and our obligations under international law. Strong cyber defences and law enforcement measures will continue to sit at the forefront of our response to cybercrime threats.[7]

7. Conclusion and the way forward

The cybercrimes perpetrated in Nigerian banks include hacking, identity theft, BVN scam, phishing and spamming, card theft, computer related fraud, electronic cards related fraud, email fraud and system interference. Obviously, these identified crimes are still being perpetrated by cybercriminals. Arguably, there is no functional computer response team comparable to what is obtainable in the developed economies with the ability to respond immediately to cyber initiated attacks against the banking industry and their customers.[8] Successes can only be achieved in these circumstances by cooperating with international institutions and organisations, which is arguably lacking in the banking industry's fight against cybercrimes.[9] A major drawback is the absence of a

[1] Homeland Security, "Combating Cyber Crime" available at <https://www.dhs.gov/topic/combating-cyber-crime> Last accessed 21 March 2018.
[2] *Ibid*
[3] "National Cyber Crime Unit" available at < http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit> Last accessed 21 March 2018.
[4] *Ibid.*
[5] Euronews, "Germany Army Launches New Cyber Command" Available at <https://www.euronews.com/2017/04/06/germany-army-launches-new-cyber-command> Last accessed 20 November 2018.
[6] M. Mayer, L. Martino, "Cyber Defense and Cyber Security " p.24 Available at <https://www.google.com.ng/url?sa=t&source=web&rct=j&url=https://www.rise.unifi.it/upload/sub/eu-conference--may-6_mayer.pdf&ved=2ahUKEwik8NqRifeAhVGQRoKHbh_AhwQFjAFegQIARAB&usg=AOvVaw1BRqe62tbxppCl4uPDiRwF&cshid=154285886273> Last accessed 20 November 2018.
[7] Australia's International Cyber Engagement Strategy, "Cybercrime" Available at <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/part_3_cybercrime.html> Last accessed 20 November 2018.
[8] See 6. International dimensions to cybercrime
[9] *Ibid.*

centralized data base in Nigeria which would have assisted financial institutions and law enforcement agents to trace and track perpetrators of cybercrimes in the banking industry compared to what is obtainable in the US and UK.[1]

Drawing lessons from advanced economies like the United States of America, which has the Social Security Number (SSN) Policy, Nigeria, suffers lack of proper identification and record keeping system of her citizens and this has contributed to level of cybercrime and unsuccessful prosecutions especially when suspects cannot be traced. Essentially, the SSN contains the compiled details of citizens of the U.S.A. and it is updated as their citizens grow, travel and advance. As a matter of fact, this has aided investigations, but particularly the fight against crimes. Hence the Federal Government of Nigeria needs to expand the database a little more from where it is right now. Consequently, it is humbly recommended that the National Identification Scheme be enforced, whereby all Nigerians will be registered in the NIC Portal, and the details of all nationals should be linked to their respective BVN and mobile numbers. More so, all details relating to Permanent Voters Card (PVC), International Passport, Driver's License, should be compiled in the same record. This will in turn bring to a halt the unnecessary multiplicity of Identification numbers each Nigerian citizen tend to have.

Accordingly, considering the nature of cybercrime, especially the fact that it transcends boundaries, international cooperation is advised. Thus, Advanced Economies, Emerging Economies, and Developing Economies all over the world should pull resources together and adopt practical measures to wade off this universal menace. As discussed earlier in this research work, this is a major approach adopted by advanced countries in the fight against cybercrime. As they fight cybercrime, they take measures to tackle future cyber-attacks that have the potential to affect the countries and citizens.

Nevertheless, it is also recommended that the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 should be amended to incorporate all cybercrimes perpetrated in the banking industry like that of the BVN scam and cyber money laundering. Concurrently, the Act should be more specific about who can prosecute cybercrimes and enforce the Act as Section 41(1) of the Act merely mentions "the office of the National Security Adviser" as the coordinating body for all security and enforcement agencies. Furthermore, the Act established the Cybercrime Advisor Council in Section 42(1) of the Act without expressly clothing it with the powers to enforce the Act. This is contrary to the Economic and Financial Crimes Commission (Establishment) Act, 2004 that established the EFCC in Section 1 and spelt out her functions and powers in Sections 6 and 7, which includes her power to enforce the EFCC Act. The absence of similar express provision in the Cybercrimes Act makes it vague and as such needs revisiting.

Undoubtedly, payments system in Nigeria has revolutionised from traditional to modern, and interestingly there is a legal framework validating this advancement i.e the CBN Act. Notwithstanding, just as mentioned earlier, there are challenges accompanied by the revolutionised payments system but we see that the CBN is at the forefront in ensuring a more efficient and effective payments system. Hopefully, in a matter of time, the payments system would be more advanced and efficient than what we have today.

Instructively, the Nigerian Cybercrimes Act places certain duties on financial institutions to checkmate cybercrime activities in the banking industry as seen in Section 37. Some of these duties include verifying the identity of customers carrying out electronic transactions and applying the principle of KYC in documentation of customers preceding execution of customers' electronic transfer, payment, debit and issuance orders. Materially, the banking industry has become a key target for cyber criminals by the nature of their stock in trade money. The speed at which frauds can be effected through malicious attacks on the financial system has assumed alarming degree. It took only four hours for fraudsters to carry out coordinated withdrawal of $45 million dollars from ATM networks of banks across various countries around the world.[2] It is in this light that this research work has discussed decided cybercrime cases in Nigeria and exposed the strategies adopted by cybercriminals in the perpetration of cybercrimes in the banking industry. Apparently, the systems and communication networks that provide accessibility for usage in our daily transactions are potential targets of cybercriminals,[3] and it is imperative that more security measures are taken to minimise cybercrime in the banking industry, while the law enforcement agencies particularly the EFCC should endeavour to be at their best to prosecute cybercriminals. Nevertheless, it is necessary to state at this point that not all the cybercrimes perpetrated in the banking industry are provided for in the Cybercrimes Act, for example, the BVN scam and cyber money laundering. This is indeed a cause for concern and such acts that amount to cybercrime should be criminalised by Nigerian legislation.

References

Books

Clancey, T. K., (2011) *Cybercrime and Digital Evidence: Materials and Cases.* San Francisco: Lexis Nexis.

[1] *Ibid.*
[2] A. O. Akinwunmi, *op.cit*
[3] *Ibid*

Clough, J., (2010) *Principles of Cybercrime*. Cambridge, United Kingdom: Cambridge University Press.
Eboibi, F.E.(ed), (2018) *Handbook on Nigerian Cybercrime Law.* Benin: Justice Jeco Printing & Publishing Global.
Garner, B. A., (2009) *Black's Law Dictionary*, 9th edn. United States of America: West Publishing Cow.
Jimoh, L. S. (2012) *The Mandate of the Central Bank of Nigeria.* Series No. 19, Understanding Monetary Policy Series 1.
Koops B. J. and Brenner S. W. (ed.), (2006) *Cybercrime and Jurisdiction, A Global Survey*. Hague: T.M. C Asser Press.

Journal Articles

Akinwunmi A. O. (2012) "Central Banking and Cyber Threats: Implications and Management of Emerging Risks" *Central Bank of Nigeria Bullion*,(36)1, 31
Eboibi, F.E, (2017) "A Review of the Legal and Regulatory Frameworks of Nigerian Cybercrimes Act 2015" *Computer Law & Security Review*, 33(5),581 – 750
Gul Z. and Terkesli R.(2012) "Crime of the Millennium: Cybercrime" *Humanity and Science Journal*, (7)1, 18.
Islam, S. (2015) "An Algorithm for Electronic Money Transaction Security (Three Layer Security): A New Approach" *International Journal of Security and it's Applications,* (9(2), 203, available at <http://DX.doi.org/10.142527ijsla.2015.9.2.19> Last accessed 12 July 2017.
Nwanu, O. (2015) "E-Fraud in Nigeria: Growing or Dying Trend" CBN NeFF *2015 Annual Report: Improving and Securing the Cyber-Environment*, 18
Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M and Esan, A. O.(2016) "Cybercrimes in Nigeria: Analysis, Detection and Prevention" *Federal University Oye Ekiti Journal of Engineering and Technology,* (1)1, 1.
Rathore, D. S. H. and Marwaha, K. (2015) "Cybercrime in Banking Sector" *International Monthly Journal*, (2)7, 1.
Tassebehji R. and Kamala M. A., (2012) "Evaluating Biometrics for Online Banking: The Case for Usability" *International Journal of Information Management*, 32, available at <www.elsevier.com/locate/ijinfomgt> Last accessed 12 July 2017

Internet Materials

Ahuja A.V, "Cybercrime in Banking Sector" available at <http://www.scribd.com/mobile/doc/28079943/Cyber-crime-in-Banking-sector>Last accessed 15 July 2017.
Biometric Update, "Nigeria's Central Bank Extends Biometric Identification Deadline" available at <http://www.biometricupdate.com/201507/nigerias-central-bank-extends-biometric-identification-deadlin> Last accessed 20 March 2018.
EFCC, "EFCC Secures Conviction of ATM Fraudster" available at <http://EFCC Nigeria.org/EFCC/news/2741-efcc-secures-conviction-of-atm-fraudster> Last accessed 21 March 2018.
EFCC, available at <http://efccnigeria.org/EFCC/news/1840-n3-8m-scam-court-jails-credit-card-fraudster-3-years>Last accessed 21 March 2018 EFCC, available at <http://efcc.nigeria.org/efcc/news/1160-efcc-arraigns-youth-corps-members-two-others-for-cybercrime> Last accessed 21 March 2018.
EFCC, available at <http://efccnigeria.org/efcc/news/1330-efcc-arraigns-five-suspected-internet-fraudsters> Last accessed 21 March 2018.
EFCC, "EFCC Secures Conviction of ATM Fraudster" available at <http://efccnigeria.org/efcc/news/2741-efcc-secures-conviction-of-atm-fraudster>Last accessed 21 March 2018.
EFCC, "Court Jail's Two for ₦8m BVN Scam" available at <http://efccnigeria.org/efcc/news/2410-court-jails-two-for-n-8m-bvn-scam> Last accessed 21 March 2018.
Ejike, S. "Court adjourns leaving of BVN matter till March 1 at FG's instance" available at <http://www.tribuneonlineng.com/adjourns-fg-access-bank-19-other-banks-bvn-case> Last accessed 21 March 2018.
Gross Archive, "The Role of Central Bank of Nigeria in the Development of Money Market" available at <http://www.grossarchive.com/upload/1414764202.htm> Last accessed 10 July 2017.
Homeland Security, "Combating Cybercrime" available at <http://www.dhs.gov/topic/combating-cyber-crime> Last accessed 21 March 2018
Kreazetofa Odey, "Bank Customers With BVN Rise To 31.4m In 2017- NIBSS" available at <http://www.google.com.ng/amp/s/leadership.ng/2018/01/19/bank-customerw-bvn-rise-31-4m-2017-nibss/amp/> Last accessed 20 March 2018.
Law Yard, "Federal Government Set To Take Over Bank Account Without BVN As Court Grants Order" available at <http://www.lawyard.ng/federal-government-set-to-take-over-bank-accounts-without-bvn-as-court-grants-order/> Last accessed 21 March 2018.
"National Cyber Crime Unit" available at <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-unit> Last accessed 21 March 2018.

Nairaland Forum, "who is a yahoo-yahoo boy" available at <http://www.nairaland.com/71121/yahoo-yahoo-boy> Last accessed 10 July 2017.
Nnochiri, I. "Court vacates interim forfeiture order on accounts without BVN" available at http://www.google.com.ng/amp/s/www.vanguardngr.com/2017/11/court-vacates-interim-forfeiture-order-accounts-without-bvn/amp/> Last accessed 21 March 2018.
Technopedia,"Spamming" available at http://www.technopedia.com/definition/23763/spamming> Last accessed 20 March 2018.

Online Newspapers

Leadership Nigeria Newspapers, "Business Cybercrime: Nigeria's Losing Battle Against Unrelenting Enemies" available at
<http://leadership.ng/2017/09/30/cybercrime-nigerias-losing-battle-unrelenting-enemies/> Last accessed 20 March 2018.
Premium Times Nigeria, "Nigeria Ranks 3rd in Global Internet Crimes Behind UK, U.S.- NCC" available athttp://www.google.com.ng/amp/s/www.premiumtimesng.com/news/top-news/241160-nigeria-ranks-3rd-global-internet-crimes-behind-uk-u-s-ncc.html/amp> last accessed 16 March 2018.
The Guardian, "Financial Institutions and Challenges of Cybercrime"available at http://guardian.ng/business-services/money/financial-institutions-and-challenges-of-challenges-of-cybercrime/> last accessed 7 July 2017.
Thisday, "Curbing Cybercrime in Nigeria" available at
<http://www.thisdaylive.com/index.php/2016/11/07/curbing-cybercrime-in-nigeria/>last accessed 6 July 2016.

Interviews

Interview with Dr. B. Nurudeen, Head, Forensic Unit, EFCC Headquarters, Wuse II, Abuja, 6 November 2017.
Interview with A. Sambo, Head, Cybercrime Section, Operations Department, EFCC, Wuse II, Abuja, 6 November, 2017.
Interview with Mr. Mamman, Staff in the Forensic Unit, ICPC Headquarters, Garki, Abuja, 7 November, 2017.

Reports

CBN Financial Markets Departments Annual Activity Report (2015)
Central Bank of Nigeria, Fraud Landscape in Nigeria, 2nd edn (2014)
Central Bank of Nigeria 2015 Annual Report
Central Bank of Nigeria, "The Nigerian Payments System" (2011) Series No. 6, Understanding Monetary Policy Series.