GAL EXAMINATION OF CYBER FRAUD IN NIGERIA BANKING TRANSACTIONS

Hamisu Sani PhD
Abuja-based Legal Practitioner

Abstract

The advent of technology has revolutionised the global financial sector and provided unprecedented convenience and efficiency in banking operations. However, this transformation has ushered new challenges, especially the alarming rise in cyber fraud in Nigeria's banking transactions. The aim of the paper is to examine the multifaceted cyber fraud in banking transactions, with a focus on the relevant provisions of the Cybercrimes (Prohibition, Prevention) Act, 2015. The paper provided an overview of the evolving cyber threat to the banking transactions in Nigeria, thereby outlining the various forms of cyber fraud that continuously affect the Nigeria's banking transactions. It discussed the tactics employed by cybercriminals to defraud the banks and their respective customers, wherein the criminals include the staff of the bank and third party in order to perpetrate the cybercrime in banking industry. The paper discussed the duties of banks towards mitigating cyber risks, implementation of robust cybersecurity measures and customer sensitisation. It was observed that when a customer is defrauded, hen is required to prove that the bank has failed to put security measures in place to protect his data and/or information. It was also observed that some provisions of the Cybercrimes (Prohibition, Prevention) Act, 2015 did not take into the balance of probability as well as economic impact of the cyber frauds while prescribing the punishment for the offence hence the recommendations to place burden of proof on the bank that the customer has compromised his password or banking details, and the amendment of Cybercrimes (Prohibition, Prevention) Act, 2015 in line with the reality and capacity of the parties to banking transactions.

1.1 Introduction

The State is enjoined to direct its policy towards ensuring the promotion of a planned and balanced economic development.[1] Such policy includes legislation which will provide conducive environment for economic activities. As a result, the Federal Government passed several legislation that are geared towards prevention and prohibition of Financial Malpractices and Fraud in Nigeria.

However, the change of pattern in commission of crimes from conventional system to cyberspace fraud, especially in banking operations, is bound to drastically affect economic growth. Therefore, the prevalence of cyber fraud and malpractices in the banking operations is harmful to the economic activities and growth of the nation and it becomes worrisome. In view of this unfortunate situation, this paper aims to identify and examine, within the context of Cybercrimes (Prohibition, Prevention) Act, 2015, the prevalence of cyber frauds and malpractices in banking operations in Nigeria to disclose their respective characteristics and method of operation.

1.2 Cyber Fraud in Banking Operations

One of the sectors that have been affected by the growing trend of cybercrimes in Nigeria is the banking and financial services sector. In this regard, both banking and financial institutions as well as their customers have become target of cybercrime activities. To protect computer and network, the Federal Government of Nigeria enacted Cybercrimes (Prohibition, Prevention) Act, 2015 (the Act) which criminalises cybercrime and provides for protection of critical national information infrastructure. The Act also introduced a range of provisions that aimed at protecting the users of electronic banking and payment services from cybercrimes.

The word "Cyber" refers to "internet or computer wide area of network."[2] It also denotes "a platform to perform different human activities which congregate on internet."[3] Any offence that is committed through cyberspace is called "cybercrime" or "computer crime." The cybercrime or computer crime refer to instances where digital technologies are either the target of a malicious or

---

[1] Section 16(2)(a) Constitution of the Federal Republic of Nigeria 1999 (as amended), Cap. C 23, Laws of the Federation of Nigeria, 2004.

[2] Nwaze, C. (2020), Financial Fraud in Nigeria: The Banking Perspective with Evidence-Based Cases and Preventive Measures, CIBN Press Limited, p. 303.

[3] Joshi N. (2018) *E-Crimes & Fraud*, Kamal Publishers, D-232, New Delhi, p. 9.

unlawful activity or the instrument for facilitating a crime or malicious activity. Cybercrime has also been defined as "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks."[4]

Accordingly, the term is used to describe a range of offences including traditional computer crimes, as well as network crimes. However, there are different views as to the most appropriate legal definition of what constitutes 'cybercrime' or 'computer crime'. Generally, cyber security laws tend to avoid such explicit definitions.[5] The Cyber fraud in banking operations can be committed through several ways. Some of the methods for committing such offence are discussed hereunder.

1.2.1 Automated Teller Machine Fraud

Automated Teller Machines (ATM) fraud occurs in two broad ways. First is by skimming, where a device is attached to the card entry slot of the machine to record or copy the electronic details from the magnetic stripe of the cards inserted into a cash machine. A separate miniature pinhole is hidden overlooking the Personal Identification Number (PIN) pad to film the card holder inputting the PIN.[6] This enables the fraudster to produce counterfeit card with real card details and withdraw money at the cash machine using the PIN of the actual card holder.[7]

The second way for committing ATM Fraud is by card trapping. A device is inserted into a cash machine card slot, which retains the card inside the machine. The fraudster then tricks the cardholder into re-entering his PIN while the former looks helpful but in fact, he is copying the card particulars for fraudulent use.[8] These two types of ATM fraud have been prohibited and punished by Section 22(2) & (3) of Cybercrimes Act, 2015, which provides as follows:

---

[4] Orji, U.J. (2019) Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. Tilburg Law Review Journal of International and European Law. https://doi.org/10.5334/tilr.137 p.105 accessed on 7th June, 2020 at 12:00pm

[5] Ibid.

[6] Ibanichuka, E.A.I., *et al.* (2019), Electronic Fraud and Financial Performance of Quoted Commercial Banks in Nigeria, International Journal of Advanced Academic Research, Vol. 5, Issue 4, pp. 21-22.

[7] Emiefo, P. (2019), Electronic Banking and Fraud: Issues Related to Effective Implementation, available at http://www.globalacademicgroup.com/journals/pristine, accessed on 27th April, 2020.

[8] Olukole, O. (2009), (2009), Nigerian Electronic Banking Law, Nonesuch House Publishers, Kings Plaza, Alaafin Ave, Ibadan, p. 72,

Section 22(2) "Any person fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person"; or

Section 22(3) "fraudulently impersonates another entity or person, living or dead, with intent to-

a) Gain advantage for himself or another person:
b) Obtain any property or an interest in any property:
c) Cause disadvantage to the entity or person being impersonated or another person; or
d) Avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice. with not more than five years imprisonment or a fine of not more than N7 million or both.

A practical illustration of the above provisions is contained in the case of *Public Prosecutor vs. Navaseelan Balasingam.*[9] The accused was a British national of Sri Lankan descent who had entered Singapore on 28th February 2006 on a 14-days social pass. At the invitation of a person called 'Kumar', he engaged in a course of conduct that involved withdrawing cash from ATMs of the United Overseas Bank (UOB) by using fake ATM cards,[10] which had been supplied by Kumar. During the illegal cash withdrawals, the accused wore a cap provided to him by Kumar to avoid identification by CCTV cameras installed at the ATMs. Despite this, video images of the accused withdrawing cash from the ATMs were captured by the cameras. On 4th March, 2006, the accused was seen and detained by the bank officer while trying to make an unauthorized withdrawal from an ATM located at Havelock Road in Singapore's city center. On being arrested by the Police, a search revealed that he had 22 counterfeit ATM cards in his possession, cloned from originals belonging to account holders living in the UK. At trial, the accused pleaded guilty to 5 charges of computer access with intent to commit or facilitate the commission of an offence under section 4 of the Computer Misuse Act and 5 charges under section 379 of the Penal Code for stealing funds from UOB through these transactions.[11]

---

[9] [2006] SGDC 156 [Navaseelan Balasingam (D.C.)] See also the case of *Guaranty Trust Bank vs Motunrayo-Tolulope Aloegena*, Suit No. CA/L/461/2016 (Unreported); Judgment delivered on 1st March, 2019.

[11]Urbas G. (2008), An Overview of Cybercrime Legislation and Cases in Singapore, Asia Law Institute, ASLI
Working Paper No. 001, p. 11. Available at http://law.nus.edu.sg/asli. Retrieved on 17th November, 2019.

An ATM fraud can also be committed against the bank whereby the fraudster steals bank's money from ATM. In the case of *Patty vs Commonwealth Bank of Australia,*[12] the Australian Dollars in the sum of $27,400.00 was stolen from the ATM of Commonwealth Bank of Australia (the Bank), located at 150 Smith Street, Collingwood branch. The Bank reported the case to the police and the latter investigated the complaint and reached a conclusion that there was insufficient evidence to prosecute. The Bank then used its Internal Investigation report wherein its staff, Mr. Patty was suspected to have committed the fraud. As a result, the staff was dismissed from the employ of the Bank. Consequently, the staff filed a petition before Industrial Relations Court of Australia and challenged his dismissal. At the trial, the Court held that the Bank has contravened section 170DE (1) of the Australian Labour Act by terminating the employment of the applicant without a valid reason for doing so.

Similarly, in the case of *Adeniyi Momodu Allison vs Bow Street Magistrates' Court*[13] Joan Ojomo was an employee of American Express at credit section. She fraudulently gave the information of their customers to Mr. Allison, which were used by the later to obtain large sum of money from ATMs. The above case showed how staff of financial institutions could fraudulently supply customers' information to a third party for commission of automated teller machine fraud which is termed as Identity Theft and Impersonation under Cybercrime Act.[14]

1.2.2 Electronic Fund Transfer Fraud

Electronic Fund Transfer (ETF) is a transaction which could be carried out from one bank to another or from one account to another, through ATM,[15] Internet, Mobile Phone or Point of Sale device.[16] ETF is simply the use of electronic means to transfer funds directly from one account to another, rather than by cheque or cash.[17] According to Section 205(3)(b)[18] the term "Electronic Fund Transfer" means:

---

[12] Industrial Relations Court of Australia, VI-2542 of 1996; (2000) FCA 1072.
[13] (1998) FWHC Admin 536.
[14] Section 22(2) and (3), Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
[15] Goldface-Irokalibe, I.J. (2020), Law of Banking in Nigeria, Malthouse Press Ltd, 43, Onitsha Street, Surulere,
Lagos.
[16] Joshi, N. (2018), E-Crimes & Fraud, Kamal Publishers, D-232, Sarvodaya Enclave, New Delhi, p. 224
[17] Stanley, K.O., *et al.* (2019) "Electronic Fraud and Credit Facilitation in Banks in Nigeria", Journal of Accounting Information and Innovation, Vol. 5, No. 10: Available at https://www.cird.online/JAII; accessed
on 2nd February, 2020.
[18] United States Electronic Funds Transfer Act, 1978.

> Any transfer of funds other than a transaction originated by a cheque, draft or similar paper instrument, which is initiated through an electronic terminal, telephone instrument or computer or magnetic tape, so as to order, instruct, or authorize a financial institution to debit or credit an account. Such term includes, but not limited to, Point of Sale Transfer, Automated Teller Machine transactions, direct deposit or withdrawal of funds and transfer initiated by telephone and transfers resulting from debit card transactions, whether initiated through an electronic terminal.

To regulate Electronic Fund Transfer transactions, the Central Bank of Nigeria issued a revised Regulation on Instant (Inter-Bank) Electronic Funds Transfer Services in Nigeria.[19] The Regulation set out guidelines for settlement of funds transfer between financial institutions and procedure for dispute settlement. While banks provide electronic means to enable their customers transact banking business without going to their branches, fraudsters are taking advantage of such electronic medium to commit fraud against banks or customers. EFT fraud is normally perpetrated when a third-party gains access to the database of the bank and withdraws funds from the system.[20] It also happens when a fraudulent insider within the bank divulges the relevant coded numbers required for payment to a third party or customer.[21]

1.2.3 Transfer Fraud by Hacking

Transfer fraud could be committed by hacking into the system of a bank and intercepting the code of innocent bank's staff that logged on to the system for operation. The fraudster then uses the password of such innocent staff and debit either the bank's general ledger or customer's account and transfer the amount of money to different account(s) in either the same bank or another bank. In the case of *Unity Bank Plc vs Mr. Akande Temitope &n 3 Ors,*[22] an operation staff of the appellant went to the Branch on Saturday with some of her colleagues for the purpose of balancing the ledger of the appellant. At the time the staff was logging into the system, fraudsters intercepted and used her password and

---

[19] Circular No. BPS/DIR/GEN/CIR/05/11, 13th September, 2018.

[20] Ibrahim, U., (2019), The Impact of the Cybercrime on the Nigerian Economy and Banking System, NDIC Quarterly- Q1-and-Q2 2019 Article, available at https://www/ndic.gov.ng Accessed on Monday, 11th May, 2019.

[21] Olukole, O., Op. cit. p. 76.

[22] Suit No. OY/HC/MISC/59/ (unreported).

eventually debited the appellant's general ledger with the sum of N1.2Billion and credited same into various accounts of the appellant's customers. Fortunately, the attempted fraud was discovered before transferring the money outside the bank's system.

In the case of *R vs. Stubbs,*[23] the Appellant was convicted for an offence of conspiracy to defraud. A sentence of 5 years imprisonment was subsequently imposed on the Appellant for his involvement in a fraudulent money transfer from HSBC Bank totaling about 11.8 million pounds. This type of offence is prohibited by Section 12(1) of the Act[24] which states that: " Any person, who intentionally and without authorization, intercepts by technical means, non-public transmissions of computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment."

1.2.4 Unlawful Manipulation of ATM and Point of Sale Terminals

Section 30(1) of the Cybercrimes Act provides that any person who manipulates an ATM or POS terminal with the intention to defraud shall be guilty of an offence and, upon conviction, sentenced to five years imprisonment or a fine of N5 million or both.[25] Similarly, subsection (2) thereof provides that: "Any employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using an ATM of Point of Sale device, shall be guilty of an offence and, upon conviction, sentenced to Seven Years imprisonment without an option of fine."[26]

The above provisions of Section 30(1) and (2) of Act[27] criminalise the manipulation of ATM and PoS terminals with intent to defraud. They also prohibit the commission or facilitation of such act by a staff of banks and financial institutions. The section did not require that the intent to defraud will have to be targeted at either a customer or banking/financial institution for criminal liability to attach. Therefore, the provision also applies to a situation where an ATM or POS terminal is manipulated for the purpose of defrauding a

---

[23] (2006) EWCA Crim 2312
[24] Cybercrimes (Prohibition, Prevention Etc.) Act, 2015, Op. cit.
[25] *Jude v. Citibank, N.Y. City Civ. Ct.*, 435 N.Y.S. 2d 210.
[26] Section 30(2), Cybercrimes (Prohibition, Prevention Etc.) Act, 2015, Op. cit.
[27] Ibid.

customer. Consequently, the provision promotes the protection of customers that use ATM and POS terminals for electronic banking or payment transactions, and, therefore, it enhances consumer trust in the use of such electronic banking and payment channels.[28]

1.2.5 Phishing Scams and Electronic Card Fraud

The Cybercrimes Act criminalises phishing scams that target consumers in the banking and financial sector. Section 32(1) of the Act[29] provides that "Any person who knowingly or intentionally engages in computer phishing shall be liable upon conviction to 3 years imprisonment or a fine of N1,000,000.00 or both." Section 58 of the Act[30] defines 'phishing' as "the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through e-mails or instant messaging either in form of an email from what appears from a bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user." The Act also aims to protect consumers who use electronic cards on electronic banking and payment platforms by prohibiting fraudulent activities that target cards used on such platforms. For example, Section 33(1) of the Act[31] criminalises the use of electronic cards (including credit cards, debit cards and other forms of electronic cards) to fraudulently obtain cash, credit, goods, or service.

1.2.6 Computer Related Forgery and Fraud

For preventing computer forgery and fraud, Section 13 of the Act[32] prohibits accessing computer or network and inputting, altering, deleting or suppressing any data to mislead. Such acts attract not less than 3 years imprisonment or a fine of not less than N7million or both. Similarly, the Act[33] prohibits intentional cause of loss of property by altering, inputting, or suppressing a computer data without authority or in excess of authority. This act attracts not less than 3 years imprisonment or a fine not less than N7million or both. In the case of *Cox vs Riley,*[34] the accused was found guilty of criminal damage because he

---

[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Section 14(1), Ibid.
[34] 1986 (83) Cr. App. R. 54.

intentionally erased programme from a plastic circuit card which was used to operate a computerized system.

Section 14(1)[35] further makes any person that fraudulently sends electronic message, which caused damage or loss to the person relying on such message, liable for five years imprisonment or N10 million fine or both. This provision deals with criminals that send SMS to their victims to make them believe that a certain amount of money is sent and credited into the victims' accounts and collect their goods or services.

Furthermore, manipulation of a computer or electronic payment device by a staff in order to short pay or over pay any employee is punishable by seven years imprisonment without an option of fine.[36] Also, fraudulent diversion of emails by bank's staff is punishable by five years' imprisonment or N7 million fine or both.[37] Likewise, if a bank's staff connived with a third party to perpetuate fraud by using electronic means, he shall be liable for imprisonment of not more than seven years and refund the stolen money.[38]

1.3 Duties and Obligations of Banks in Cybercrimes

The Cybercrimes Act does not only prohibit some acts by financial institutions and their employees, but also imposes duties on them to effectively combat fraud and financial malpractices in banking operations in Nigeria. The duties include the following:

1.3.1 Duty to Establish Effective Measures to Prevent Cybercrime

Banks and financial institutions are required to establish effective measures to prevent cybercrime to protect both the banks and their customers. Section 19 of the Act provides that: "Financial institutions must as a duty to their customers put in place effective counter fraud measures to safeguard their sensitive information. Where a security breach occurs the proof of negligence lies on the customer to prove the financial institution in question could have done more to safeguard its information integrity"[39] Indeed, the electronic banking fraud has been causing a huge financial loss to both customers and banks, which results to

[35] Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
[36] Section 14(4), Ibid.
[37] Section 14(4)(a), Ibid.
[38] Section 14(5), Ibid. See also the case of Adeniyi Momodu Allison v. Bow Street Magistrates' Court, Op. cit.
[39] *UBA Plc. vs. Wasiu Bakare,* (2017), Op. cit.

negative impact on the economy and financial mediation. Lem Chin Kok has his to say:

> Cyber related fraud risk is the most significant challenge faced by financial institution in all three regions are in connection with the digital transformation that the world is going through. Financial institutions need a paradigm shift in their approach to mitigate fraud risks going forward. Fundamentally, financial institutions need to understand the digital transformation that is happening rapidly all around us, appreciate the evolving fraud risks arising from this rapid change and design a fraud risk management framework that can mitigate these fraud risks in a sustainable, effective, and efficient manner. I don't think the existing "boxes" or solutions within financial institutions, while costly to maintain, can deal with the evolving fraud risks as they are too fragmented and simplistic. The new generation of fraud risk management should be able to deal with the ever-evolving digital transformation, identify the unknown fraud risks, harness the benefit of technology, and reduce the cost of compliance.[40]

To a large extent under section 19(3) of the Cybercrimes Act, when a security breach occurs, the proof of negligence lies on the customer to prove that the bank or financial institution could have done more to safeguard his information. This requirement appears to defeat the consumer protection objective of Section 19(3) of the Act. This is because the section does not put the bank or financial institution in a position where it will bear greater liability for the breach of consumer data held in its computer system.[41] Rather, the section places consumers in a difficult position to prove that their bank or financial institution is negligent in all situations where their sensitive data was accessed by unauthorized third parties.[42] In addition, the requirement to prove the bank's negligence weakens the implied fiduciary obligation of secrecy and confidentiality that banks and financial institutions owe the consumers to safeguard their information.[43] However, imposing a greater or strict liability

[40] KPMG Global Banking Fraud Survey (2019), p. 8, Op. cit.
[41] *Porter vs Citibank N.A.* 123 Misc. 2d 28, 472 N.Y.S. 2D 582.
[42] *UBA Plc. vs. Wasiu Bakare,* Op cit.
[43] *Public Prosecutor v. Meng* (2006) SGDC 243.

regime on banks and financial institutions under section 19(3) of the Act[44] will make them have a higher degree of liability for the breach of consumer data and encourage them to develop better security measures to prevent cybercrime including fraud. Such a higher liability approach has been adopted as a governing principle under the European Union (EU) Directive on Payment Services in the Internal Market which requires that:

> Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer should be considered to be null and void. Moreover, in specific situations ...it is appropriate that the payment service provider be required to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases.

In line with the EU practice, the decision of the Court of Appeal in the case of *UBA Plc. vs. Wasiu Bakare*[45] could have been an order for retrial of the matter by the lower court had the Appellate Court considered the requirements of "Know Your Customer" (KYC) for bank account operations. This is because, Mr. Wasiu had deposited N140,000.00 into his account with the Appellant on 2nd June, 2008. He then applied for an ATM card and same was issued to him. After two days, he attempted to pay school fees but discovered that the sum was transferred into an account with First Bank on 3rd June, 2008. At the time he was issued the ATM card, he had not activated same by inserting his PIN. He then wrote to the Appellant and CBN for return of his money, but he was advised to liaise First Bank Plc for refund of his money. As a result, he filed an action against the Appellant.

The trail court held that the advent of electronic banking does not detract or discharge banker from its duty to safeguard the customer's funds in its custody. Therefore, the Appellant is liable. Being dissatisfied with the decision, the Appellant filed an appeal at the Court Appeal and the decision of the lower court was subsequently reversed by referring to the CBN Guidelines on Electronic

[44] Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.
[45] (2017) 4 NWLR (Pt. 1555) 318, Op. cit.

Banking in Nigeria, 2003. The Guidelines provides that where there is a case of PIN misuse, the cardholder is liable.

It was already established in that case that the money was transferred to First Bank Plc., and with the application of BVN at the time the judgement was given (2017), the Appellate Court should have ordered for retrial of the matter at the lower court and/or investigation by law enforcement agency. Had it been such order was given, First Bank Plc would have been under obligation to provide full details of the fraudster, otherwise, it will be held liable for incomplete KYC.

1.3.2 Duty of Banks and Financial Institutions to Report Cyber Threats

Banks and financial institutions are required to report cyber threats for the purposes of security of assets. Section 21(1) of the Act imposes obligations on persons or institutions that operate a computer network to report cyber threats to National Computer Emergency Response Team (CERT) Coordination Center. In addition, the CBN's Risk-based Cyber security Framework and Guidelines for Deposit Money Banks and Payment Service Providers impose a similar reporting obligation on banks and electronic payment service providers by requiring them "to report all cyber-incidents whether successful or not immediately, after such incident was identified, to the Director of Banking Supervision of the CBN."[46]

1.3.4 Duty to Verify Customer's Identity before Executing Electronic Banking Transactions

Section 37(1) of the Cybercrimes Act[47] imposes obligation on banks and financial institutions to verify the identity of a customer before issuance of ATM cards, credit cards, debit cards and other related electronic devices. In practice, the identification of a customer by a bank and financial institution in Nigeria includes the acquisition of the customer's personal data and biometric details, and the issuance or confirmation of BVN. This duty is commonly known as "Know Your Customer" principle.

1.3.5 Duty to Reverse Unauthorized Withdrawals

According to the customer-banker's contract, the bank is required to reverse any unauthorized withdrawal within 72 hours of written notification by the customer. Failure to reverse such unauthorized withdrawal within such period renders the bank liable for restitution of the debit and a fine of N5 million.[48] The Act[49]

---

[46] Ibid., p. 117

[47] Cybercrimes (Prohibition, Prevention Etc.) Act, Op. cit.

[48] Section 37(3), Ibid.

[49] Ibid.

requires a bank or financial institution that made an unauthorized debit on a customer's account to provide clear legal authorization for such debit upon a written notification by the customer or reverse such debit within 72 hours.[50]

To some extent, the CBN Consumer Protection Framework attempts to address a card user's liability for unauthorised debits on his or her account arising from negligence. The Framework provides that "financial institutions shall promptly refund customers for actual amounts lost due to fraud with interest at the CBN prescribed rate unless it can be proved that loss occurred as a result of customer's negligence or through fraudulent behavior". The CBN Guidelines on Operations of Electronic Payment Channels in Nigeria (2016) also attempts to address the liability of a card holder for unauthorized account debits which arise from negligence by providing that "the cardholder shall be held liable for fraud committed with his card, arising from the misuse of his PIN or his card".[51]

1.4 Conclusion

i. Many e-banking frauds are committed without the fault of account holders. However, the law requires the account holder to prove that the financial institution has failed to safeguard its information integrity thereby exposing the information of its customers. This position of the law contradicts the provision of section 19(3) of the Act, which states that "Financial institutions must, as a duty to their customers, put in place effective counter-fraud measures to safeguard their sensitive information." Therefore, the duty on customer to prove negligence of financial institution that it has failed to safeguard its information integrity is not on the balance of probability.

ii. Some of the punishment provisions in the cybercrimes act are to the extreme. Although the punishment for offences is to deter the commission of the prohibited acts, but the prescription of penalty for contravention of some provisions of the Act is not in line with the legal maxim that says: *"Summum Jus, Summum Injuria, Summum Lex, Summum Crux"* which connotes that: "Extreme Law is Extreme Injury. Strict law is strict punishment." An example of this is the provision of Section 17(1)(c) of the Act[52] which provides that:

---

[50] *UBA Plc vs Wasiu Bakare*, Op. cit.
[51] *UBA Plc vs Uzochukwu* (2017) LPELR-CA/E/339/2007.
[52] Ibid.

> Any person who, with the intent to defraud and or misrepresent, forges through electronic devices another person's signature or company mandate, commits an offence and shall be liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than N10,000,000.00 or to both fine and imprisonment.

Likewise, Section 14(1)[53] that deals with forgery of electronic signature or mandate with 5 years imprisonment or N10,000,000.00 fine or both is not in compliance with that legal maxim on punishment prescription. Based on the above the following recommendations are hereby made

i. The Act should put burden on the financial institutions to provide evidence of alleged negligence from part of the customer since the payer's means to do so are very limited in such cases at it applies in E.U. countries. The proof of negligence should not be the burden of the customer, but rather the bank to prove that it puts effective counter-fraud measures to safeguard its information integrity and the customer was negligent in protecting his account sensitive information which led unauthorized withdrawal from the account of customer.

ii. Sections 14(1), 17(1)(c), and 19(2) should be amended to harmonise the fine and imprisonment in order to align with the legal maxim.[54] This is recommended because the sanctions prescribed against offences under Banks and Other Financial Institutions Act, 2020 do not exceed N5 million fine or 5 years imprisonment.[55]

---

[53] Ibid.
[54] *Summum Jus, Summum Injuria, Summum Lex, Summum Crux.*
[55]