Proliferation of Internet Financial Frauds in the Face of the Nigerian Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024: Necessity for Review

Prof. (Dr.) Dennis U. Odigie* *.

Dr OkpakoOmudhowo*.

Abstract

In recent years, science and technology have left both positive and negative indelible marks on the banking sector of the Nigerian economy. On the positive side is the enlarged horizon of the banking sector by the rendition of many banking services at incredible speeds and convenience through the use of computer and internet services. This development was taken to greater heights in the banking sector when the cashless Nigeria project which aims at encouraging electronic based transactions and reduction of the physical cash in circulation in the Nigerian economy was implemented. The cashless policy received a boost in 2020 following the outbreak of the corona virus pandemic tagged, "COVID 19" which forced persons, organisations and the government to embrace the electronic modes of business transaction throughout the lockdown period and beyond. On the negative side, fraudsters were attracted to the "large market" created by the exponential increase in the number of bank customers and the volume of bank transactions. The inherent anonymity and convenience of the net permitting users operation from comfort zones have caused the manipulation of electronic transactions to the detriment of bank customers. Hacking of bank accounts and making of unauthorised withdrawals have resulted to weeping and wailing of victims who are inconsolable because law enforcement agents appear lost as regards taming the menace. This article sets out to examine the effect of the implementation of the cashless Nigeria project on electronic frauds amidst the difficulties in the investigation of cybercrimes even in the face of the Nigerian Cybercrime Act as amended.

Keywords: Banker; Cashless; Customer; Cybercrime; Electronic Fraud; Service Providers.

*Professor of Law and Coordinator of Postgraduate Programmes, Faculty of Law, University of Benin, Benin City, Edo State. PhD, Mc.Arb, Chartered Arbitrator, Notary Public.

*PhD (Law), LLM, Ekpoma; LL.B (Hons.), Ibadan; BL, Lagos; M.Sc. (Econs), B.Sc. (Hons.) Benin. Lecturer, Faculty of Law, Benson Idahosa University, Benin City, Edo State. GSM: 08163040404; E-mail: ogomedede@gmail.com and ookpako@biu.edu.ng

1. INTRODUCTION

Cybercrimes refer to all crimes that came to be as a result of computer technology. They are crimes that are committed in the cyberspace through the use of the computer system[1] and internet service. It is to be noted that many societies including Nigeria had prohibited many conducts before the advent of the computer and internet. When such crimes are committed without the use of the computer and internet service, they are known as "crimes" simpliciter and can only be distinguished by the names given to them by law. However, when the commission of the crime is computer and internet dependent, such crimes are referred to as "cybercrimes". The crimes that are committed through the computer and internet are but not limited to computer related forgery, fraud, stealing, cheating, obtaining money by false pretence, blackmail / defamation through the social media or computers, cyber stalking, cyber-squatting and child pornography.

The use of computer has grown very fast and made almost routine in our societies such that it has become indispensible in our world. Its usage is convenient and brings speedy results in split seconds. These qualities are often manipulated by criminally minded persons and we are prone to some risks which we must learn to manage since it is not feasible for this world to be without computer and internet services anymore.

One of the areas where science and technology through the use of computer and internet service have created and left indelible marks in the Nigerian economy is the banking sector. A few decades ago, banking business was transacted manually in an analogue system. Under it, a customer is expected to approach a bank physically for the purpose of opening a bank account and he is expected to be there physically when making cash withdrawals for himself. In that system, a customer can only access his funds in the bank where he owns an account and also in the very branch of the bank where he opened the account. Credence is laid to this position by Lord Atkin in *Joachimson v. Swiss Bank Corporation*[2] when he highlighted the obligation in a banker – customer relationship as follows:

> The terms of the contract involve obligation on both sides. They appear upon consideration to include the following provisions: the bank undertakes to receive money and to collect bills for his customer's account. The proceeds so received are not to be held in trust for the customer, but the bank borrows the proceeds and undertakes to repay them. *The promise to repay is to repay at the branch of the bank where the account is kept and during banking hours*.[3] It includes a promise to repay any part of the amount due against the written order of the customer.

[1] Section 58 of the Cybercrime (Prohibition, Prevention, etc) (Amendment) Act, 2024 inter alia defines computer system as, "any device or group of interconnected or related devices, one or more of which, pursuant to a program performs automated or interactive processing of data. It covers any type of device with data processing capability including but not limited to computers and mobile phones". Thus, a computer includes smart phones, laptops and desktop.

[2](1921) 3 K.B. 110.

[3] Italics mine for emphasis.

Thus, where a customer opened an account in First Bank Plc., market road, Sapele, he can only make withdrawal of his money from First Bank and in that particular branch of First Bank. In other words, it was not possible for that customer to make withdrawal of his money from First Bank Plc., in Warri. If withdrawal of money was not possible for a customer in a different branch of the same bank, then, it is needless we say that a customer cannot access his money in one bank when he has his money in another bank, for example, a customer of Union Bank Plc., cannot make withdrawal of his money from Access Back Plc or Zenith Bank Plc in Nigeria.

Under the above scenario, the volume of banking was not only very low but people were also encouraged and compelled by difficulties and bottlenecks in the banking system to keep their money at home or in their persons. This was one of the reasons why the crime of armed robber was rampant in many homes and victims of such crimes were parting with their hard earned cash that was kept at home. The volume and number of frauds in the banking system especially as they relate to money belonging to individual customers were respectively low and small.

2. DIGITAL BANKING IN NIGERIA

Today, the slow and burdensome system of operation in the banking industry described above is gone for good. The transition from analogue to digital system has occurred through science and technology that have revolutionised the communication and banking sectors. The results are: (i) bank accounts can be opened electronically without the physical presence of a customer in the bank; (ii) withdrawal of funds can be made through electronic transfers anytime, anywhere and any day without the physical presence of a customer in any bank; (iii) withdrawal of funds by customers from any bank through the automated teller machine[4] (ATM) provided they have funds in bank accounts to their credit.

Under the digital regime, all transactions take place at an incredible speed and convenience to the advantage of the customers in genuine transactions whereas they are to their detriment, agony and pain where the transactions are fraudulent, illegal and unauthorised. It is this revolution in the banking sector that paved way for the pursuit of the cashless economy by which physical possession of cash is discouraged while electronic transactions through debit cards, electronic transfer of funds etc are encouraged. The above has engendered large scale banking and a reduction in the cash in the informal sector. Ironically, these technological breakthroughs are being used by fraudsters to the disadvantage of many bank customers through the unauthorised withdrawal of their money amidst the difficulties in securing credible electronic evidence.

The number of the victims of electronic fraud especially involving the low income group is on the increase on daily basis and their situation appears hopeless. This is because when their monies are fraudulently removed from their accounts and a report is made to

[4] This is an electronic banking outlet that allows customers to complete basic transactions without the aid of a branch representative or teller. Anyone with a credit or debit card can access cash at most ATMs. Visit: www.investopedia.com>Personal Finance>Banking. Accessed on 24/12/2021 at 0030 hours.

the police, the police are not able to do much immediately because the identity of the fraudster(s) cannot be ascertained without relevant information from the bank where such account is domicile. On their part, the banks can neither release the information nor do a reversal of such transactions without the order of court whereas there are serious bottlenecks in the process of securing court orders to freeze or post a no debit status on an account while time is of essence in internet transactions.

3. CYBER AND NON-CYBER CRIMES IN NIGERIA

In view of the fact that this article essentially centres on “cybercrimes” and there is disparity in the way juvenile offenders are treated in contradistinction with adult offenders, we shall briefly examine how crimes are classified in Nigeria. It is however important to remark here that any attempt at cataloging injurious human conducts that have been regulated for the purpose of preserving law and order in the society will hit a brick wall.[5]

In Nigeria, some classifications are based on the seriousness of the crime or punishment hence we have classifications like felony, misdemeanour, and simple offences;[6] capital and non-capital offences;[7] while some others are based on whether the crimes can be compounded of not hence we have compoundable and non-compoundable offences.[8] Again, while some classifications are from the perspective of the place of trial such as summary and non-summary trials, some others are based on the process or method of trial hence we have indictable and non-indictable offences.[9] Similarly, crimes can be classified from the angle of the degree of force used hence we have violent and non-violent crimes just as they can be classified based on whether or not there is an identifiable victim of the crime hence we have “victimless crimes”.

Furthermore, crimes can be classified based on the primary victim of the injury hence we have offences against persons and offences against property,[10] just as they can be classified based on whether the crime was committed through the cyberspace or not hence we have “cybercrimes and non-cybercrimes”. It must be remarked that some other classifications exist in some statutes.

[5] This is because the number is endless and the conduct or part of the conduct that constitutes one crime may in conjunction with other conducts constitute another kind of crime. The multiple nature of crime typology and the dual nature of the Nigerian legal system account for the non-uniform classification of crimes in Nigeria. While some classifications are just for administrative purposes, others are based on the pronouncement of the law.

[6] Criminal Code, Cap. C38, LFN, 2004 in section 3. Also, see section 2 of the CPA, Cap. “C41”, LFN, 2004.

[7] *Ibid*., in section 53(1).

[8] *Ibid*., in section 127; and section 339(9) of the CPC, Cap. “C42”, LFN, 2004.

[9] Criminal Procedure Act, Cap. “C41”, Laws of the Federation of Nigeria, 2004. See section 2 thereof.

[10] See the annual report of the Nigeria Police Force, 2012 in pages 164-167 and year 2013 in pages 220-224.

4. THE CASHLESS NIGERIA PROJECT

The cashless Nigeria project is a policy introduced by the Central Bank of Nigeria whereby a limit was set for the daily amount of cash transactions (deposit and withdrawal) that can be made by individuals and corporate bodies without "handling charges" while cash transactions above that limit are to be subjected to "handling charges". By this policy, daily cash deposits or withdrawals in excess of N150, 000.00 for individuals and N1, 000,000.00 for corporate bodies attract "handling charges". The policy was aimed at encouraging electronic based transactions and the reduction of the amount of physical cash circulating in the Nigerian economy. Through the cashless policy, more people were encouraged and in some ways "forced" to keep their money in the bank and at the same time resorting to electronic means of transacting financial businesses. The policy has succeeded in this regard because no doubt, more persons in Nigeria have opened bank accounts and have embraced electronic means of paying and receiving money for their daily business transactions since January 1st, 2012 when it was first introduced in Lagos and June 1st, 2012 when it was rolled out to other states across the country.[11]

Besides the above, given the fact that there is a positive correlation between economic growth and development on the one hand and an efficient and modern payment system on the other hand, the cashless policy was deployed and intended to develop and modernise the payment system in Nigeria for the purpose of actualising the then "vision 2020" of Nigeria being among the top 20 economies in the world. Other aims of the cashless policy include:[12] (i) reduction of the cost of banking services (including cost of credit) and derivation of financial inclusion by providing more efficient transaction options and greater reach; (ii) improvement in the effectiveness of monetary policy in the management of inflation thus constituting a driving force on economic growth and development; (iii) curbing high cost of cash maintenance in the economy; (iv) checking the high risk of using cash since robberies, stealing and other cash related crimes will be discouraged; (v) preventing financial losses in case of fire and flooding incidents; (vi) encouraging more money to be in the formal sector thus enhancing the effectiveness of monetary policy in managing inflation and by extension economic growth and development; (vii) discouraging inefficiency, corruption, leakages and money laundry amongst other cash related activities.

4.1 Natural Boost to the Cashless Policy

As the saying goes, "man proposes but God disposes", the major reason why the Central Bank of Nigeria introduced the cashless policy was for the citizens to embrace more of electronic transactions than physical cash transactions. The introduction of the policy thus paved ways for the financial institution to introduce many advanced electronic payment options such as the mobile banking and internet banking. About seven years after the introduction of the cashless policy, the world was struck by the

[11]The cashless Nigeria project – Central Bank of Nigeria wwwcbngovng>cashless.Accessed on 15/12/2021 at 2.45 am.

[12]*Ibid.*

corona virus pandemic in 2019 (COVID 19) that compelled many countries including Nigeria to go on lockdown thereby forcing every person to be at home throughout the period(s) of the lockdown. Under this situation, business organisations, citizens and the government were compelled to be dependent on technology and to do their businesses and social connections online from their homes. This restriction on mobility unpremeditatedly acted as a serious boost to the cashless policy because almost everybody embraced the electronic system of transactions amidst the surge in financial frauds.

4.2 Benefits of the Cashless Policy

No doubt, the cashless policy expanded the horizon of the banking sector through increase in the number of banking outlets, customers and volumes of transactions. This cannot be contended because evidence of banking activities especially through the point of sale (PoS) is seen even in remote villages where there are signals for internet service[13] thus bringing banking closer to the people. Besides, the policy has compelled many people (including the young and the old, literate and illiterate etc) who were not interested in having bank accounts to have a rethink and embraced the transaction of one form of business or the other with the banks especially that of receiving or sending of money to loved ones both in the villages and cities. The policy has brought a great deal of transformation in the business and social lives of Nigerians with better service delivery, enhanced turn overs and robust communication and information sharing.

All stakeholders have derived a variety of benefits from the cashless policy which is based on the electronic payment system. In specific terms, while the individual customers enjoy increased convenience and proximity to banking services, more service options, reduced risks of cash related crimes, cheaper access to banking services especially the “out of branch” services, and access to credit; the corporate bodies enjoy faster access to capital, reduced revenue leakage and cash handling costs. Similarly, while the government enjoys increased tax collection, greater financial inclusion and increased economic growth and development, the banks make more money from charges for services to their numerous customers and on cash deposits and withdrawals that are above the limit set by the Central Bank of Nigeria. They also enjoy less human physical contact and traffic on their facilities especially their premises and personnel with the attendant health implications during the era of the corona virus pandemic.

5. PROBLEMS FROM THE ENHANCED ELECTRONIC MEANS OF TRANSACTIONS

One of the outcomes of the implementation of the cashless policy is the exponential increase in the number of internet users. This has left us with the daunting problems of fraud and hacking of accounts of internet users by fraudsters which have created untold hardship for individuals, organisations and society. Various methods are being used by

[13] The internet service in most interior villages is weak thus making financial and other electronic transactions to be slow.

the fraudsters in exploiting the cyberspace. Crimes are committed through the web channels as well as the mobile apps and the ATM. We shall consider some of the methods in use by fraudsters in the succeeding subsection but suffice to say that the Nigerian Inter-Bank Settlement System Plc has identified social engineering as the fraud technique that is mostly in use and which accounted for 56% of all financial frauds in 2020. Other techniques includes the lack of two-factor authentication (2FA), card / phone theft, compromise of pin, fake assistance, robbery and missing / loss cards.[14]

5.1 Modus Operandi of Fraudsters in Electronic Transactions

Cybercrimes are committed through attacks on the information of a potential cybercrime victim using the cyberspace. The followings are some of the methods being adopted by fraudsters in committing cybercrimes:

i. Friendly fraud through the use of the victim's PIN:[15] a fraudster who may be a close friend, relation or colleague (social engineering) may get to know his victim's PIN and without authorisation, gets hold of the victim's phone and withdraws money from the victim's account.

ii. Fraud through the use of USSD[16] codes: a fraudster (as in above) may get hold of the victim's phone and by using different USSD codes without authorisation, transfers the victim's money to a different account or pay bills and or buy air time.

iii. Fraud through the use of lost / stolen ATM cards: when an ATM card is in the hands of fraudster(s), spirited "trial by error" is made by him (them) and in the process; the fraudster(s) may stumble on the victim's PIN. The fraudster does this by approaching the social media where a load of information is available about the victim which is downloaded and patiently analysed with a view of getting his PIN.

iv. Fraud by the use of account number and transaction alert number: the fraudsters get hold of the victim's account number, the phone number for the receipt of transaction alert and the guarantee that the account had not been in use for at least one month which can be gotten from the service providers and bankers and quickly, the money is gone.

v. Fraud through the use of hacked e-mail: victim's e-mail is hacked and his financial transaction intercepted. His communication is then disrupted and

[14] Mobile frauds up by 330% in Nigeria, says NIBSS – Benjamin Dada www.benjamindada.com>nibss-financial-fraud-report. Accessed on 10/01/2022 at 5 pm.

[15] This is a numerical code used in the process of authenticating a user who is accessing a system and it is used in many electronic financial transactions. PIN stands for Personal Identification number. Visit: en.wikipedia.org>wiki>Personal identification number. Accessed on 23/12/2012 at 2300 hours.

[16] This is a communication protocol used by GSM cellular telephone to communicate with the mobile network operator's computer and it stands for Unstructured Supplementary Service Data (USSD). It is sometimes referred to as "quick code" or "feature code". Visit: en.wikipedia.org>wiki> Unstructured-Supplementary-Service-Data. Accessed on 24/12/2021 at 0027 hours.

concluded by a third party leading to the unlawful transfer of funds from the victim's account.

vi. Fraud through SIM[17] swap: victim's phone is lost and the fraudster lays hand on the sim-card before a welcome pack is done. Through active connivance with the service providers, the fraudster effects a sim swap which automatically transfers the SIM and all embedded data to the fraudster who then transfers and withdraws the victim's money.

6. OVERVIEW OF THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC) (AMENDMENT) ACT, 2024

The Nigerian Cybercrime (Prohibition, Prevention etc) (Amendment) Act, 2024 which was signed into law on the 28th of February, 2024 and which amended Act, No. 17 of 2015 provides a comprehensive legal, regulatory and institutional framework for prohibiting, preventing, detecting, prosecuting and punishing cybercrime offenders in Nigeria. We shall briefly examine this subsection of this article under the following headings, existing legal framework for curbing cybercrimes in Nigeria, jurisdiction, law enforcement agencies and other critical stakeholders.

6.1 Existing Legal Framework for Curbing Cybercrimes in Nigeria

The need to curb cybercrimes in Nigeria received legislative nod in May, 2015 when the Cybercrimes (Prohibition, Prevention, etc) Act, 2015 was specifically enacted for cybercrimes. It was amended[18] in February, 2024. The Act provides a comprehensive regulatory and institutional framework for the prohibition, detection and prosecution of cybercrimes in Nigeria. It vested the relevant law enforcement agencies with prosecution power subject only to the power of the Attorney General of the Federation.[19] The relevant law enforcement agencies[20] shall however, obtain the approval[21] of the Attorney General of the Federation before prosecuting any case under sections 19 and 21 of the Act. The office of the National Security Adviser shall be the coordinating body[22] for all security and law enforcement agencies under the Act. The coordinating body shall establish a National Computer Emergency Response Team who is to manage cyber incidences,[23] the sectoral Computer Emergency Response Team, the

[17] A SIM card, also known as Subscriber Identity Module or Subscriber Identification Module is a microchip in a mobile phone that connects it to a cellular network or a particular phone network. Visit: www.collinsdictionary.com>dictionary>english>sim-card. Accessed on 3/2/2022 at 12.50 am.

[18] Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act, 2024.

[19] *Ibid*. See section 47.

[20] Section 58 of the Cybercrimes (Prohibition, Prevention etc) Act, 2024 defines law enforcement agencies to include "any agency for the time being responsible for implementation and enforcement of the provisions of this Act". Although the Act did not identify the relevant law enforcement agencies in Nigeria, they include: the Nigeria Police Force, the Economic and Financial Crimes Commission and the Independent Corrupt Practices Commission.

[21] Cybercrimes (Prohibition, Prevention etc), Act, as amended in section 47.

[22] *Ibid*. See section 41(1).

[23] *Ibid*.See paragraph c.

sectoral Security Operation Centres[24] that shall feed into the national CERT., a National Computer Forensic Laboratory[25] and appropriate platforms for public private partnership.[26] The Act made it mandatory for cybercrimes to be reported as follow:

> Any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team (CERT) Coordination Centre through their respective sectorial CERTs or sectorial Security Operation Centres (SOC) of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network so that the National CERT can take the necessary measures to tackle the issues.[27]

The coordinating body shall also coordinate Nigeria's involvement in international cyber security to ensure the integration of Nigeria into global framework on cyber security,[28] and do such other acts that can enhance effective performance of the relevant security and law enforcement agencies.The Act also empowers a law enforcement officer to apply *ex-parte* to a judge in chamber for issuance of a warrant for obtaining electronic evidence in related crime investigation. Such authority empowers any law enforcement officer to enter and search any premises and person, seize and detain anything which contains evidence of the commission of a crime under the Act.[29]

6.2 Law Enforcement Agencies

Although the Cybercrimes (Prohibition, Prevention, etc) Act, as amended did not specifically identify the relevant law enforcement agencies, the Nigeria Police Force is a major law enforcement agency in Nigeria and by statute[30] has the primary responsibility of prevention, detection[31]and prosecution[32] of criminal cases in Nigeria irrespective of their type and classifications. It is instructive to note that the law empowers the police to enforce all laws and consequently all criminal matters whether or not a specialised agency is established for them. The Act provides:

> The Police Force shall – (a) prevent and detect crime, and protect the right and freedom of every person in Nigeria as provided in the Constitution, the African Charter on human and peoples right and any other law; (b) maintain public safety, law and order; (c) protect the lives and property of all persons in Nigeria; (d) enforce all laws

[24]*Ibid*. See paragraph d.
[25]*Ibid*. See paragraph f.
[26]*Ibid*. See paragraph h.
[27]Cybercrimes (Prohibition, Prevention etc), Act, 2024. See section 21.
[28]*Ibid*. See section 41(1) (i).
[29]*Ibid*. See section 45.
[30]The Nigeria Police Act, 2020.
[31]*Ibid*. See section 4(a).
[32]*Ibid*. See section 66.

and regulations without any prejudice to the enabling Act of other security agencies.[33]

We shall therefore make reference to the Nigeria Police Force as a lead law enforcement agency to represent all other relevant law enforcement agencies in this article.

6.3 Jurisdiction

The Act vested jurisdiction on the Federal High Court. Consequently, any Division of the Federal High Court in Nigeria has jurisdiction of offences under this Act the venue of crime in Nigeria notwithstanding. The Federal High Court also has jurisdiction where the offence is committed in a ship or aircraft that is registered in Nigeria and where the offence is committed outside Nigeria if the victim of the offence is a citizen or resident in Nigeria or the alleged offender is resident in Nigeria and not extradited to any other country for prosecution.[34] Also, cases brought to court under this Act shall be given accelerated hearing[35] frivolous request for adjournment shall not be granted.[36]

6.4 Other Critical Stakeholders

The other critical stakeholders we shall mention here are financial institution and the service providers. Under the Act, while financial institution include any individual, body, association or group of person whether corporate or unincorporated that carries on the business of investment and securities etc; service provider means any public or private entity that provides to users of its services, the ability to communicate by means of a computer system, electronic communication devices, mobile network; and any other entity that processes or stores computer data on behalf of such communication service.[37] Financial institutions have not only the duty of verifying the identity of their customer before the issuance of ATM cards, credit cards, debit cards and other related electronic devices but also the duty of applying the principle of “know your customers” in their documentation preceding execution of customers’ electronic transfer, payment and debit issuance order.[38] Similarly, it is the duty of the service providers to keep and protect specific traffic data and subscribers information in accordance with the provision of the Nigeria Data Protection Act for a period of two years and shall not only preserve, hold or retain any traffic data, non-content, content and subscriber information but also release any information required to be kept by law to an authorised officer[39] for his agency.

[33] *Ibid.*See section 4(d). See also the case of *Inspector General of Police v. Daniel Andrew* (2014) All FWLR 729 at p. 1202.
[34] Cybercrimes (Prohibition, Prevention etc), Act, 2024. See section 50.
[35] *Ibid*. See section 50(3).
[36] *Ibid*. See section 50(4).
[37] *Ibid.* See section 58.
[38] *Ibid*. See section 37. In facilitating the known your customer policy, the banks are required to use the National Identification Number and other valid documents.
[39] *Ibid*. See section 38.

7. UPSURGE IN ELECTRONIC FINANCIAL FRAUDS

The recorded success from the implementation of the cashless policy is not without its fair share of problems. This is so because as the policy received a boost through much patronage so also did the nation's financial fraud rate received a "super boost" to the point of threatening the benefits derived from the policy in the face of the Nigerian Cybercrimes Act. It is germane to remark that although financial fraud has been recurring in Nigeria, it was on a "whole new level" in year 2020 accounting for a 186% increase against 2018 and 2019 where its growth rate was low and the mobile led fraud channel saw a 330% Year-on-Year growth in 2020 as revealed by the Nigerian Inter-Bank Settlement System Plc.[40]

Similarly, a former National Security Adviser under the late former President Muhammadu Buhari's administration,[41] Gen. Babagana Monguno (retd), while revealing that Nigeria, South Africa and Kenya recorded over two million phishing (cyber) attacks in the first half of 2021 going by the survey conducted by a Bucharest based (Kaspersky Laboratory) a Romania also stated that 86% of Nigerian companies fell prey to cyber-attacks in 2020 being only second to India while South Africa with 64% settled for the third position.[42]

While many cybercrimes are not reported in Nigeria, the victims of electronic financial fraud are often frustrated and helpless. This is because while the police are handicapped because the information that can reveal the identity and consequent arrest of the suspect is not domicile with them; the banks and service providers are handicapped in giving out information concerning their customers without their consent and or valid court processes / order because of their duty of care and protection to their customers.

Again, while meeting the standard set for obtaining court orders is not easy especially for the illiterates and low income group; it may happen that there is the connivance of some of the banks' staff with the fraudster such that the relevant information is revealed to the suspect by his internal collaborator(s) to enable him (them) evade arrest. The result is that many victims will only cry and abandon their cases after much frustration. We shall examine these problems in details in the succeeding subsections of this article but needless to say that many businesses have collapsed and many victims of cybercrimes have died painfully as a result of the activities of fraudsters.

[40]Mobile frauds up by 330% in Nigeria, says NIBSS – Benjamin Dada www.benjamindada.com>nibss-financial-fraud-report. Accessed on 10/01/2022 at 5 pm.

[41] By section 41 of the Cybercrimes (Prohibition, Prevention etc) Act, 2024, the office of the National Security Adviser shall be the coordinating body for all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria.

[42] This was disclosed in a sensitisation workshop for the implementation of the "National Cyber Security Policy and Strategy 2021" for the private sector and professional bodies on Tuesday 16th November, 2021 in Lagos.

7.1 Factors Responsible for the Increase in Electronic Financial Fraud

There are many factors responsible for the fast growth in electronic financial fraud in Nigeria. We shall consider the factors that have encouraged the proliferation of electronic financial fraud in Nigeria under two subheads namely, general and specific causes.

7.2 General Factors: The general causes of the proliferation of cybercrimes include:
7.2.1 Anonymity: Exploration on the cyberspace through the internet is convenient, fast and anonymous. Users can operation from the comfort of their bedrooms anywhere provided there is network and internet service. A user can make a large volume of transactions in split seconds with incredible results and yet his identity may not be immediately known. In other words, cyber offenders are largely anonymous at least on the surface or at the point of a victim becoming aware of the commission of a cybercrime. For example, a fraudster in Ugep, Cross River State who has the correct and relevant information that are needed for making a bank transaction can conveniently make withdrawals / transfers from somebody's bank account that is domicile in Wudil, Kano State, the distance notwithstanding. All the data concerning the identity of cyber operators including cyber fraudsters may not be known to the owner of a bank account and even the bank. This is because some of the information is domicile with the internet owners and telecommunication service providers.

It must be noted that none of the bodies having these information is statutorily saddle with the primary responsibility of crime prevention and detection. Thus, when a report of cybercrime is made to the relevant law enforcement agencies saddled with such responsibilities, getting to the root of the crime requires the identity of the erstwhile unknown offender being laid bare. This of course necessitates a synergy between all the bodies concerned for the achievement of the desired result while time is of essence in internet transactions.

7.2.2 Illiteracy: Arising from the fact that the cashless policy is based on the electronic system of payment which is computer and internet service based, there exists a problem for persons who cannot operate a computer especially the illiterates. This will of necessity compel them to employ the services of other persons for the purpose of assisting them to input their data into the computer system to enable them complete their transactions. These data in the hands of another person can be used to the detriment of the customer through unauthorised withdrawals and other fraudulent practices. Regrettably, about 90% of bank[43] customers belong to the low income group whose daily transactions are always below the N150,000.00 which is the ceiling for "free handling charge" as fixed by the Central Bank of Nigeria for individuals.

7.2.3 Poverty: It is no news that majority of the population of Nigeria is poor and given the monetary policy of the government as encapsulated in the cashless policy, the poor populace has been driven to embrace the electronic system of transactions. Where the

[43] See CBN Further Classifications on Cashless. Available: www.cbngovng>gud>cashlesslagos. Accessed on 15/12/2021 at 2.00 am.

poor become victims of electronic fraud and the wherewithal to pursue the case is lacking, they resign to fate.

7.2.4 Ignorance: Very often, when poor and uneducated persons are victims of electronic financial fraud, they may not know what to do and will rather bear the loss without complaining or reporting to any person.

7.2.5 Lack of Cyber Security: Cyber security is also known as information technology or computer security. It is the protection of computer systems and networks from theft, disruption and disclosure of information as well as damage to the systems' hardware, software and electronic data. Many users of the cyberspace have no cyber security in their systems. It is important to remark here that all bank customers are potential victims of fraudsters if they did not protect their information very well since the banking system operates through electronic means and the internet service.

7.2.6 Bottlenecks in the System: It is always very difficult for the victims of electronic financial fraud especially the poor to seek redress and recover their monies in good time given the bottlenecks in the system and the means of tracing / tracking of the suspect through the police, banks, communication and service providers as well as the court.

7.2.7 Non Reporting of Cyber Attacks: It must be remarked here that many crimes including cybercrimes are not reported in Nigeria. Some organisations and rich individuals fail to report their cases when they consider the impact such report may have on their goodwill and investment as well as the effect of such fraud on the organisation. Many other companies and individuals especially the poor or the low income class fail to report their cases in Nigeria for reasons ranging from not knowing what to do; cost of sponsoring investigation; frustration of the victims of crime in the investigation process; possibility of easy identification and arrest of cybercrimes suspects; possibility of recovering the defrauded property especially money; time taken to dispose off the case in court; and lack of automatic compensation for the victims of such crimes since there is no State funded compensation scheme in Nigeria.

7.3 Specific Causes: We shall examine the specific caused of the proliferation of cybercrimes under the following headings: investigation and prosecution of cybercrimes, clogs on the wheel of investigation of cybercrimes, conflict between bankers' duty of care to their customers and the need from speedy investigation of cybercrimes, the skewed nature of the Cybercrimes Act of Nigeria and judicial technicalities and the resultant delay in cybercrimes investigation.

7.3.1 Investigation and Prosecution of Cybercrimes:
Having considered some of the salient provisions of the Nigerian Cybercrimes Act, it is pertinent to observe generally that detection of crime starts with the awareness by the body saddled with the responsibility of crime detection of the commission of a crime. It is this awareness which may be through a verbal or written report that propels the investigation body into the taking of necessary steps. This may be the reason why the Cybercrimes Act made it mandatory for a victim of cybercrime to immediately inform the

National Computer Emergency Response Team for necessary action.[44] Being armed with such report, the investigating body attempts to confirm the veracity of the report which may involve intelligence gathering to know whether or not an offence has been committed. In the course of doing this and before the conclusion of the investigation, arrest is expected to be made to pave way for prosecution because criminal cases are not charged to court without a suspect or the person alleged to have committed the crime.

It is however unfortunate to observe that in recent times, when a victim of cybercrime especially of electronic money transfer reports to the police, he would be referred to his bank and his bank that has plenty of information about what has happened will in turn refer the victim back to the police and or the court. The result is that many victims of such crimes are frustrated and give up further pursuit of their cases especially when the amount of money involved in the fraud is small. As more of our people fall victims, the Nigeria Police and indeed all the other law enforcement agencies appear to be at a loss as to what should be done to end, or at least curtail this menace.

7.3.2 Clogs on the Wheel of Investigation of Cybercrimes

The reasons for the apparent inability of the police and other law enforcement agencies to tackle this menace headlong are not far-fetched. Apart from the anonymity of the fraudster occasioned by the fact that cybercrimes are based on attacks[45] on the information of an entity which may be an individual, organisation or even the government, the attacks are not coordinated physically rather, the coordination is by electronic devices through the internet. Other causes of the seeming inability of the police and other law enforcement agencies to crack the menace of cybercrimes are but not limited to the fact that the data that are necessary for the successful investigation of cybercrimes are domiciled with third parties as follows:

(a) **Telecom Service Providers**:[46] It is the telecom service providers that have the necessary information for the generation of (a) Call Data Record (CDR) for voice mails; (b) the Short Message Service (sms) for the content of messages; (c) records to determine the owner of IP address of mails; (d) identity to determine the user of some phone numbers and other connected numbers.

---

[44]Cybercrimes (Prohibition, Prevention etc), Act, 2024. See section 21.

[45] Cyber-attacks can be carried out in various ways including: (i) malware; (ii) phishing; (iii) denial-of-service (DOS); (iv) password attack or cracking; (v) SQL injection; (vi) man-in-the-middle variously known as monster-in-the-middle; machine-in–the-middle, monkey-in-the-middle, meddler-in-the-middle or person-in-the-middle; and (vii) emotet. Visit: 7 types of cyber security threat – Online Degree Programs onlinedegrees.und.edu>Blog. Accessed on 23/12/2021 at 12.45 am.

[46] Telecommunication Service Providers operating in Nigeria include: the Mobile Telecommunication Network (MTN) or the MTN Group Limited which is a South African Multinational Mobile Telecommunications Company, operating in many African and Asian countries with headquarters in Johannesburg; the Global Communications Limited (GLOBACOM) which is a Nigerian Multinational Telecommunications; and the BhartiAirtel Limited with headquarters in New Delhi, India.

(b) **Commercial Banks and Other Money Deposit Institutions:** It is the financial institutions that have information concerning the identities and addresses of their customers. They can also generate data on (a) the movement of cash between accounts within same bank and or (b) between accounts in different banks; (c) authentication of different e-channels-Mobile-Money-Apps, ATM, PoS[47] and USSD transfers.

(c) **Courts:** It is the courts that grant court orders to enable the police elicit necessary information from the relevant service providers and the banks.

Very unfortunately, none of the above organisations is responsible to the police or any security agency for that matter, and they seem to have no way of holding them accountable. It must be noted that because of the duty of the banker to conduct the account of his customer in a condition of secrecy, subject to some exceptions, the breach of which can be a subject of litigation, the banks rely on the order of court to act otherwise. Telecom service providers have followed suit by demanding for court orders before divulging information at their disposal thus, even when there is a situation that requires urgency, the banks and service providers rely on such technicalities and unwittingly give room for the escape of the suspected perpetrator of the cybercrime since time is of essence. It is to be noted that obtaining the necessary court orders to elicit information and cooperation of the service providers and banks is not easy at least to the common man or the low income earners due to the prevailing judicial standards.

7.3.3 Conflict between Bankers' Practices and Speedy Investigation of Cybercrimes

The banker – customer relationship is a contractual relationship that imposes rights and duties on both parties whose violation can be subject of litigation. Chief among the duties of the banker to its customer aside acceptance of deposits is the conduction of the account of the customer in secrecy subject to some exceptions[48] such as the order of court. It must be realised that bankers need and will always like to retain many customers so as to remain in business and since a customer would not want his account to be conducted in the open without their consent, the banks naturally key into this and deploy all tactics[49] aimed at refusing to divulge information concerning their

[47] Point of Sale (PoS) refers to the place where customers execute payments for goods or services. The PoS systems provide retailers or companies with sales and marketing data. Available: www.invetopedia.com>small business> how to start a business.

[48] The duty of secrecy of the banker to the customer is not absolute but qualified. The circumstances under which the banker may disclose information concerning the customer and his account are: (i) when disclosure is under the compulsion of law such as when a bank is served a summons to attend court and disclose the customer's affairs; (ii) disclose under duty to the public such as disclosure to prevent crime or protect the public and bank against crime or fraud; (iii) disclosure under customer's consent which may be express or implied; and (iv) disclosure under banker's interest such as when the customer is indebted to the bank and all effort to pay fails, the bank may put the matter in other "hand". See Afolabi, L., *Law and Practice of Banking*, (Heinenmann Educational Books (Nig.) Plc., 2005), pp. 39-45.

[49] This appears to have received judicial backing in the case of *GTB Plc v. Adedamola* (2019) 5 NLWLR (Pt. 1664) 30 at 43 when Abubakar JCA, admonished financial institutions as follows, "our financial

customers unless the courts give order to that effect. Since releasing certain information about their customers may conflict with the bankers' objectives and duties to their customers, the bankers take advantage of these technicalities and in the process unwittingly hamper the needed cooperation in good time whereas time is of great essence in internet transactions. It is unfortunate to remark here that some fraudsters transact their fraudulent businesses in their bank accounts with the knowledge and unethical connivance of some bank workers. The arrest of such fraudsters is always very difficult because as soon as issues bordering on investigation come up, the fraudsters are quickly alerted by their "insider collaborator(s)" to enable them take all precautions to evade arrest. This is essentially because the arrest of the fraudster may ultimately lead to the arrest of such bank staff and the consequent risks of losing his employment and eventual prosecution in the court of law. This inadvertently makes the banks to insist on "due process" and in the process of insisting on technicalities which are about small details in a law or set of rules especially those that seem to be unfair, time passes by without arrest of the suspect. These practices amount to a kind of tacit encouragement of cybercrimes by the bankers through delays in investigation and very often, the victims of such fraudulent transactions are thus frustrated and compelled to abandon their case.

7.3.4 The Skewed Nature of the Cybercrime Act of Nigeria

Let us try and proffer solution to this basic question: Is the Cybercrimes (Prohibition, Prevention, etc) Act, 2024 meant for all cybercrimes in Nigeria? Going by section 21 of the Act which mandated any person or institution who operates a computer system or network to immediately report the occurrence of a cyber-attack, it may seem obvious that the Act is for all cybercrimes. It is however germane to note that although cybercrimes include pornography, computer related forgery, phishing, defamation etc, it is unarguably true that cyber fraud through electronic money transfer is perhaps more common. This is so because the underlying purpose for most internet users is the intention of transacting one form of business or the other. Given the fact that ignorance and illiteracy are on the high side in Nigeria and computer education is low, many users of the cyberspace in every corner of Nigeria especially individual account holders of the lower class often fall victims of electronic fraud. This notwithstanding, the Act in sections 50 and 47 respectively conferred jurisdiction only on the Federal High Court and also made the prosecution of offences under sections 19 and 21 of the Act only possible with the approval of the Attorney General. It is important to remark here that these two section dealing with offences for which the approval of the Attorney General must be sought before prosecution essentially deal with where the financial institutions fail in their duties to customers to put in place adequate counter-fraud measures to safe guide their sensitive information and person or institution who fail to report cyber-attack incident(s). The following fundamental questions come to mind. How many private individuals in Nigeria will pursue their cases in the Federal High Court especially when the amount of money involved is small? Can it be convenient for a person whose only

institution must not be complacent, reticent and toothless in the face of brazen and reckless violence to the rights of their customers. Whenever there is a specific provision regulating the procedure of doing a particular act, that procedure must be followed."

N20,000 or N50,000 is fraudulently transferred from his account to follow the investigation process to the prosecution stage in the Federal High Court? How compatible is seeking and obtaining the approval of the Attorney General with speedy investigation and prosecution of violators of the Act? These are some of the mind budging questions why some persons are of the view that the Cybercrimes Act is skewed in favour of corporate bodies and wealthy individuals in Nigeria.

7.3.5 Judicial Standards and Delays in Cybercrimes Investigation

By judicial standard we mean the level or quality that is normal and acceptable in judicial processes. Since the judiciary is the hope of the common man, the judicial process must have a minimum standard below which its affairs must not be conducted for the purpose of guaranteeing fairness, consistency, efficiency and reliability. It is however observed that the judicial standard in place in Nigeria whereby court orders are needed in relation to eliciting information from bankers and telecom service providers in the course of investigation impedes speedy investigation in no small measure. This is against the backdrop that the courts have in recent times insisted on full scale legal processes / procedures before the issuance of order(s).[50] This is in consonance with the declaration of Abubakar, JCA, in the case of *GTB Plc v. Adedamola*[51] in the following words, "Whenever there is a specific provision regulating the procedure of doing a particular act, that procedure must be followed."

The implication of this is that investigators have the burden of initiating legal processes if they are legal practitioners or seek to employ the services of legal practitioners where they are non-lawyers and waiting for days or weeks if there are factors that can inhibit speedy attention in the courts such as weekends and public holidays to get a banker's order to be served on the bank / service providers who will also bid their own time for as long as they desire, even if the order is to be acted upon. This is worrisome in that unlike conventional crimes, electronic frauds require only split seconds or at best, minutes to be accomplished. So, even if the culprits were arrested owing to these unending delays, the money involved would have been frittered away thereby making the eventual arrest and or prosecution of the culprit virtually meaningless. Hardship is created in this regard in two ways as follows:

---

[50] By section 45(1) of the Cybercrimes Act of Nigeria, a law enforcement officer may apply to a judge *ex parte* for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation. It must be realised that judges are not in every nook and cranny of the society where cybercrimes can be committed and reported to the police. The "local police" may therefore not be able to handle such matter and so such cases may be transferred to the State Criminal Investigation Department in the State capital where there may be better facilities. Taking the case to a higher authority outside the locality of the victim imposes extra cost for instance, cost of transportation on the victim of crime. The consequence is that the victim who may not be having money will weigh the cost and the inconveniences he is likely to face and the benefits he is likely to derive at the end of investigation and prosecution of the case which may make him to consider the dropping of the case a worthwhile venture.

[51] *Supra.*

(a) Magistrate's Courts Lacked Power to Issue Order Freezing Bank Account: Following the declaration by the Federal High Court in Abuja that the Magistrate's Courts lacked the power to issue an order freezing bank accounts or placing a "post-no-debit" order on personal account, it follows that where there are information to be obtained from the banker in respect of a customer's account, necessary proceedings must commence in the High Court.[52] The question that comes to mind is, given the fact that instituting proceedings for the purpose of obtaining court order is not free, how many victims of fraudulent transactions will pursue the investigation of their cases? Certainly, most of the victims of the low income group will be frustrated to abandon their case.

(b) Court Orders Must be Obtained Through Court Processes: Where investigation is to be carried out touching the bank account of a customer, due process must be followed. In the case of *GTB Plc v. Adedamola*[53], Abubakar JCA, explained as follows:

> Where there is an allegation of commission of crime against a customer of a bank in relation to the funds in his account, the Economic and Financial Crimes Commission is empowered by law to set in motion the process of investigating any such funds perceived to be derived from proceeds of crime. In conducting the investigation, the Commission is required to observe due process and satisfy the requirements of the law. The Commission or its officers must go to court and obtain an *ex parte*[54] order before freezing the account; any failure to follow due process will render the action taken by the Commission a violation of the right of a customer.

In that case, the court went further to stress that the bank must be satisfied that there is the order of court before it can freeze a customer's account or place any form of restraint on any bank account because the Economic and Financial Crimes Commission (and indeed the other investigation bodies) has no power to give direct instructions to bank to freeze the account of a customer without a court order.

---

[52] In the suit marked FHC/ABJ/CS/1635/2019, Justice InyangEkwo made a declaration ordering banks to desist from acting on "bankers' order" obtained from magistrate's court and served on them, particularly by the police, to freeze or place a post no debit order on personal account. In his words, "a magistrate lacks the power to make bankers' order and / or post no debit on bank accounts pursuant to non-existent / repealed section 7 of the Banker Order, Act, 1847".

[53] *Supra*.

[54] An *ex parte* order is an order obtained through the filling of an *ex parte* motion. It is call *ex parte* because upon the motion being filled, the applicant is not obliged to serve same on the other party. It is enough if the application is brought to the attention of the court as it is permitted by law to consider it and grant same (if necessary) without hearing the person to be affected. The purpose of such interim order is basically to preserve the subject matter (in this case the money in the suspicious account) from being disposed of, usually, such order are only to last for a short period (pending the hearing and determination of a motion on notice). Thus, in many cases, the *ex parte* motion is to be accompanied by a motion on notice which would be served on the person affected, thereby giving him opportunity to be heard. The motion on notice would then be seeking for an order that will last till the case is ultimately heard and decided. The court will rule on the application, one way or the other, after hearing both sides.

8. FRUSTRATION OF VICTIMS OCCASIONING INCREASE IN CYBERCRIMES

It must be remarked that the nearest places for the report of criminal cases are the police stations which are relatively visible in every Local Government Area in Nigeria. It should be noted also that although the police can investigate and prosecute all cases in any court in Nigeria, most of the prosecution duties of the police are carried out in the lower courts. At the moment and going by the provisions[55] of the Police Act, 2020, the Administration of Criminal Justice Act, 2015 and the Administration of Criminal Justice Law for States that have domesticated the Act whereby only police lawyer can prosecute criminal cases, it means many police officers may not be able to prosecute cases in the courts especially the High Courts. The fundamental question that comes to mind is, how many qualified lawyers do we have in the Nigeria Police Force at the moment that can file court processes and prosecute criminal cases in the 774 Local Government Areas of Nigeria? It must be noted here that most of the lawyers in the Nigeria Police Force are in the legal section of the Force and States Criminal Investigation Department which are in the capital cities.

Thus, where cases that require the touch of a lawyer are reported to the Police, the implication is that such cases are transferred to the State Criminal Investigation Department in the capital city of that State and the next problem that confronts the victims of such crimes is the cost and time of investigation. The consequence of this is that the victims of such crimes will consider the amount of money that would be involved, the man hour (time) that would be wasted, and the risks and energy that would be dissipated on the one hand and the possibility of recovering the money involve and the benefit they would derive from the entire process on the other hand. The very likely result after considering all the issues above is that the victims of such crimes will not report such cases and where they report such cases, they will abandon them as a result of frustrations in the entire process.

9. CONCLUSION

It is crystal clear from the foregoing that the commission of cybercrimes in Nigeria is on the increase even in the face of the Cybercrimes (Prohibition, Prevention etc) Act, 2024. This is a function of some factors which have been classified as general and specific in this study. Many business organisations have collapsed and many individual victims are in pains and others have died whereas taming this menace appears not to be in sight. The agony faced by victims of cybercrimes calls for urgent and more radical steps being taken by all stakeholders to turn the situation around. This is with a view of reducing the commission of not only cybercrimes to the barest minimum but also non cybercrimes since the commission of every crime today is either cyber facilitated, dependence or cyber-enabled.

---

[55] Section 66(1) of the Police Act, 2020 provides as follows, “subject to the provisions of sections 174 and 211 of the Constitution of the Federal Republic of Nigeria, 1999 and section 106 of the Administration of Criminal Justice Act which relate to the powers of the Attorney General of the Federation and of a State to institute, takeover and continue or discontinue criminal proceedings against any person before any court of law in Nigeria, a police officer who is a legal practitioner, may prosecute in person before any court whether or not the information or complaint is laid in his name”.

10. RECOMMENDATIONS

Arising from the above, the following recommendations are hereby offered: (i) lawmakers should revisit the Nigerian Cybercrimes Act and grant jurisdiction to the magistrate courts all over the country when electronic financial fraud involves amount not exceeding N500,000.00 while the Federal High Court can be left with frauds that exceed that amount. (ii) banks should be mandated to develop mobile money applications that would require second-level-authentication (2-face-authentication) using the biometric, since every account holder has his or her biometrics with the banks. For corporate accounts, voice call confirmation for every transaction should be required. (iii) SIM swap should require the physical presence of the owner of the SIM in addition to his or her biometric confirmation as well as a valid identity card. (iv) all request for information to either the banks or mobile service providers should be responded to within a stipulated time of not more than 48 hours after the making of such request, otherwise section 46 of the Cybercrimes (Prohibition, Prevention etc) Act, 2024 should be invoked. (v) requests signed by an Assistant Commissioner of Police in the case of the Force, Zonal and State Criminal Investigation Department; and the Divisional Police Officer in the case of Divisions should be honoured without delay. (vi) the Chief Justice of Nigeria and the Chief Judge of each state to designate a Judge / Magistrate and Police Officers (as in (v) above) who will mutually agree on ways to ease the process of obtaining orders from the courts since many police officers are non-lawyers.