EDU REKHA INTERNATIONAL JOURNAL OF ARTS, LAW AND SOCIAL SCIENCE

Journal Homepage: https://edurekhapublisher.com/erijalss/

Volume- 2 Issue – 6 (November - December) 2026

ISSN: 3107-5169 (Online)

Frequency: Bimonthly

PAGES: 19-24

ARTICLE TITLE:



E-BANKING, CYBERTHREATS AND DIGITAL FRAUD IN THE NIGERIAN FINANCIAL SECTOR: A LEGAL APPRAISAL OF REGULATORY FRAMEWORKS, INSTITUTIONAL ENFORCEMENT AND REFORM IMPERATIVES

DR. EJIKE FRANCIS OKAPHOR[1*], MARYJANE OLUEBUBE EJEBUGHAOBI[2] & NKIRUKA EDITH OKAPHOR[3]

[1]Head of Department, Commercial and Industrial Law Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.

[2,3]Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.

ARTICLE HISTORY

RECEIVED
26-10-2026

ACCEPTED
05-11-2026

PUBLISHED
11-11-2026

Corresponding author:

DR. EJIKE FRANCIS OKAPHOR

Head of Department, Commercial and Industrial Law Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.

Abstract

The electronic banking sector in Nigeria has been beset by cyber threats and digital frauds since its inception, with losses escalating from ₦2.9 billion in 2019 to ₦17.67 billion in 2023 alone. This article undertakes a doctrinal legal appraisal of the legislative and institutional framework designed to govern e-banking security, prevent digital fraud, and provide remedies to victims in the Nigerian finance sector. Drawing on the Deterrence Theory, Routine Activity Theory, and the Fraud Triangle Theory as its theoretical framework, the article examines the adequacy of the principal legislative instruments, including the Cybercrime (Prohibition, Prevention, Etc.) Act 2015 as amended, the Banks and Other Financial Institutions Act 2020, and the Nigeria Data Protection Act 2023 alongside the institutional roles of the Central Bank of Nigeria, the Economic and Financial Crimes Commission, and allied regulatory bodies. The article finds that while Nigeria has constructed a multi-layered regulatory architecture, a systemic enforcement deficit produced by legislative fragmentation, weak institutional coordination, low prosecution rates, and inadequate technical infrastructure leaves e-banking customers structurally exposed to harm. Comparative analysis with the United Kingdom and South Africa identifies concrete legislative models capable of addressing this deficit. The article concludes with targeted recommendations for legislative reform, institutional coordination, and capacity building.

Keywords: E-banking, Cyber threats, Digital Fraud, Regulatory Frameworks, Institutional Enforcement, Reform Imperatives

1. INTRODUCTION

In Nigeria, the financial sector has undergone a profound transition over the past two decades. The progressive migration from paper-based, cash-oriented transactions to electronic banking platforms has integrated millions of previously unbanked Nigerians into the formal financial system. Electronic payment channels, USSD codes, Point of Sale terminals, mobile banking applications, Automated Teller Machines, and internet banking portals which make up the electronic banking system now collectively process billions of naira daily, forming the technological backbone of what the Central Bank of Nigeria (CBN) has deliberately cultivated as a cashless economy[1]. In fact, electronic banking is the order of banking in today's world, a world away from the traditional and over the counter banking which existed within the early 2000's.

This digital revolution has, however, carried within it the seeds of a profound security crisis. The same accessibility that makes e-banking commercially indispensable simultaneously creates an attack surface of extraordinary breadth for cybercriminals. Within the period 2019 to 2023, fraud in the finance sector increased by 112 per cent, with losses in the digital banking system rising from ₦2.9 billion to ₦17.67 billion.[2] According to the Nigerian Deposit Insurance Corporation (NDIC), fraud-associated losses jumped by 39.4 per cent between 2021 and 2025, with electronic channels accounting for 88.7 per cent of fraud cases and 69 per cent of losses in 2021 alone.[2]

According to the Nigerian Deposit Insurance Corporation, fraud associated losses jumped within the years of 2021 to 2025 by a 39.4% increase, owing majorly to digital exploitation.[3]The legal response to this crisis has been real but fragmented and, in critical respects, inadequate. The Cybercrime (Prohibition, Prevention, Etc.) Act 2015, amended in 2024, stands as the primary legislative instrument for the criminal prosecution of digital financial crime. The CBN has issued a number of successive cybersecurity frameworks. The Nigeria Data Protection Act 2023 introduced data protection obligations with direct bearing on e-banking security. Yet despite this proliferation of instruments, prosecution rates for sophisticated e-banking cybercrime remain critically low, civil remedies are practically inaccessible for most fraud victims, and regulatory jurisdiction is fragmented across competing agencies without effective coordination.

2. The Nature of E-Banking, Cyber Threats and Digital Fraud

2.1 Electronic Banking:

This refers to services provided by banks using Information and Communication technologies. Overtime, Electronic Banking has evolved to manifest in different ways which include the computer-based systems to perform transactions electronically. In fact, it is a system allowing banks to pay money from one bank to another, pay bills and transfer funds using recognized electronic channels.[4]

2.2 Cyberthreats and Digital Fraud:

In Nigeria, these encompass a sophisticated and continuously evolving range of methodologies. Phishing and social engineering, including vishing, smishing, and SIM-swap fraud remain the primary enabling mechanism for mobile channel fraud, prosecutable under section 27 of the Cybercrime Act. Account takeover, frequently enabled by SIM-swap, was responsible for 28 per cent of total fraud value in 2023, making it the most financially damaging single fraud category. Identity theft is addressed under the Cybercrime Act, [5] which specifically targets insider-facilitated identity theft within financial institutions. Card theft and ATM skimming, as well as malware and ransomware attacks targeting banking infrastructure represent a qualitatively different threat category: they target institutional systems, potentially compromising thousands of customers simultaneously, and are addressed through the CBN's Cybersecurity Frameworks rather than through specific criminal provisions. Business Email Compromise (BEC) identified by INTERPOL as one of the highest-value fraud threats in the West African sub-region is prosecutable under the provisions of the Cybercrime Act, though the investigation of BEC demands levels of digital forensic capability and international cooperation that currently exceed the EFCC's institutional capacity.

3. AN APPRAISAL OF THE LEGAL FRAMEWORK GOVERNING E-BANKING AND CYBERSECURITY IN NIGERIA

In the Nigerian legal context, several authors have advanced literature on the advancement of electronic banking, while others have attempted to draw a delineation between the cyber threats and digital frauds which have plagued the Nigerian financial sector in recent times. Ishiguzo, in his work, specifically undergoes a journey into the prospect of cybercrime investigation and prosecution, especially with regard to the financial losses it has wrought in the electronic banking sector and Nigeria's financial system as a whole.[6] In his work. He delineates the challenges encountered by the law enforcement agencies in combating cyber threats and digital fraud in Nigeria so far, with a focus on the roles these security and intelligence personnels play in combating cyber threats. In his appraisal, he explains the legal and institutional framework which are charged or have been charged with regulating the financial sector as well as cyber threats in the electronic banking space.

---

[1] Central Bank of Nigeria, Payments System Vision 2025 (CBN 2022); CBN, Guidelines on Operations of Electronic Payment Channels in Nigeria (CBN 2020).

[2] Nigerian Deposit Insurance Corporation, Annual Report and Statement of Accounts 2022 (NDIC 2023).

[3] C Akujobi, F Ogwueleka, G Aimufua and S. Bassey 'Cyber Fraud in Nigerian Banks: Trends, Regulatory Gaps, and Mitigation Strategies' [2026] (11) (01) *Everant Journal* <Cyber Fraud in Nigerian Banks: Trends, Regulatory Gaps, and Mitigation Strategies (2020–2025) | Engineering And Technology Journal> accessed 10th May, 2026

[4] AO Agbada, 'Electronic banking in Nigeria: Problems and Prospects from the Customer's Perspective' *CBN Bullion* (2008) 32(1) 19-22.

[5] Section 22 of the Cybercrime (Prosecution, Prohibition etc) Act, 2015

[6] RO Ishiguzo, 'Prospects of Cybercrime Investigation and Prosecution in Nigeria and the Role of Security and Intelligence agencies in curbing Cybercrime' *International Review of Law and Jurisprudence.*[2024] 6(2) <https://www.nigerianjournalsonline.com/index.php/IRLJ/article/view/5444> accessed 30th May, 2026.

Nwocha, Iteshi and Awada[7], in their 2024 review of the Cybercrimes Act instead, focus on the role the Cybercrimes Act plays in regulating cyber threats and digital frauds as a whole in the Nigerian sector. On the foundation built by some of these existent literatures, we will delve into the extant legal and institutional frameworks regulating these in Nigeria.

3.1.1 The Constitution of the Federal Republic of Nigeria 1999 (As Amended)

The Constitution of the Federal Republic of Nigeria 1999 is the Grund norm of the Nigerian legal order, and its provisions establish the foundational legal basis upon which every instrument governing e-banking and cybersecurity rests, By the combined application of Sections 1(1) and 1(3), the CFRN provides that that any laws inconsistent with the provisions of this Grund norm is void to the extent of its inconsistency. [8] Section 16(1)(b), though a non-justiciable part of the constitution, directs the State to control the national economy in a manner that secures the maximum welfare of every citizen, providing the constitutional basis for the State's regulatory obligation over the financial sector. [9] Section 37 guarantees the fundamental right to privacy of correspondence, telephone conversations, and telegraphic communications, a provision that extends, in the digital age, to the privacy of electronic financial data and banking credentials. The Second Schedule places banking and the allocation of revenue on the Exclusive Legislative List, ensuring nationally uniform regulation and excluding state legislatures from enacting competing banking security regimes.

3.1.2 The Cybercrime Act 2015 and the Cybercrimes (Prohibition, Prosecution) Amendment Act,2024.

The Cybercrime (Prohibition, Prevention, Etc.) Act 2015, amended in 2024, is Nigeria's most significant and comprehensive legislative response to digital financial crime. Section 14 targets computer-related fraud in the financial sector, imposing upon conviction a fine of not less than ₦10 million and imprisonment of not less than five years, or both. Section 22 specifically addresses insider identity theft within financial institutions, prescribing seven years' imprisonment, a fine of ₦5 million, or both. Part III broadly addresses cyber threats and digital fraud across sectors, while Part IV imposes duties on financial institutions and service providers to frustrate cybercrime.

Despite these provisions and the 2024 amendment, significant legislative gaps persist. The Act does not expressly criminalize SIM-swap fraud as a distinct offence, does not address AI-assisted social engineering or deepfake-enabled identity fraud, which is currently on the rise, and does not impose specific civil liability obligations on financial institutions whose inadequate security enables customer losses. The legislative pluralism that characterizes Nigeria's cybercrime legal landscape, with relevant provisions scattered across the Criminal Code Act, the Advance Fee Fraud Act, the EFCC Act, and the Money Laundering Act, further compounds the problem.

3.1.3 The CBN Act 2007 and CBN Regulatory Guidelines

The Central Bank of Nigeria Act 2007 establishes the CBN as the apex financial regulatory authority, with powers under section 51 to make regulations and issue guidelines covering all aspects of banking operations. Through this authority, the CBN has issued the foundational regulatory architecture for e-banking security: the Guidelines on Electronic Banking in Nigeria (2003); the Guidelines on Operations of Electronic Payment Channels (2020), which mandate two-factor authentication for internet banking transactions; the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks (2024), which mandates risk assessments, incident reporting, and the appointment of a Chief Information Security Officer; and the Consumer Protection Regulations (2019), which require banks to resolve customer fraud complaints within prescribed timeframes.

A structural tension pervades the CBN's regulatory function. Its dual mandateto promote financial inclusion and digital banking expansion on one hand, and to maintain the security and stability of the financial system on the other has not always produced consistent outcomes.

3.1.4 The Banks and Other Financial Institutions Act 2020

BOFIA 2020[10] represents a landmark modernization of Nigeria's primary banking statute. Section 59[11] prescribes fines of up to ₦50 million for violations of the Act or license conditions. Significantly, theAct's extended definition of financial institutions encompasses entities conducting financial business electronically, virtually, or digitally, bringing fintech operators and digital-only financial service providers within the full ambit of CBN supervision. Section 66 mandates all banks to implement policies preventing transactions that could facilitate criminal activities, providing an indirect but important cybersecurity obligation applicable to all e-banking platforms.

3.1.5 The Nigeria Data Protection Act 2023

The NDPA 2023 introduces a transformative data protection dimension to the legal framework for e-banking fraud. The Act imposes on all data controllers and processors, including financial institutions, obligations of integrity and confidentiality under section 24, requiring appropriate technical and organizational security measures against unauthorized access, loss, or destruction.[6] Section 29 specifically requires financial institutions to implement security measures and conduct data privacy impact assessments. A financial institution whose inadequate cybersecurity measures enable a data breach facilitating identity theft or account takeover may face administrative fines of up to 2 per cent of annual gross revenue or ₦10 million, whichever is greater. Section 48 further provides that data subjects whose personal data has been unlawfully processed may seek compensation from the Nigeria Data Protection Commission (NDPC) or institute civil proceedings in a court of competent jurisdiction.

3.1.6 The Evidence Act 2011 and Evidence (Amendment) Act 2023

The Evidence Act 2011, as amended, governs the admissibility of electronic evidence in Nigerian proceedings. Section 84(1) provides for the admissibility of computer-generated documents, subject to conditions in section 84(2) that the computer system was operating properly and that the document accurately reproduces the relevant information.

---

[7] M Nwocha and C Iteshi and P Awada, 'An overview of the Nigerian Cybercrime Act 2015, As Amended' *African Journal of law and Human Rights*. (AJLHR)[2025] 9(2). <https://journals.ezenwaohaetorc.org/index.php/AJLHR/article/viewFile/3419/3549 accessed 19 May 2026.

[8] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 1(3).

[9] Part II of the CFRN (As Amended), 1999.

[10] Banks and Other Financial institutions Act, 2020

[11] *Ibid,* Section 59

3.1.7 The Economic and Financial Crimes Commission (EFCC) Act 2004

The Economic and Financial Crimes Commission (Establishment) Act 2004 established the EFCC with a mandate under section 6 that expressly encompasses all forms of financial fraud perpetrated through electronic means. The Act empowers the EFCC to investigate, arrest, and prosecute any person suspected of committing any offence under the Act or any other law relating to economic and financial crimes, a provision wide enough to encompass the full range of Cybercrime Act offences relevant to e-banking fraud.

3.1.8 Federal Competition and Consumer Protection Act (FCCPA)

Bankers are largely consumers of the services of electronic banking, and thus, fall under the jurisdiction of the FCCPA by virtue of Section 2 of the Act. In this regard, by virtue of the provisions of Section 104 of the FCCPA which says; 'Notwithstanding the provisions of any other law but subject to the provisions of the Constitution of the Federal Republic of Nigeria, in all matters relating to competition and consumer protection, the provisions of this Act shall override the provisions of any other law', it is evident that the Act has jurisdiction over any customer complaint, even overriding any other law though subject to the constitution.

3.1.9 International and Regional Frameworks

Nigeria's domestic framework is supplemented by international and sub-regional instruments of varying legal effect. Nigeria ratified the Budapest Convention on Cybercrime on 6 July 2022, creating a binding international obligation to criminalize the offences defined in the Convention and to cooperate in cross-border cybercrime investigations. The Convention's ratification without full domestication through National Assembly legislation means, however, that its provisions have not yet achieved direct domestic legal force under section 12(1) of the 1999 Constitution.

The ECOWAS framework constitutes a complementary sub-regional architecture: the Supplementary Act on Personal Data Protection (2010) and the Supplementary Act on Electronic Transactions (2010) and the Directive on Fighting Cybercrime (2011) required all member states to implement cybercrime legislation by January 2014. Nigeria's Cybercrime Act 2015, enacted a year after that deadline, represents partial compliance. The ECOWAS Regional Cybersecurity and Cybercrime Strategy (2021) further establishes the sub-regional normative benchmark against which Nigeria's national cybersecurity framework must be measured.

3.2 THE INSTITUTIONAL FRAMEWORK

The governance of e-banking security in Nigeria is distributed across some principal institutional actors, each with a distinct but overlapping mandate. The absence of a statutory coordination mechanism among these actors is one of the most consequential structural weaknesses of the existing framework.

The CBN is the most significant institutional actor, with regulatory authority over all licensed financial institutions and the power to issue and enforce the guidelines that constitute the operational substance of e-banking security law. Through the Nigeria Electronic Fraud Forum (NeFF), established in 2011, the CBN coordinates responses to e-banking fraud across financial institutions and law enforcement. In January 2026, officials at the NeFF Forum reported a significant decline in electronic payment fraud losses for 2025, evidence that CBN regulatory action and NIBSS data intelligence can produce measurable results when coordination functions effectively.[8]

The NIBSS manages the central payment infrastructure, operates the NIBSS Instant Payment (NIP) platform, and administers the Bank Verification Number (BVN) database. It publishes the definitive annual Industry Fraud Landscape, the most authoritative empirical source on the scale and nature of e-banking fraud in Nigeria. The 2023 report documented ₦17.67 billion in fraud losses across 95,620 incidents, a fraud reporting compliance rate of only 37 per cent among profiled institutions, and the mobile channel as the highest-volume fraud vector.[9]

The NCC regulates the telecommunications infrastructure upon which e-banking authentication systems depend. The structural dependence of OTP-based authentication on mobile networks makes SIM-swap fraud an inherently bi-jurisdictional problem requiring coordinated response from both the CBN and the NCC, coordination that has historically been inadequate. The NDIC conducts annual supervisory examinations of financial institutions in conjunction with the CBN, serving as an important early detection mechanism for systemic fraud patterns. The NDPC, established by the NDPA 2023, investigates data breaches, receives complaints from data subjects, and imposes administrative sanctions, providing a novel enforcement pathway for fraud victims whose losses result from a bank's failure to protect personal data. The EFCC serves as the principal prosecuting authority under the Cybercrime Act 2015.

4. LEGAL REMEDIES AVAILABLE TO VICTIMS OF CYBERTHREATS AND DIGITAL FRAUDS.

4.1 Civil Remedies

These rest primarily on the fiduciary duty of care that Nigerian courts have consistently held banks to owe their customers. Section 19(3) of the Cybercrime Act imposes on financial institutions an express duty to put in place effective counter-fraud measures to safeguard sensitive customer information, though the provision locates the burden of proving negligence on the customer, a placement that significantly undermines the practical utility of this provision for fraud victims.

The bank's duty of confidentiality, affirmed by the House of Lords in *Tournier v National Provincial and Union Bank of England*[12] and consistently applied in Nigerian banking law, creates an additional basis for civil liability where a breach of customer data confidentiality enables e-banking fraud. The NDPA 2023's section 48 supplements these common law remedies with a statutory right to compensation through the NDPC or civil proceedings. Despite these rights, the practical remedy is, for the majority of fraud victims, inaccessible: civil litigation in Nigeria is protracted, expensive, and technically demanding.

[12] Tournier v National Provincial and Union Bank of England [1924] 1 KB 461

The recently decided *Stanford International Bank Ltd v HSBC Bank Plc*[13] illustrates how the duty of care and the *Quincecare* duty[14] can be invoked against banks that execute payment instructions without heeding obvious fraud indicators, and provides a model for how Nigerian courts might develop a more proactive bank liability doctrine. This was also addressed in the Nigerian landmark case of *Kuda Microfinance Bank Ltd v. Amarachi*. [15] Still, structural challenges remain.

4.2 Criminal Prosecution:

Prior to 2015, Cybercrime in its entirety, including cyber threats and digital fraud were governed by limited legislation. However, with the amendment of the act in 2024, by the President Bola Ahmed Tinubu in February, 2024, a number of new, yet important additions quite necessary to the growth of cyber threats in the Nigerian financial ecosystem were added.

The Cybercrime (Prohibition, Prevention, Etc.) As amended Act of 2024 remains the cornerstone of Nigeria's criminal law response to e-banking fraud. The entirety of the Act creates the offences of computer-related fraud in the financial sector, imposing upon conviction fines of different amounts in naira with provision for imprisonment where necessary, or both among the most severe penalties in the Act, reflecting the legislature's recognition of the particular gravity of financial cybercrime.

5. STRUCTURAL CHALLENGES INHERENT IN COMBATING CYBER THREATS AND DIGITAL FRAUDS IN ELECTRONIC BANKING AND THE NIGERIAN FINANCIAL SECTOR

1. **Legislative fragmentation and loopholes.** The Cybercrime Act, even as amended, does not address SIM-swap fraud, AI-assisted social engineering, or deepfake-enabled fraud as distinct offences. Legislative pluralism across multiple statutes, each prescribing different penalties for overlapping conduct undermines coherence and deterrence. The absence of a specific statutory civil liability regime for unauthorized electronic transactions means that fraud victims bear the burden of proving bank negligence under common law principles that are ill-adapted to the digital banking environment.
2. **Enforcement weakness.** The EFCC lacks the forensic digital infrastructure, specialist investigators, and cyber intelligence capacity to effectively prosecute sophisticated e-banking cybercrime. The NIBSS's 37 per cent fraud data reporting compliance rate in 2023 fundamentally compromises the evidential foundation for investigation. In fact, cyber threats and digital frauds are still prosecuted largely across a variety of laws.
3. **Challenges in Evidence Gathering:** The strict conditions of section 84(2) of the Evidence Act for the admissibility of computer-generated evidence impose demands that prosecutors frequently cannot meet. As the Deterrence Theory predicts, this evidentiary obstacle produces a prosecution deficit that emboldens rational criminal actors.
4. **Transnational challenges.** The most financially significant forms of e-banking fraud are orchestrated by transnational networks. Nigeria's ratification of the Budapest Convention on 6 July 2022 provides an important framework, but full domestication through National Assembly legislation is necessary before its mutual assistance provisions can be directly invoked.
5. **Inadequate technical infrastructure.** Significant disparities persist between the cybersecurity infrastructure of large tier-one banks and that of smaller banks and fintech operators, many of which operate on legacy systems with weak authentication controls and limited real-time fraud monitoring.[16]

6. COMPARATIVE LESSONS FROM OTHER JURISDICTIONS

The **United Kingdom** has addressed the most critical weakness in Nigeria's civil liability framework; the customer's burden of proving bank negligence through Regulation 77 of the Payment Services Regulations 2017. Where a customer denies authorizing a payment transaction, the payment service provider bears the immediate burden of proving that the transaction was authorized or that the customer acted fraudulently or with gross negligence. This reversal of the evidential burden is the single most transformative consumer protection reform a legislature can make in the e-banking fraud context. The ***Quincecare*** duty, most recently applied at Supreme Court level in **Stanford International Bank Ltd v HSBC Bank Plc** *16* imposes on banks a proactive duty not to execute payment instructions when they have reasonable grounds to suspect fraud, creating an affirmative obligation of fraud vigilance that goes significantly beyond the passive duty of care recognized in Nigerian banking law.

South Africa's Electronic Communications and Transactions Act 2002 codifies minimum authentication standards for electronic transactions as primary legislation, establishing clear statutory liability for losses arising from inadequate authentication systems. This primary legislative approach, as opposed to Nigeria's reliance on subsidiary CBN guidelines for authentication standards, provides greater legal certainty for financial institutions and their customers. The International Monetary Fund's 2022 Financial Sector Assessment Program for South Africa confirmed the effectiveness of this legislative model in producing consistent cybersecurity standards across the financial sector.

7. CONCLUSION AND RECOMMENDATIONS

This article has undertaken a comprehensive doctrinal appraisal of the legal framework governing e-banking, cyber threats, and digital fraud in the Nigerian finance sector. Nigeria has constructed a legislative and institutional architecture that is, in its broad design,

[13] Stanford International Bank Ltd v HSBC Bank PLC [2022] UKSC 34

[14] Barclays bank v Quincecare Ltd. (1992) 4All ER 363.

[15] *Kuda Microfinance Bank Ltd v. Amarachi Kenneth Blessing*, CA/EK/48/2024

[16] Stanford International Bank Ltd v HSBC Bank PLC [2022] UKSC 34

comprehensive: the Cybercrime Act criminalizes the principal modalities of digital financial fraud; BOFIA subjects all financial institutions including digital-only entities to CBN supervision; the NDPA 2023 imposes data security obligations with significant financial penalties; and the institutional actors command a formidable array of regulatory and enforcement powers. These are genuine achievements.

The framework fails however, largely due to the inherent challenges existing as listed above. In this author's opinion, it is believed that the problem lies not on the fact that legislations do not exist. In fact, enough legislations exist. However, enforcement of the existing legislations where these problems arise. In addition to this, the gap existent in unifying laws to reach international best practices and enable transnational collaboration remains.

The following recommendations are directed at the National Assembly, the CBN, the EFCC, and the Federal Executive.

First, the CBN should mandate full implementation of its Cybersecurity Frameworks across all regulated institutions with non-extendable deadlines, conduct independent annual cybersecurity audits with published results, mandate full and timely fraud incident reporting to the NIBSS with automatic sanctions for non-compliance, and establish a presumption of institutional liability for fraudulent transactions conducted through channels that do not meet prescribed minimum-security standards.

Second, the National Assembly should impose a statutory obligation on all licensed financial institutions to provide mandatory, standardized cybersecurity literacy training to all customers at account opening, and the CBN's National Financial Inclusion Strategy should incorporate digital financial safety literacy as a prerequisite of all financial inclusion initiatives.

Third, the Federal Government should establish, by statute, a **Financial Cybersecurity Council**, a permanent inter-agency body chaired by the CBN Governor and comprising the heads of the EFCC, the NDPC, the NCC, the NIBSS, and the ONSA with a specific mandate to develop a joint CBN-NCC protocol for SIM-swap fraud prevention.

Fourth, partnership between the FCPC and the NCC should be tightened to avoid gaps and lapses in prosecution. The NCC being the body in charge of communications and regulating major communication networks such as MTN, Airtel amongst others, will be a good partner to the FCPC in investigating incidences of cyber threats and digital frauds for individuals as customers.

Fifth, transnational collaboration should be encouraged and tightened. By doing this through the partnerships between the EFCC, INTERPOL, and other international cyber police bodies, the threats which cyber fraudsters pose to electronic banking customers and the world at large can be curbed, especially since it is widely agreed that these activities are not only domestic but transnational. In addition to these, proper domestication should be made to the international treaties and conventions curbing cyber threats to in line with the provisions of the CFRN, 1999. [17]

The ₦17.67 billion lost to e-banking fraud in 2023 was not an act of God. It was, in large part, a failure of law. It does not have to happen again.

[17]Section 12, CFRN,1999.