Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2023 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Prosecution of Electronic Banking Offences and Data Insecurity Cases in Nigeria: The Law, The Gaps & The Prospects

Dr. Ufuoma Veronica Awhefeada[a] Ogechi Bernice Ohwomeregwa[b] Ulisan Mogbitse Ogisi[c]

[a]Associate Professor of Law, Delta State University, Oleh Campus, Abraka, Nigeria [b]Doctoral Candidate, Faculty of Law, Delta State University, Oleh Campus, Nigeria [c]Faculty of Law, Delta State University, Oleh Campus, Nigeria

Received 26 March 2023; *Accepted* 12 April 2023; *Published* 18 April 2023

The myriad of problems confronting law enforcement agents in prosecuting cases arising from electronic banking operations and associated data insecurity in Nigeria constitutes a huge setback to these agencies and the nation at large. These range from issues of jurisdiction and choice of court, the anonymity of electronic banking and general ICT offenders, extradition rules, and the problem with the admissibility of electronically generated evidence among others. This paper identifies and examines the extent to which these problems have affected the output of law enforcement agents in Nigeria when prosecuting cases of data insecurity in electronic banking operations and practices in Nigeria. To accomplish this task, the paper adopts the doctrinal method of research, by examining primary and secondary sources of law in their original form. This paper finds that the job of determining jurisdiction and choice of courts in cyber offenses is problematic owing to the borderless nature of the cyberspace and absence of a generally accepted theory on the extraterritorial application of cyber laws. Furthermore, despite the provisions of the Evidence Act of 2011, the difficulties associated with extradition rules as well as admitting electronically generated evidence in Nigeria have not abated. This piece concludes by canvassing the position that there is a need to strengthen the applicable legal framework on Extradition and Mutual Legal Assistance in Nigeria to make for ease of extraditing fugitives from other countries to Nigeria as well as to enable Law Enforcement Agents in Nigeria to request and receive assistance from their foreign counterparts in prosecuting persons accused of electronic banking offenses in Nigeria despite their country of origin or residence.

Keywords: *prosecution, electronic banking offenses, cybercrime, cyberspace, data insecurity*.

INTRODUCTION

Prosecution of offences arising from electronic banking transactions is not without some challenges owing to the nature of electronic banking business and transactions that take place in cyberspace. In Nigeria today, the major agencies charged with the role of prosecuting criminal offences generally are the legal officers attached to the office of the Attorney-General and the Minister of Justice, the office of the Director of Public Prosecutions, the Economic and Financial Crimes Commission, and the Nigerian Police among others. Electronic banking and cyber offences especially those arising from data insecurity and breach fall within the ambit of criminal offences which the agencies listed above can prosecute. To this end, this research work focuses on the role of these agencies especially the Economic and Financial Crimes Commission and the Nigerian Police in tackling data insecurity issues associated with electronic banking operations.

THE ROLE OF EFCC IN THE PROSECUTION OF INTERNET CRIMES IN NIGERIA

The Economic and Financial Crimes Commission (EFCC) was established through the EFCC Act 2004 with the sole aim of fighting economic and financial crimes. The EFCC has the mandate to prevent, investigate and prosecute economic and financial crimes of which electronic banking crimes form a part. Under Section 6 of the EFCC Act, the Commission is empowered to enforce and administer the provisions of the EFCC Act, Investigate all financial crimes including advance fee fraud, counterfeiting, money laundering, illegal charge transfer, online market fraud, computer credit card fraud, cybercrime, contract scam. The Commission is also to coordinate and enforce all economic and financial crimes laws as well as adopt measures to identify, trace, freeze, confiscate or seize proceeds from terrorist activities, economic and financial crime-related offences, etc.[1]

[1] Economic and Financial Crimes Commission Act 2004, s 6(1-4)

The Act also empowers the Commission to liaise with the office of the Attorney-General of the Federation, the Nigerian Customs Service, the Immigration and Prison Service Board, the Central Bank of Nigeria, the Nigerian Deposit Insurance Corporation, the Nigerian Drug Law Enforcement Agency and all other security and law enforcement agencies in the fight against economic and financial crimes; facilitate an efficient exchange of scientific and technical information and the conduct of joint operations towards the eradication of economic and financial crimes; also the commission must receive reports of suspicious financial transactions, analyze and disseminate same to all relevant government agencies among others.[2] By the functions vested in it, the Commission has the power to investigate any person, corporate body or organization that is suspected to have committed an offence related to economic and financial crimes under the EFCC Act or any other enactment under which the Commission has powers to administer.[3] The Commission is structured into various units for ease of operation and optimal functionality including the General Investigation Unit,[4] the Legal and Investigation Unit,[5] and the Nigerian Financial Intelligence Unit.

The investigative and prosecutors role of the EFCC in tackling cases of financial and banking crimes was showcased in some cases handled by the commission[6] Recently, it is reported that the Ibadan Zonal Command of the EFCC secured the conviction of seventeen internet banking fraudsters in Ogun, Oyo and Abeokuta. It has also been reported that the EFCC has secured convictions on Two Thousand, Two Hundred and Twenty (2,220) cases in the year 2021.[7] This figure is said to represent a 98.49% success rate in prosecution.

The EFCC has also mapped out strategies and policies to effectively tackle the transnational nature and scope of cybercrime and cybercriminals.[8] It collaborates with the National

[2] Economic and Financial Crimes Commission Act 2004, s 6 (5-8)
[3] Economic and Financial Crimes Commission Act, 2004, s 7(1)
[4] Economic and Financial Crimes Commission Act 2004, s 13(1)
[5] Economic and Financial Crimes Commission Act 2004, s 13(2)
[6] *Ude Jones Udeogu & Ors v Federal Republic of Nigeria* [2016] LPELR 40102 (SC)
[7] Adelani Adepegba, 'EFCC Flaunts 98.5% Prosecution Success Rate in 2021' (*Punch*, 07 January 2022) <https://punchng.com/efcc-flaunts-98-5-prosecution-success-rate-in-2021/> accessed 12 August 2022
[8] E Adomi and S E Igun, 'Combating Cybercrime in Nigeria' (2008) 26(5) Electronic Library Journal <https://doi.org/10.1108/02640470810910738> accessed 12 August 2022

Communications Commission (NCC) as well as the Federal Ministry of Justice in prosecuting cybercrime in Nigeria. The EFCC could be said to have attained a remarkable feat towards the prosecution of cybercriminals in Nigeria since its inception and establishment,[9] it has been acknowledged as having had substantial achievements in the prosecution of cybercriminals in Nigeria.[10]

THE ROLE OF NIGERIAN POLICE IN PROSECUTING ELECTRONIC BANKING OFFENCES IN NIGERIA

Another agency clothed with the power to prosecute cybercrime including electronic banking crimes in Nigeria is the Nigeria Police Force (NPF). The power to investigate crimes generally is vested in the NPF by the Nigerian Police Act, 2004 as amended.[11] The Police Force is a fundamental institution in any society as it helps in maintaining law and order by ensuring that crimes are combated if not eradicated from society.[12] The force is also assigned specific roles in the prosecution of cybercrimes in Nigeria by the force being listed as one of the major stakeholders in enforcing the provisions of the Cybercrime Act, of 2015.[13] The Nigerian Police is named among the Cybercrime Advisory Council alongside 24 others drawn from different ministries, departments and agencies.[14] However, the level of police achievement in prosecuting cybercrime in Nigeria is quite uncertain. While some think that the police have done tremendously well, others argue that the presence of police in Nigeria has yielded little or no results in cybercrime control in Nigeria. The low achievement of the police in cybercrime control and prosecution in Nigeria may not be unconnected to the fact that the police are vested with

---

[9] J N Edeh et al., 'Economic and Financial Crimes Commission Performance in Combating Corruption in Nigeria: Buhari's Administration in Perspective (2015-2020)' (2022) 17(1) International Journal of Development and Management Review <http://dx.doi.org/10.4314/ijdmr.v17i1.8> assessed 12 September 2022

[10] S Lazarus and G Okolorie, 'The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents' 40 Telematics and Informatics <http://dx.doi.org/10.1016/j.tele.2019.04.009> assessed 12 September 2022

[11] Nigeria Police Act 2020, s 4

[12] I. Oraegbunam, 'The Nigerian Police and Problem s of Cybercrime Investigation: Need for Adequate Training' (*Academia*) <https://www.academia.edu/26360705/The_Nigeria_Police_and_Problems_of_Cybercrime_Investigation_Need_for_Adequate_Training1> assessed 12 September 2022

[13] U Ismail, 'The Nigeria Police Force and Cyber Policing: A Synopsis' (2020) ResearchGate <http://dx.doi.org/10.13140/RG.2.2.30325.60647> assessed 12 September 2022

[14] Cybercrime Act 2015, s 42

the power of prosecuting matters at the Magistrate Court whereas electronic banking crimes and cybercrime generally statutorily fall outside offences under the jurisdiction of the Magistrate Court.

CHALLENGES OF LAW ENFORCEMENT AGENTS IN PROSECUTING ELECTRONIC BANKING OFFENCES IN NIGERIA

The effort of law enforcement agencies in the prosecution of cybercriminals is not without some challenges. These range from issues of jurisdiction and choice of court, extradition, mutual legal assistance and the challenge of admitting electronically generated evidence in courts. Others are corruption among law enforcement agents and underreporting of electronic banking offences.

JURISDICTION AND CHOICE OF COURT

The concept of jurisdiction has been defined as the authority, capacity, power or right to act or refrain from acting in a given manner. It could be described as the power conferred on courts to competently try and decide a matter before it. Before a court can competently try and decide a matter before it, it must ensure that it is clothed with the requisite jurisdiction to act.[16] Internationally, the concept of jurisdiction is often linked to sovereignty and provides States with the requisite power and authority to define and preserve the rights and duties of persons within their territory, enforce laws and punish violation of laws.[17] The choice of court is hinged on jurisdiction. States and countries primarily claim jurisdiction over crimes committed within their territories and try the same by the guidelines and provisions of their laws relating to the trial of such offences. For instance, Article 22 (1) of the Council of Europe's Convention on Cybercrime, 2001 states that parties to the Convention shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence when the offence is committed in its territory.

[16] *Dairo v Union Bank of Nigeria Plc* [2007] 16 NWLR 99
[17] UNODC Legal Framework on Human Rights 2013, n 9

However, the task of determining when an offence is committed in a nation's territory to assume jurisdiction is not an easy task when the offence involves cyberspace.[18] The growth and development of electronic commerce and communication have reduced the world into a global village and the international market into one accessible market by all and sundry.[19] Cyberspace has grown in both proportion and contents and presently seems borderless.[20] In electronic banking, services are delivered using the internet which functions in cyberspace. Different forms of crimes against electronic banking also take place in cyberspace.

Traditional offences are usually committed within a geographical location and territory, enabling law enforcement agents to easily define and determine the territorial authority and jurisdiction to apply in prosecuting the same. Cyber offences on the other hand take almost a formless and borderless shape.[21] In other words, determining jurisdiction and territorial boundary in cybercrime offences is not as easy as it is in other physical and conventional offences. The problem of jurisdiction faced in prosecuting cybercrime offences stems from the fact that cyberspace is devoid of any form of territorial boundaries. Usually, cybercrime, including electronic banking crimes is multi-national, cutting across several states, geographical entities and sovereign states. In some cases, an act of electronic banking crime may originate from one country, the proceeds passed through another country before it gets to perpetrators in yet another different country. In other cases, a server located in a country can be assessed in other countries. Also, a website registered and owned by a continent can be used and assessed in another continent entirely.

Owing to its multi-national nature, it is usually confusing determining the particular country reposed with jurisdiction in the prosecution of cybercrime offences. In other words, the nature, form and extent of cybercrime, by extension, electronic banking offences jurisdictions is not so clear as there seems to be no generally accepted mode of determining jurisdiction in electronic

[18] I.K.E Oraegbunam, 'Jurisdictional Challenges in Fighting Cybercrimes: Any Panacea from International Law?' (2015) 6 Nnamdi Azikiwe University of International Law and Jurisprudence

[19] Tushar Kanti Saha, 'Cyberspace: Conflicting Jurisdictional Spheres of Litigation Claims' (2010) 15(1) Journal of Intellectual Property Rights <http://docs.manupatra.in/newsline/articles/Upload/07D8E605-DE8C-435E-A7D5-16508E156554.pdf> accessed 27 Septmeber 2022

[20] *Ibid*

[21] P Prevey, 'Cyberspace and Jurisdiction' (2016) 2(5) Journal on Contemporary Issues of Law

banking offences especially when the offence cut across different states or countries which is almost always the case.

EXTRADITION

The issue of extradition is one of the brick walls faced by Nigerian law enforcement agents in the prosecution of electronic banking offences. Extradition can be defined as a procedure of transferring an accused person from his country of origin or residence to the country where an alleged offence is committed to attend his trial.[22] Extradition is directly tied to jurisdiction in that it can only apply if it is established that the court in the country where the fugitive is sought to be extradited to has the requisite jurisdiction to try the offence. In Nigeria, the procedure for extradition is controlled by the Extradition Act. Regarding electronic banking offences and cybercrimes generally, the Cybercrime Act provides that the Federal High Court has jurisdiction to the exclusion of other courts unless it is established that the accused person has been extradited to another country.[24] The above provision presupposes that the Federal High Court can order the extradition of any fugitive on Nigerian soil or territory whether or not the fugitive is a Nigerian.[25]

However, for an extradition request or proceeding to be effective, there must be an enabling instrument in the form of a bilateral treaty between the requesting state and the custodian state. Such treaties usually specify the form and nature of extraditable crimes that the states involved can entertain. For instance, the Extradition Treaty between Nigeria and the United States of America specifies extraditable crimes between the two states. These include offences relating to obtaining money, valuable security or obtaining goods by false pretense, receiving money, valuable security or other property knowing same to have been stolen or unlawfully obtained.[26] Apart from a treaty between a requesting state and a custodian state, extradition requests can only be honoured where the requesting and custodian states are members of the Economic

[22] O Ladipo and E O Okebukola, 'Cases and Materials on Extradition in Nigeria' (2016) 3 United Nations Office on Drugs and Crime Country Office in Nigeria
[24] Cyber Crime (Prohibition, Prevention, etc) Act 2015, s 50 (b)
[25] *Attorney General of the Federation v Dion Kendrick Lee* (2016) FHC/L/465C/11
[26] Extradition Treaty between Niigeria and the United States, art 3

Community of West Africa States (ECOWAS),[27] where the requesting and custodian states are members of the Commonwealth; and or where there is a reciprocity understanding between the custodian state and the requesting state.

Also, for a request for extradition to be honoured, the offence alleged must constitute an offence in both states. It must also be established that the alleged offender has not been earlier convicted in respect of the same offence and there is no likelihood of prejudice during the trial.[28] Where there is reasonable ground to believe that the fugitive will be tortured or prejudiced during the trial as a result of his race, colour, religion or nationality, an extradition request may not be honoured. This is in line with the United Nations Convention against Torture and other Inhuman or Degrading Treatments and Punishments.[29] The Extradition Act provides that where there is a pending criminal proceeding in any court in Nigeria over the same crime for which the fugitive is sought to be extradited, such extradition request will not stand.[30] Also, an extradition request may likely not be granted where the alleged fugitive is already being tried for another offence similar or different from the offence for which he is seeking to be extradited in the resident country.[31] This provision came to the fore in the 2022 extradition case involving the Federal Republic of Nigeria represented by the Attorney-General of the Federation and Deputy Commissioner of Police (DCP) Abba Kyari who is currently standing trial for Money Laundering and involvement in drug peddling.

Generally, an extradition request can succeed where there is an extradition enabling statute and documents between Nigeria and the fugitive country. These statutes sometimes specify the nature of extraditable offences that it entertains. For instance, extradition requests made to the United States of America from Nigeria may enjoy a smooth sail based on the existence of a recognized instrument. However, it becomes problematic when there are no such statutes. For instance, extradition of any form is grossly prohibited in Brazil. The Brazilian constitution of

[27] ECOWAS Convention on Extradition 1994, art 32(1)
[28] Extradition Act 1962, s 3(2)(b)
[29] Human and Peoples' Rights, art 3
[30] Extradition Act 1962, s 3(6)(a)
[31] Extradition Act 1962, s 3(6)(b)

1934 provides that 'no Brazilian citizen or national shall be extradited to any country for any form of prosecution irrespective of the nature of the offence.

MUTUAL LEGAL ASSISTANCE

Usually, Mutual Legal Assistance is employed towards obtaining useful materials that cannot be obtained based on police cooperation especially inquiries that require coercive means. Generally, for mutual legal assistance to exist and operate between states, there must be an enabling statutory document between the State Parties. For instance, there is a treaty between Nigeria and the United States of America on mutual legal assistance. This treaty was signed in Washington on the 13th day of September 1989.[32] In Nigeria, the Mutual Legal Assistance in Criminal Matters Act came into force in 2019. The main purpose of the Act is to obtain on a reciprocal basis from other countries, mutual assistance in the prosecution of criminal matters. To this end, Nigerian law enforcement agents can apply to other countries to be assisted in this regard following the legal procedure stated in the applicable laws[33]. Mutual Legal Assistance in the prosecution of electronic banking offences is provided for under section 52 of the Cybercrime Act, 2015 which provides that

(1) The Attorney-General of the federation may request or receive assistance from any agency or authority of a foreign state in the investigation or prosecution of offences under this Act; and may authorise or participate in any joint investigation or cooperation carried out to detect, prevent, responding prosecuting any offence under this Act.;

(2) The joint investigation or cooperation referred to in sub-section (1) above may be carried out whether or not any bilateral or mutual agreement exists between Nigeria and the requesting or requested state etc.

As earlier stated, mutual legal assistance operates between states that agree among themselves to assist one another when necessary in the prosecution of criminal matters. The problem may however arise where there is no such mutual agreement. The law enforcement agents of a

[32] *Ibid*
[33] *Ibid*

requesting state cannot force that of a requested state in assisting her. Despite the enabling law of the requesting state, it cannot prevail on the requested state to deliver information when the requested state is not willing to do so. Thus despite the wording of section 52(2) of the Cybercrime Act of 2015 which seems to rule out the existence of a prior treaty or agreement, the law enforcement agents in Nigeria cannot compel their counterparts in other states to deliver any information towards prosecution of a criminal in Nigeria.

ISSUES RELATING TO THE ADMISSIBILITY OF ELECTRONICALLY GENERATED EVIDENCE

This is yet another challenge faced by law enforcement agents in Nigeria in the prosecution of electronic banking offences and data insecurity relating to the delivery of electronic banking services by banks in Nigeria. The concept of evidence has been defined as anything that has to do with testimony, documents and tangible objects that tend to prove or disprove the existence of an alleged fact. Statutorily, evidence has been defined as 'anything other than testimony, admissible hearsay or document, the content of which are offered as evidence of fact at a trial, which is examined by courts as a means of proof of that fact.' Evidence is an integral part of every judicial system; it plays a vital role in establishing the parties' cases before the court.[35] Among the different types of evidence is electronic evidence which is defined as 'any evidence obtained from data contained in or created by any device, the operation of which depends on software or data stored or transmitted through a computer system.'[36]' Electronic evidence can take many forms such as writing, pictures, audio and photographs through which a crime perpetrator and the victim can be linked to the crime.[37] In general law of evidence, the admissibility of a piece of evidence including electronic evidence is based on the relevance of the piece of information or evidence sought to be tendered to the facts in issue. The relevance of

[35] M Danjuma et al.,'Science, Electronic Evidence and Cybercrime Prosecution in Nigeria' (2018) Journal of Cyber Criminology and Technology <https://www.researchgate.net/publication/341480412_Forensic_science_electronic_evidence_and_cybercrime_prosecution_in_Nigeria> accessed 12 September 2022

[36] A F Mousa,' Electronic Evidence and its Authenticity in Forensic Evidence' [2021] 11(20) Egyptian Journal of Forensic Sciences <https://ejfs.springeropen.com/articles/10.1186/s41935-021-00234-6> accessed 12 September 2022

[37] *Esso West Africa v Oyegbola* [1969] 1 NMLR 194

electronically generated evidence or any form of evidence is tied to its authenticity; that is fulfilling the requirements for the admissibility of the piece of evidence. Thus, law enforcement agents have the task of ensuring that the required procedure is followed to the latter. Failure to achieve this may be disastrous despite the importance of the evidence sought to be tendered.

Another requirement for admissibility of electronically generated evidence is provided for under section 84(4) of the Evidence Act which provides for certification of the piece of evidence by the party seeking to tender it or the party from whose custody it emanates. The provision of this subsection may spell doom for a law enforcement agent or any person in possession of credible electronically generated evidence, relevant to the case as some would nevertheless be rejected for want of certification.[38] The task of establishing that the device is regularly and properly used for activities regularly carried out by it in the ordinary course of business can only be established by one person - the owner or operator of the device. This fact makes the job of law enforcement agents more tasking. For instance, where an internet fraudster is being prosecuted, the device through which the crime is committed belongs to the user-the accused and more often than not, the devices/phones are secured or encrypted with passwords and codes best known to the user who for obvious reasons will not be willing to disclose the password or any vital information contained in the phone. A more intricate situation arises where the accused elects to exercise his constitutional right to remain silent.[39] This right implies the right of an accused person, in this case, the owner and or user of the telephone not to be compelled by the court even through a subpoena to testify in his trial.[40]

WEAKNESSES IN THE APPLICABLE LAWS

The job of law enforcement agents is to enforce the provisions of statutes as interpreted by courts through judicial decisions. However, weaknesses in substantive laws affect the output of the court's decisions. This in turn limits the level of success of law enforcement agents. In prosecuting electronic banking and cybercrime offences in general, the applicable laws in

[38] *Ohamuo v UBA* [2016] KK/007CV/14
[39] Evidence Act 2011, s 36(11)
[40] *Igbele v State* [2006] All FWLR 1797

Nigeria range from the Cybercrime Act, 2015, the Economic and Financial Crimes Commission (EFCC) Act, Money Laundering Act among others. Two major challenges are inherent under the Cybercrime Act are discussed in the next two sub-segments of this paper.

BURDEN OF PROOF UNDER SECTION 19 (3)

Considering the nature of electronic banking crimes and the nature of facts sought to be proven, one cannot but agree with scholars who opine that the Subsection places a stringent and harsh liability regime on bank customers.[41] More so, when the provision of section 84(2) of the Evidence Act, 2011 on the manner electronically generated evidence can be tendered is considered. Section 84(2) provides that anybody seeking to tender electronically generated evidence must lead evidence to show that the device from where the evidence sought to be tendered is derived is used for the purpose for which it is used in the ordinary course of business. As such, a bank customer faced with this will have an uphill task attempting to prove the fact of this negligence from a device owned and maintained by the bank.

THE REQUIREMENT OF OBTAINING A WARRANT OF ARREST BEFORE AN ARREST CAN BE VALIDLY MADE

This constitutes a clog in the wheel of progress for law enforcement agents.[42] Before a law enforcement officer can legally carry out an arrest or search in respect of any offence provided for under this Act, including electronic banking offences, the police officer involved has to obtain a warrant of search or arrest as the case may be. The requirements of the Act can be fulfilled by obtaining an *ex parte* order which appears easy enough to secure. However, the nature of cybercrime offences which is committed on the internet where evidence can be wiped off in a couple of seconds poses a worrisome situation. This is in addition to prevalent delays in the Nigerian judicial system which leaves much to be desired. A law enforcement agency may validly suspect a person or premises of an act of cybercrime but will not act immediately as the

[41] Uchenna Jerome Orji, 'A Review of Special Duty of Banks Under the Nigerian Money Laundering Act' (2011) 26 (6) Journal of International Banking Law and Regulation <https://www.researchgate.net/publication/322078292_A_Review_of_the_Special_Duties_of_Banks_under_the_Nigerian_Money_Laundering_Act> accessed 12 September 2022

[42] Economic and Financial Crimes Commission Act 2004, s 45

law requires a warrant before any step can be taken. However, the same evidence for which a warrant is sought for may be wiped off the device before the warrant is secured. More so, a warrant of arrest is expected to carry the name of the suspect as well as the address of the premises and gadgets used in the commission of this crime. The task of securing this information before applying to the court for a warrant makes the job of law enforcement officers tedious. Again, granting an application for a warrant is not automatic under the Act. By subsection (3), before a judge can issue a warrant of this nature, he has to be convinced that the warrant is going to be used for the purpose for which it is sought which is the prevention of crime commission, investigating an act of cybercrime and security breach. To convince a judge in this direction may not be as easy as it may entail presenting facts that may not be at the disposal of the applicant.

In reality, police officers in Nigeria are presently in the habit of randomly arresting and searching young men and women suspected to be involved in cybercrime usually based on their dress and general outlook. This may be justified under the Police Act of 2004 which equips police officers in Nigeria with the power to arrest and search without a warrant in deserving circumstances. However, by sections 37(1) and 41 of the 1999 Constitution as amended, an alleged internet fraudster, arrested and or searched without a warrant reserves the right to sue for enforcement of his fundamental right to privacy and right to freedom of movement. Section 37 of the 1999 constitution provides that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications are guaranteed and protected' while section 41 provides that 'every citizen of Nigeria is entitled to move freely…' Thus, the aggrieved person who is wrongfully arrested and or searched can institute an action against the concerned police officer for enforcement of his fundamental human right under the above sections of the constitution. In the case of *Hassan v Atanyi,*[43] it was held that an action of this nature does not lie against the concerned police office alone but against the entire police force.

[43] *Hassan v Atanyi* [2002] 8 NWLR 587

ANONYMOUS NATURE OF CYBER FRAUDSTERS

Anonymity could be defined to mean the state of facelessness or absence of identity. The perpetrators of fraud in cyberspace could best be described as anonymous, faceless and without identity in most cases. The nature of cyberspace makes it possible for identity to be easily hidden, stolen, and duplicated at will. Cyber fraudsters usually pose as who they are not to attack vital information of unsuspecting bank customers and members of the public and corporate organizations. For instance, the rate at which different social media accounts are presented purportedly owned by top and influential businessmen and women, politicians and celebrities is alarming.[45] Fraudsters usually create these fictitious accounts on different social media handles to impersonate these personalities to defraud unsuspecting members of the public including foreigners.[46]

For instance, these fraudsters can pose as businessmen who have been awarded contracts but have no funds to execute them; imploring their victims to finance the fictitious contract with the promise of a certain percentage of remuneration once the contract is fully executed. The victims, especially foreign investors buy into this idea believing that they are dealing with real businessmen. However, once they are cajoled into parting with money, the fraudsters delete all traces of the fraudulent transaction and block the victim from getting close to him by all means.[47]

Anonymous cyber fraudsters can strike any individual or corporate body's account in any part of Nigeria or the world.[48] For instance, in 2018, it was reported that commercial banks in Nigeria lost more than 39 Million Dollars to electronic Fraud perpetrated by unknown fraudsters.[49] An act of cyber fraud can cut across countries and continents even while the perpetrator's identity

---

[45] Jesse D. Bray, 'Anonymity, Cybercime and the Connections to Cryptocurrencey' (*Encompass*, 2016) <https://encompass.eku.edu/etd/344/> accessed 12 September 2022
[46] *Ibid*
[47] *Ibid*
[48] *Ibid*
[49] Chidubem Izuakor, 'Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context' (2021) 1 International System Security Association Journal <https://www.researchgate.net/publication/350941930_Cyberfraud_A_Review_of_the_Internet_and_Anonymity_in_the_Nigerian_Context> accessed 12 September 2022

is hidden. For instance, the allegation and arrest of two Nigerian citizens resident in the United Arab Emirate- Ramon Olorunwa a.k.a Hushpuppi and Olalekan Jacob Ponle a.k.a Woodberry by Dubai security operatives and their subsequent extradition to the United States to answer to crimes committed against the United States while resident in Dubai and Nigeria respectively is a clear case of intercontinental crime.[50] This usually poses a difficult task on the law enforcement agents who face the initial take or unraveling the true identity of the fraudsters before delving into prosecution proper.[51] In his case, it was alleged that Hushpuppi and his team posed as businessmen intending to finance a school, impersonating bank officials by creating a bogus website for that purpose.[52]

UNDERREPORTING

Another factor affecting the effort and output of law enforcement agents in the prosecution of electronic banking offences and cybercrime generally is the fact that incidences of cyber-attacks are underreported by victims and affected persons. Law enforcement agents usually act upon information available to them often volunteered by persons and bodies directly involved or affected by acts of electronic banking fraudsters. The statistics of prosecuted cyber offences and prosecuted offences or dearth of cyber-attacks are incomparable.

While cyber-attack is on the rise, the prosecuting index appears static and sometimes dwindling.[53] Unfortunately, only a few affected persons come out to report their ordeal especially when the loss seems insignificant. For instance, a cyber-fraudster may target and attack five hundred thousand bank accounts, fraudulently deducting say, One Thousand Naira from each of the accounts which culminates into a whooping sum of fifty Million Naira. Sadly, only a very few persons among these affected account holders will approach appropriate law

---

[50] *Ibid*
[51] *The Federal Republic of Nigeria vs Olayinka* [2013] LCD/177/2012
[52] 'Hushpuppi: Nigerian Influencer Pleads Guilty to Money Laundering' (*BBC News*, 29 July 2021) <https://www.bbc.com/news/world-africa-58002932> accessed 20 November 2022
[53] Suleman Ibrahim, 'Social and Contextual Taxonomy of Cybercrime: Socio-Economic Theory of Nigerian Cybercriminals' (2016) 47 International Journal of Law Crime and Justice <https://doi.org/10.1016/j.ijlcj.2016.07.002> accessed 25 July 2022

enforcement agents to lay complaints; the rest will shove it aside, sometimes considering the physical and financial stress that may be involved in bringing this type of complaint to law enforcement agents in Nigeria. Organisations in Nigeria suffer more cyber-attacks than any other country in Africa. However, these attacks go unreported despite a mandatory statutory regulation for disclosure.[54] According to the president of the Cybersecurity Experts Association of Nigeria (CSEAN), Remi Afon, while the Cybersecurity landscape in Nigeria evolves rapidly and attacks increase in number and sophistication, most data breaches in Nigeria go unreported. Thus, law enforcement agents are usually stalled towards effective enforcement and prosecution in the face of underreporting and lack of scanty information.

PREVALENCE OF CORRUPT PRACTICES LAW AMONG ENFORCEMENT AGENCIES IN NIGERIA

The major law enforcement agent saddled with the responsibility of prosecuting cybercrime prosecution in Nigeria is the Economic and Financial Crimes Commission, using the instrumentality of the Nigerian police and collaborating with the Federal Ministry of Justice.[56] The police carry out arrest, search and investigation of persons suspected to have engaged or premises suspected to have been used in perpetrating cybercrime and offences against electronic banking. Over time, policing in Nigeria has developed and evolved. However, corruption in the police force has equally evolved in form and format.[57] Police corruption is a universal problem; however, it is a serious challenge in Nigeria with ever-increasing misconduct that impact negatively on the development of police institutions in Nigeria.[58] The problems with the

[54] Abubakar Idris, 'Why some of Nigerian Worst Cyber Attacks are not Reported' (*Techabal,* 24 April 2023) <https://techcabal.com/2020/07/21/why-some-of-nigerias-worst-cyberattacks-are-not-reported/> accessed 25 July 2022

[56] F E Eboibi, 'Curtailing Cybercrime in Nigeria: Applicable Laws and Derivable Sources' (2017) 2 African Journal Of Criminal Law And Jurisprudence <https://www.researchgate.net/publication/336243066_Curtailing_Cybercrime_in_Nigeria_Applicable_Laws_and_Derivable_Sources> accessed 25 July 2022

[57] R Aborisade and J A Fayemi, 'Police Corruption in Nigeria: a Perspective on its Nature and Control' (2006) 18(2) Nigerian Journal of Social Studies <https://njss.org.ng/publications/NJSS%20Vol.%20XVIII%20(2)%20October%202015/Untitled-55.pdf> accessed 25 July 2022

[58] *Ibid*

Nigerian police span all levels and cadres of the police force. At the topmost cadre, senior police officers embezzle staggering sums of public funds. Meanwhile, at the lower levels, rank-and-file police officers regularly extort money from the public including crime victims before handling their cases.[59] Corruption in the police force manifests more in the fight against cybercrime and a crime against electronic banking service delivery. For instance, a police officer in Nigeria faced with a complaint on unauthorized access to bank accounts or other forms of cyber fraud usually demands some form of gratification, mostly monetary, from the affected individual or organisation before commencing action of any sort.

LIMITED KNOWLEDGE OF ICT BY THE PROSECUTION

Through their training, lawyers and judges possess some knowledge about different spheres and aspects of human life and existence. However, owing to the nature of the Internet which is relatively new, not many lawyers are well-equipped and acquainted with the functional and operational mechanisms of the Internet. This usually poses a serious challenge considering the proposition of the realist school of law which states that law is what the courts will do in fact and nothing more pretentious. Judges are guided by the evidence adduced during the trial to arrive at a decision one way or the other. When the prosecuting counsel is not knowledgeable in the workings of the internet, he may not have what it takes to appropriately present evidence before the court to sway the mind of the court. This, no doubt constitutes a serious setback to law enforcement agents in Nigeria.

SLOW PACE OF JUDICIAL PROCEEDINGS IN NIGERIA

The long period usually taken to conclude a matter in Nigeria is worrisome. This challenge is even more acutely felt in the trial of offences involving the Internet. Delay in the prosecution of cyber offences may lead to loss of evidence as a result of virus invasion, breakdown and malfunctioning of devices that house the needed evidence, etc. It is common knowledge that

[59] Marvellous Iheukwumere, 'Fighting Police Corruption in Nigeria: An Agenda for Comprehensive Reform' (*The Global Anticorruption Blog,* 06 Septmeber 2019) <https://globalanticorruptionblog.com/2019/09/06/fighting-police-corruption-in-nigeria-an-agenda-for-comprehensive-reform/> accessed 25 July 2022

access to our courts for legal redress has been hampered on account of several reasons. This has negatively affected the quality of decisions and judgments delivered by the courts in Nigeria which in turn leads to diminished confidence and interest in the judicial system by the masses.[61] These challenges affecting law enforcement agents in Nigeria constitute a clog in the wheel of effective prosecution of cybercrime, including electronic banking offences in Nigeria. This problem is so fundamental that it has almost crippled the functionality of these agencies

PROSPECTS IN PROSECUTING ELECTRONIC BANKING OFFENCES IN NIGERIA

The above-identified problems have bedeviled the effort of the relevant law enforcement agencies in prosecuting electronic banking crimes in Nigeria. Despite these challenges and shortcomings, it is expected that prosecuting cyber criminals and perpetrators of electronic banking crimes will enjoy a positive atmosphere in the nearest future. In other words, it is believed that if the recent innovation in laws, policies and procedures in the area of criminal litigation is applied towards prosecuting perpetrators of electronic banking crimes, cases of data insecurity associated with electronic banking will enjoy smooth prosecution, free from hitches and bottlenecks in the nearest future. This in turn will reduce cases of data insecurity in the banking sector to the barest minimum.

Several factors may serve to whittle down the challenges associated with prosecuting electronic banking offences in the nearest future if clinically implemented. Foremost among these factors is the Passage of the Administration of Criminal Justice Act (ACJA) in 2015. The ACJA brought about several groundbreaking innovations which ultimately serve to guarantee the speedy dispensation of justice in criminal litigation. Also, the introduction of the Know Your Customer (KYC) Scheme by the Central Bank of Nigeria vide a Manual in 2003 is another factor that may serve to reduce the problems associated with the prosecution of electronic banking offences. This manual, which predates the era of electronic banking, stipulates that banks and other financial institutions should not establish business relationships until all relevant parties to the transaction are known. This applies to the opening of accounts, fund transfers, cash withdrawals

[61] Rufai Muftau, 'Access to Judicial Justice in Nigeria: The Need for Some Future Reforms' (2016) 47 Journal of Law Policy and Globalization <https://core.ac.uk/download/pdf/234650565.pdf> accessed 04 August 2022

as well as deposits. This will go a long way in checking the menace of identity theft associated with electronic banking offences.

The introduction of the Bank Verification Number (BVN) Scheme by the Central Bank of Nigeria in 2014 is another positive step that can ensure the drastic reduction of the incidence of electronic banking offences and facilitate the prosecution of the same. The BVN consists of eleven digits and assigns a single identity to a bank customer despite the number of accounts maintained in various banks. The BVN ensures the safety of depositors' funds and the prevention of identity theft and checkmate fraud. It, therefore, serves to reduce illegal banking transactions and shores up bank/customer confidence. Another very important prospect in enhancing the prosecution of cybercrime is the proposed amendment to the Cybercrime Act. The call for the amendment of the Act followed a decision by the Economic Community of West African State (ECOWAS) court wherein Section 24 of the Cybercrime Act was held to be incompatible with certain provisions in the African Charter of Human and Peoples Rights as well as the International Covenant for Civil and Political Rights.[62] Finally, the recent Memorandum of Understanding between the INTERPOL and Law Enforcement Agents in Nigeria, among which are the Police, Independent Corrupt Practices Commission, (ICPC) and the Economic and Other Financial Crimes Commission, (EFCC) is a huge step that will bring relative ease to the prosecution of high profile criminal cases, including electronic banking offences. By this MOU, any of these agencies can issue a notice on a high-profile suspect whose notice will be seen globally. The MOU also grants the ICPC the opportunity to join a global anti-crime network that displays the identity of crime suspects in every part of the world.

In addition to the above, the following measures may be adopted and integrated by appropriate government agencies in the prosecution of electronic banking offences in Nigeria to facilitate the process and ensure maximum output. Adequate resources should be allocated to the technical presentation of cases, due diligence should be employed towards evidence gathering, and law enforcement agencies should avoid filing charges before the conclusion of investigations.

[62] *SERAP v Federal Republic of Nigeria & Ors* Unreported Suit No. ECW/CCJ/APP/53/18

Furthermore, relevant agencies must learn from their counterparts in other climes and the political class should refrain from interfering with the process,

CONCLUSION

The role of regulatory agencies such as the EFCC in the prosecution of general cybercrime and offences relating to electronic banking in Nigeria cannot be overemphasized. However, as revealed in this paper, law enforcement agencies are hamstrung with constraints that act as a clog in the wheel of effective prosecution of persons accused of electronic banking offences. Until these challenges are properly addressed, relevant law enforcement agencies will continue to experience low output despite efforts to curb electronic banking crimes by prosecuting offenders.