THE ROLE OF EFCC AND RELATED INSTITUTIONS IN THE PROSECUTION OF CYBERCRIMES IN NIGERIA*

Abstract

This article found cybercrime to have emerged as one of the most potent threats to Nigerian contemporary governance, economic stability, national security, and the protection of fundamental rights in this digital age. Nigeria, like many rapidly digitising states, was found to have responded by enacting specialised legislations and established multiple enforcement and regulatory institutions. This article found that these developments notwithstanding, persistent concerns remain regarding the effectiveness, coordination, constitutional compliance, and practical enforcement of the country's cybercrime legal framework. This study therefore examined the legal and institutional frameworks for combating cybercrimes in Nigeria, assessing their scope, operational performance, structural challenges, rights implications, and reform prospects. To addressed the missing gap found, the study, inter alia, addressed the following issues: to what extent does the existing Nigerian legal framework effectively address the different forms of cybercrimes in Nigeria? How do the policy gaps and enforcement challenges undermine the fight against cybercrimes in Nigeria? Against the backdrop of the research questions, the aim and objectives of the study were achieved by examining the provisions and enforcement framework of Nigeria's Cybercrimes Act 2015 and related laws. The doctrinal methodology was adopted in this article thus statutes, case law, juristic and non-juristic works contained textbooks, journals, internet, etcetera to achieve the aim and objectives of this article. The article found, inter alia, that Nigeria possesses a substantially developed but operationally constrained cybercrime governance system. The study recommended legal and policy reforms for a comprehensive cybercrime regime in Nigeria among other recommendations.

Keywords: EFCC, Cybercrime, Prosecution, Nigeria

1. Introduction

The rapid growth of digital technologies and internet usage has significantly transformed communication, commerce, and governance in Nigeria. However, this advancement has also led to a rise in cybercrimes such as online fraud, identity theft, hacking, and other internet-related offences. In response, the Nigerian government has strengthened institutional and legal frameworks to combat these crimes. Prominent among these institutions is the Economic and Financial Crimes Commission (EFCC), which plays a central role in investigating and prosecuting cybercrime-related offences. Other key institutions, including the Nigeria Police Force, the Independent Corrupt Practices and Other Related Offences Commission (ICPC), and the National Information Technology Development Agency (NITDA), also contribute to enforcement, regulation, and prevention efforts. Through investigation, intelligence gathering, inter-agency collaboration, and prosecution, these institutions work collectively to address the growing threat of cybercrime and to safeguard Nigeria's digital and financial systems.

2. Economic and Financial Crimes Commission (EFCC)[1]

The Economic and Financial Crimes Commission (EFCC) remains the central institutional mechanism for combating economic and financial crimes, including cybercrime, in Nigeria. It derives its legal existence and powers from the Economic and Financial Crimes Commission (Establishment) Act, 2004, which serves as its enabling statute. Section 1(1) of the Act provides that: There is established a body to be known as the Economic and Financial Crimes Commission (in this Act referred to as 'the Commission') which shall be a body corporate with perpetual succession and a common seal and may

[*]**By Lawrence Monwo ALABI, LLB, BL, LLM, PhD Candidate**, Faculty of Law, Nasarawa State University, Keffi;

[*]**David Andrew AGBU, LLB, BL, LLM, MILR, PhD,** Professor of Law, Faculty of Law, Nasarawa State University Keffi, Email: davidmaisongo2@gmail.com; and

[*]**Samuel Tolu Olumide ADESINA, LLB, BL, LLM, PhD Candidate**, Faculty of Law, Bingham University, Karu.

[1] Economic and Financial Crimes Commission.

sue and be sued in its corporate name.[2] The Commission is vested with comprehensive functions under Section 6 of the Act, which stipulates that: The Commission shall be responsible for the enforcement of all economic and financial crimes laws and the coordination of the enforcement of the provisions of any other law or regulation relating to economic and financial crimes.[3] This provision gives the EFCC a broad mandate not only to investigate and prosecute, but also to coordinate enforcement activities across other anti-graft and law enforcement agencies, including the ICPC, the Nigerian Police, and the Nigerian Financial Intelligence Unit (NFIU). Section 7(1)(a) of the Act explicitly empowers the EFCC: 'to cause investigations to be conducted as to whether any person, corporate body or organization has committed an offence under this Act or any other law relating to economic and financial crimes'.[4] This is further reinforced by Section 13(2), which provides that:

The Legal and Prosecution Unit shall be charged with responsibility for prosecuting offenders under this Act and shall perform such other legal duties as the Commission may refer to it.[5] By these provisions, the EFCC wields both investigative and prosecutorial competence, making it one of the few agencies in Nigeria that combines the two functions under one statutory framework. However, these powers remain subject to the constitutional authority of the Attorney-General of the Federation (AGF) under Section 174 of the Constitution, which empowers the AGF to 'institute and undertake criminal proceedings against any person before any court of law in Nigeria, other than a court-martial.'[6] This constitutional relationship implies that although the EFCC possesses statutory prosecutorial powers, such authority operates by delegation of the AGF. The Supreme Court in *FRN v. Osahon*[7] clarified that statutory bodies like the EFCC can prosecute offences created by their establishing statutes without prior written fiat from the Attorney-General, provided such statutes expressly empower them to do so. This interpretation strengthens the Commission's capacity to prosecute cybercrime-related offences efficiently without excessive bureaucratic delays.

The relevance of the EFCC in the prosecution of cybercrime is grounded in the fact that most cyber offences involve elements of financial fraud and economic manipulation. Cybercrimes such as identity theft, online banking fraud, phishing, and unauthorized fund transfers directly implicate Nigeria's financial systems. Hence, the Commission's jurisdiction under Section 6(b) of the EFCC Act naturally extends to the enforcement of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, particularly offences with financial dimensions. In fulfilling this role, the EFCC established a Cybercrime Unit within its Legal and Prosecution Department. The unit focuses on digital forensics, data recovery, and prosecution of offenders engaged in computer-related fraud. One of its major initiatives, 'Operation Eagle Claw', launched in partnership with Microsoft and Interpol, has been instrumental in identifying and dismantling online fraud networks across Nigeria.[8]

However, despite these successes, the Commission faces significant institutional and legal lacunae. First, the EFCC Act does not specifically mention *cybercrime*, leaving interpretive gaps that must be filled by judicial and administrative practice. Second, there exists overlapping jurisdiction between the EFCC, the Police, and the ICPC, particularly concerning offences that have both corruption and cyber elements. This overlap has led to inter-agency rivalry, duplication of effort, and occasional legal conflict, as seen in *Attorney-General of Benue State v. Attorney-General of the Federation*,[9] where the multiplicity of federal investigative agencies was challenged as unconstitutional. Third, the EFCC's dual role as investigator and prosecutor raises questions of due process and accountability. Concentrating such powers in a single agency, without sufficient judicial oversight, risks selective

[2] Economic and Financial Crimes Commission (Establishment) Act, Cap E1, Laws of the Federation of Nigeria 2004, s 1(1).
[3] EFCC (Establishment) Act 2004, s 6(b).
[4] EFCC (Establishment) Act 2004, s 7(1)(a).
[5] EFCC (Establishment) Act 2004, s 13(2).
[6] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 174(1).
[7] *Federal Republic of Nigeria v Osahon* (2006) 5 NWLR (Pt 973) 361 (SC).
[8] Economic and Financial Crimes Commission, *Annual Report 2019: Anti-Cybercrime Operations and Global Partnerships* (EFCC Publications 2020).
[9] *Attorney-General of Benue State v Attorney-General of the Federation* (2006) 12 NWLR (Pt 940) 1 (SC).

prosecution or abuse of discretion, particularly in politically sensitive cases. Critics argue that this structure may violate the principle of separation of powers, which requires that investigation and prosecution remain distinct to avoid conflict of interest. From a comparative standpoint, Nigeria's EFCC model differs from those of other jurisdictions. In the United States, for example, the Federal Bureau of Investigation (FBI) handles investigations, while prosecution is conducted exclusively by the Department of Justice (DOJ). Similarly, in the United Kingdom, the Serious Fraud Office (SFO) operates under a clear statutory division where investigative and prosecutorial powers are regulated by the Crown Prosecution Service (CPS), ensuring transparency and accountability.

Nigeria's fusion of investigative and prosecutorial powers within the EFCC has yielded faster convictions but poses systemic risks. To address this, legal scholars advocate amending the EFCC Act to clarify the extent of prosecutorial autonomy and to establish a supervisory prosecutorial council under the Attorney-General's office to ensure uniform standards and oversight.[10] While the EFCC remains indispensable in the fight against economic and cyber-related crimes, the current framework exhibits structural and procedural deficiencies. A constitutional and statutory re-alignment is necessary to ensure a clear demarcation of roles, greater accountability, and compliance with global best practices in prosecutorial governance.

3. The Cybercrime Advisory Council

The Act establishes, a Cybercrime Advisory Council otherwise referred to as 'the Council' which comprises of a representative each, of the following Ministries and Agencies;[11]

Ministries, Departments and Agencies-

(a) Federal Ministry of Justice;
(b) Federal Ministry of Finance;
(c) Ministry of Foreign Affair;
(d) Federal Ministry of Trade and Investment;
(e) Central Bank of Nigeria;
(f) Office of the National Security Adviser;
(g) Department of State Services;
(h) Nigeria Police Force;
(i) Economic and Financial Crimes Commission;
(j) Independent Corrupt Practices Commission;
(k) National Intelligence Agency;
(l) Nigerian Security and Civil Defence Corps;
(m) Defence Intelligence Agency;
(n) Defence Headquarters;
(o) National Agency for the Prohibition of Traffic in Person;
(p) Nigeria Customs Service;
(q) Nigeria Immigration Service;
(r) National Space Management. Agency;
(s) Nigerian Information Technology Development Agency;
(t) Nigerian Communication Commission;
(u) Galaxy backbone;
(v) National Identity Management Commission;
(w) Nigeria Prisons Service;
(x) One representative each let the following
(i) Association of Telecommunications Companies of Nigeria;
(ii) Internet Service Providers Association of Nigeria;
(iii) Nigeria Bankers Committee;
(iv) Nigeria Insurance Association;
(v) Nigerian Stock Exchange;

[10] A. A. Kana, 'Institutional Challenges in Nigeria's Anti-Corruption Regime: The Role of EFCC and ICPC' (2018) 4(1) *NIALS Journal of Law and Development* 45.
[11]

(vi) Non-Governmental Organization with Focus on Cyber Security listed under the First Schedule to the Act.

A representative appointed pursuant to subsection (1) of section 42 is to be an officer not below the Directorate Cadre in the Public Service or its equivalent. Under (3) of the same section, a member of the Council shall cease to hold office if (a) he ceases to hold the office on the basis of which he became a member of the Council; or (b) the President is satisfied that it is not in the public interest for the person to continue in office as a member of the Council. The meetings of the Council shall be presided over by the National Security Adviser. The Council shall meet at least four times in a year and whenever it is convened by the National Security Adviser.

The Act establishes the Cybercrime Advisory Council[12] and the Council shall:

(a) Create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and mandated to provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria: Functions and powers of the Council.
(b) formulate and provide general policy guidelines for the Implementation of the provisions of this Act:
(c) advise on measures to prevent and combat Computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues;
(d) establish a program to award grants to institutions of higher education to establish cyber security research centers to support the Development of new Cyber security defences, techniques and processes in the real-world environment;
(e) promote Graduate Traineeships in Cyber security and Computer and Network Security Research and Development. The Council shall have power to regulate proceedings and make standing orders with Respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as Council may, from time to time determine.[13]

4. Nigerian Financial Intelligence Unit

The Nigerian Financial Intelligence Unit (NFIU) serves as Nigeria's central national agency responsible for receiving, analyzing, and disseminating financial intelligence concerning suspicious transactions related to money laundering, terrorism financing, and other economic crimes.[14] It was originally established in 2004 as a department within the Economic and Financial Crimes Commission (EFCC) pursuant to Section 1(2) and Section 6(b) of the EFCC (Establishment) Act, 2004.[15] However, following sustained international pressure and Nigeria's suspension from the Egmont Group of Financial Intelligence Units in 2017, the NFIU was restructured into an autonomous entity through the enactment of the Nigerian Financial Intelligence Unit (Establishment) Act, 2018.[16]

The NFIU Act 2018, under Section 1(1), establishes the Unit as 'the central national agency for the receipt and analysis of financial disclosures, and for the dissemination of intelligence to competent authorities.'[17] This statutory reform detached the NFIU from the EFCC, granting it operational independence and direct reporting lines to the President through the Office of the Attorney-General of the Federation (AGF).[18] The Unit's autonomy was a legal and diplomatic imperative to align Nigeria's financial intelligence regime with international standards prescribed by the Financial Action Task Force (FATF) and the Egmont Group Charter, both of which require functional and structural independence for Financial Intelligence Units (FIUs).[19]

[12] S. 43 (1) and (2), CCPA, 2015.
[13] Cybercrimes (Prohibition, Prevention, etc.) Act 2015, Section 41(2)(a)-(e), Laws of the Federation of Nigeria.
[14] Nigerian Financial Intelligence Unit (Establishment) Act 2018, Long Title.
[15] Economic and Financial Crimes Commission (Establishment) Act 2004, ss 1(2), 6(b).
[16] Egmont Group, *Suspension Notice on Nigeria* (2017).
[17] Nigerian Financial Intelligence Unit (Establishment) Act 2018, s 1(1).
[18] Ibid, s 3(1).
[19] Financial Action Task Force, *Recommendation 29 and Interpretive Note* (2021).

The NFIU's core functions are articulated under Section 2(1) of its Establishment Act, which mandates it to: 'Collect, analyze and disseminate financial intelligence to competent authorities and to act as the central agency for the receipt of suspicious transaction reports (STRs) and currency transaction reports (CTRs)'.[20] This provision confers on the NFIU the role of an intelligence hub rather than a prosecutorial agency.[21] It receives information from banks, insurance companies, microfinance institutions, casinos, and other designated non-financial businesses and professions (DNFBPs), including real estate agents and legal practitioners.[22] Through these disclosures, the NFIU identifies patterns of suspicious financial behaviour indicative of money laundering, terrorist financing, or cyber-fraud.[23]

Additionally, Section 2(2) authorizes the NFIU to share intelligence with domestic agencies such as the EFCC, Independent Corrupt Practices and Other Related Offences Commission (ICPC), Nigeria Police Force, Department of State Services (DSS), and Central Bank of Nigeria (CBN), as well as international FIUs through the Egmont Secure Web.[24] The NFIU, therefore, functions as Nigeria's primary financial intelligence clearinghouse, providing actionable intelligence to enforcement agencies while ensuring compliance with confidentiality and data protection standards.[25] In accordance with Section 5(1) of the Act, financial institutions are mandated to submit Suspicious Transaction Reports (STRs) and Currency Transaction Reports (CTRs) to the NFIU within 24 hours of detection.[26] Non-compliance with these reporting obligations attracts administrative sanctions and penalties under Section 10(3), including suspension of licenses or fines.[27] This obligation ensures early detection of money laundering networks, terror financing, and cyber-enabled fraudulent transactions.[28]

The relationship between the NFIU, EFCC, and the AGF is one of functional interdependence anchored in distinct statutory roles.[29] While the EFCC retains investigative and prosecutorial powers under its enabling Act, the NFIU provides the intelligence foundation for such investigations.[30] This synergy ensures a sequential law enforcement chain: intelligence collection (NFIU) investigation (EFCC/Police) prosecution (EFCC/AGF).[31] Under Section 8(1) of the NFIU Act, the Unit is mandated to submit periodic intelligence and activity reports to the Attorney-General of the Federation, who, by virtue of Section 174(1) of the Constitution, supervises all criminal prosecutions on behalf of the Federal Government.[32] This arrangement preserves constitutional coherence by ensuring that intelligence operations support, rather than duplicate, prosecutorial functions.[33]

In practice, the NFIU works closely with the EFCC's Financial Intelligence and Analysis Department (FIAD) to trace illicit financial flows, freeze suspect accounts, and assist in asset recovery proceedings under the Money Laundering (Prevention and Prohibition) Act 2022.[34] For example, in *FRN v Jide Omokore*, the EFCC's successful asset forfeiture proceedings relied heavily on NFIU-provided intelligence linking offshore accounts to proceeds of corruption.[35] The NFIU is Nigeria's representative within the Egmont Group of Financial Intelligence Units, an international network that facilitates cross-border intelligence sharing.[36] Membership in the Egmont Group enables the NFIU to exchange financial

[20] Nigerian Financial Intelligence Unit (Establishment) Act 2018, s 2(1).
[21] Ibid.
[22] Ibid, s 2(2).
[23] Ibid.
[24] Ibid.
[25] Egmont Group Charter (2013).
[26] NFIU Act 2018, s 5(1).
[27] Ibid, s 10(3).
[28] Ibid.
[29] Ibid, s 8(1).
[30] Economic and Financial Crimes Commission (Establishment) Act 2004, s 6(b).
[31] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 174(1).
[32] Ibid.
[33] Ibid.
[34] Money Laundering (Prevention and Prohibition) Act 2022, s 2(1).
[35] *Federal Republic of Nigeria v Jide Omokore* (Unreported, FHC/ABJ/CR/21/2016).
[36] Egmont Group Charter (2013).

intelligence with over 160 FIUs worldwide, a crucial tool for tracking funds laundered through international banking systems.[37]
Additionally, the NFIU plays a critical role in Nigeria's compliance with Financial Action Task Force (FATF) Recommendations, particularly Recommendation 29, which mandates each jurisdiction to establish an independent FIU for the collection and analysis of suspicious transaction reports.[38] Nigeria's reinstatement into the Egmont Group in 2018 followed legislative guarantees of the NFIU's autonomy and budgetary independence.[39] Through these collaborations, the NFIU has assisted in high-profile transnational investigations involving internet fraud, money laundering, and terrorism financing, particularly in partnership with the United States' Financial Crimes Enforcement Network (FinCEN) and the United Kingdom's Financial Conduct Authority (FCA).[40]

Despite its progress, the NFIU's legal and operational framework contains notable lacunae that hinder optimal performance.[41] First, the NFIU Act does not expressly define the extent of its intelligence dissemination authority, leading to tensions with agencies like the EFCC and DSS over access to sensitive data.[42] While Section 9 authorizes information sharing, the absence of procedural guidelines creates the risk of data misuse or unauthorized disclosure.[43] Second, the Unit lacks prosecutorial powers, relying entirely on enforcement agencies to act on its intelligence.[44] This dependency sometimes results in delays or failures in prosecution, particularly when inter-agency rivalry or bureaucratic inertia intervenes.[45] Third, the NFIU Act omits explicit provisions for digital currency monitoring and blockchain transaction tracking, despite the increasing use of cryptocurrencies for money laundering and cybercrime.[46] Unlike jurisdictions such as the United States, where FinCEN regulates virtual asset service providers, Nigeria's framework remains technologically limited.[47] Fourth, although the Act guarantees operational independence, its budgetary allocations are still channelled through the Office of the Attorney-General, undermining the principle of financial autonomy required by FATF standards.[48]

This dependency may expose the NFIU to political influence or funding delays.[49]
Fifth, there is no clear data retention and destruction policy within the Act.[50] Given the sensitivity of financial intelligence, the absence of retention limits risks breaching privacy rights under Section 37 of the Constitution.[51] Sixth, capacity constraints persist.[52] The NFIU lacks adequate personnel trained in digital forensics, artificial intelligence-based anomaly detection, and blockchain analytics—tools now indispensable for modern financial intelligence work.[53] Seventh, there is insufficient public-private partnership engagement.[54] While financial institutions submit reports, they are rarely integrated into national intelligence planning, contrary to FATF Recommendation 20 which emphasizes feedback loops.[55]

[37] Ibid.
[38] FATF Recommendation 29 (2021).
[39] Egmont Group Re-admission Notice on Nigeria (2018).
[40] Financial Crimes Enforcement Network (FinCEN) Cooperation Bulletin (2020).
[41] NFIU Act 2018, passim.
[42] Ibid, s 9.
[43] Ibid.
[44] Ibid, s 2(1).
[45] O. Adeyemi, 'The Role of FIUs in Nigeria's Financial Crime Framework' (2022) *Nigerian Journal of Law and Finance* 74.
[46] NFIU Act 2018, passim.
[47] FinCEN Guidance on Virtual Assets (2019).
[48] NFIU Act 2018, s 13.
[49] Ibid.
[50] Ibid.
[51] Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.
[52] NFIU Annual Report (2023).
[53] Ibid.
[54] O. N. Ajibola, 'Public-Private Collaboration in Financial Intelligence' (2021) *African Journal of Financial Security* 115.
[55] FATF Recommendation 20 (2021).

In comparative terms, Nigeria's NFIU mirrors the structure of other international FIUs but falls short in technological sophistication.[56] For example, the United States' FinCEN and the United Kingdom's UK Financial Intelligence Unit (UKFIU) employ machine-learning algorithms for automated detection of suspicious activity.[57] South Africa's Financial Intelligence Centre (FIC) also integrates private sector compliance feedback into its annual risk assessments.[58] Nigeria's NFIU, though legally independent, remains structurally dependent on the Ministry of Justice for funding and administrative supervision.[59] To reach full compliance with global standards, Nigeria must strengthen its technological infrastructure, operational independence, and feedback mechanisms between intelligence and enforcement.[60]

The Nigerian Financial Intelligence Unit (NFIU) plays a foundational role in Nigeria's financial crime control architecture by serving as the intelligence backbone for enforcement agencies such as the EFCC, ICPC, and the Police.[61] Its transformation from an EFCC department into an autonomous entity marked a major advancement in Nigeria's compliance with international anti-money laundering norms.[62] However, the Unit's effectiveness depends on the timely translation of intelligence into prosecutorial action, a process hampered by jurisdictional overlap, limited capacity, and lack of digital monitoring powers.[63] To strengthen its operational impact, Nigeria should: Amend the NFIU Act to include cryptocurrency and digital asset monitoring; Guarantee full budgetary and operational independence; Establish clear data management and privacy protocols; and Enhance inter-agency coordination through real-time intelligence-sharing systems.[64] These reforms would ensure that the NFIU fulfils its mandate as a globally compliant, technologically advanced, and institutionally independent financial intelligence authority capable of supporting Nigeria's anti-financial crime efforts with precision and integrity.[65]

5. Special Control Unit against Money Laundering

The Special Control Unit Against Money Laundering (SCUML) is a specialized enforcement and regulatory unit established to monitor, supervise, and regulate the activities of Designated Non-Financial Businesses and Professions (DNFBPs) in compliance with Nigeria's anti-money laundering framework.[66] SCUML was initially created in 2005 by the Federal Ministry of Industry, Trade and Investment (FMITI), in collaboration with the Economic and Financial Crimes Commission (EFCC), pursuant to the powers conferred under Section 6(c) of the Money Laundering (Prohibition) Act 2004 (now repealed).[67] The current legal basis for SCUML's operations derives from Section 17(1) of the Money Laundering (Prevention and Prohibition) Act, 2022, which mandates the EFCC to establish and maintain a register of all DNFBPs for monitoring and compliance purposes.[68] This statutory recognition of SCUML under the 2022 Act formally integrated it into Nigeria's anti-money laundering enforcement architecture, positioning it as a compliance-focused arm of the EFCC rather than a fully autonomous agency.[69] Consequently, SCUML acts as a bridge between the regulatory functions of the CBN and the prosecutorial mandate of the EFCC, ensuring that non-financial businesses adhere to international standards on anti-money laundering (AML) and counter-terrorism financing (CFT).[70]

[56] FATF Mutual Evaluation Report on Nigeria (2022).
[57] UK National Crime Agency, *UKFIU Annual Report* (2021).
[58] South Africa Financial Intelligence Centre, *Annual Review* (2022).
[59] NFIU Act 2018, s 3(1).
[60] Ibid.
[61] NFIU Act 2018, s 2(1).
[62] Ibid.
[63] Ibid.
[64] FATF Follow-Up Review on Nigeria (2023).
[65] NFIU Act 2018, Long Title.
[66] Money Laundering (Prevention and Prohibition) Act 2022, s 17(1).
[67] Money Laundering (Prohibition) Act 2004, s 6(c).
[68] Ibid.
[69] Economic and Financial Crimes Commission (Establishment) Act 2004, s 6(b).
[70] Money Laundering (Prevention and Prohibition) Act 2022, s 17(2).

The objectives of SCUML are clearly defined under Section 17(2) of the Money Laundering Act, which provides that: 'The Special Control Unit Against Money Laundering shall be responsible for the registration, monitoring and supervision of the activities of designated non-financial businesses and professions to ensure compliance with the provisions of this Act.'[71] Pursuant to this statutory mandate, SCUML performs three interrelated functions: registration, monitoring, and enforcement.[72] First, it maintains a national database of DNFBPs such as real estate agents, car dealers, accountants, casinos, precious stone dealers, and legal practitioners who handle client funds.[73] Registration with SCUML is mandatory, and non-compliance constitutes an offence under Section 19(1) of the Act.[74] Second, SCUML monitors compliance through periodic inspections and on-site audits, ensuring that DNFBPs implement customer due diligence (CDD), record-keeping, and suspicious transaction reporting in accordance with Sections 7–10 of the Money Laundering Act.[75] These measures are crucial, as DNFBPs often serve as intermediaries for laundering proceeds of corruption and cybercrime.[76] Third, SCUML enforces compliance by referring violations to the EFCC for investigation and prosecution.[77] Under Section 6(b) of the EFCC (Establishment) Act, the Commission is empowered to 'enforce and coordinate the enforcement of the provisions of any other law or regulation relating to economic and financial crimes,' which includes AML laws administered by SCUML.[78] This operational linkage ensures that intelligence gathered by SCUML translates directly into prosecutorial action by the EFCC.[79]

SCUML operates administratively under the EFCC but maintains functional coordination with the Nigerian Financial Intelligence Unit (NFIU).[80] The relationship between SCUML and EFCC is institutional rather than hierarchical — SCUML provides regulatory oversight and intelligence on DNFBPs, while the EFCC exercises prosecutorial powers.[81] Under Section 17(3) of the Money Laundering Act, SCUML is required to share information with the NFIU, which serves as the central financial intelligence repository.[82] This triangular relationship — SCUML (regulatory), NFIU (intelligence), and EFCC (enforcement) — forms the backbone of Nigeria's AML/CFT ecosystem.[83] In practice, SCUML generates reports based on suspicious activities in DNFBPs, which are then transmitted to the NFIU for analysis.[84] If the intelligence suggests criminal intent, the NFIU disseminates the findings to the EFCC for prosecution.[85] This coordinated process ensures the continuum from compliance monitoring to intelligence analysis to criminal prosecution, reinforcing Nigeria's adherence to global anti-money laundering best practices.[86]

SCUML's establishment aligns with Financial Action Task Force (FATF) Recommendations 22 and 23, which require that DNFBPs be subject to AML/CFT preventive measures and regulatory oversight.[87] The Unit has been instrumental in ensuring Nigeria's compliance with international obligations under the United Nations Convention Against Corruption (UNCAC) and the ECOWAS Protocol on the Fight Against Corruption.[88] At the domestic level, SCUML has significantly contributed

[71] Ibid.
[72] Ibid.
[73] Ibid, s 19(1).
[74] Ibid, ss 7–10.
[75] Egmont Group, *Typologies on Money Laundering Using DNFBPs* (2021).
[76] Money Laundering (Prevention and Prohibition) Act 2022, s 17(3).
[77] EFCC (Establishment) Act 2004, s 6(b).
[78] Ibid.
[79] Money Laundering (Prevention and Prohibition) Act 2022, s 17(3).
[80] Ibid.
[81] Ibid.
[82] FATF Recommendation 29 (2021).
[83] SCUML Annual Report (2022).
[84] Ibid.
[85] Ibid.
[86] FATF Recommendations 22 and 23 (2021).
[87] United Nations Convention Against Corruption (2003); ECOWAS Protocol on Corruption (2001).
[88] FATF Mutual Evaluation Report on Nigeria (2022).

to Nigeria's removal from the FATF 'grey list' by improving DNFBP registration, monitoring politically exposed persons (PEPs), and reducing vulnerabilities in non-bank financial sectors.[89] Between 2021 and 2023, SCUML recorded over 90,000 DNFBP registrations, reflecting growing awareness and enforcement capacity.[90] Moreover, SCUML collaborates with professional regulatory bodies such as the Institute of Chartered Accountants of Nigeria (ICAN), the Nigerian Bar Association (NBA), and the Real Estate Developers Association of Nigeria (REDAN) to promote compliance awareness.[91] This partnership enhances self-regulation and accountability among high-risk professions.[92]

Despite its achievements, SCUML's operational and legal framework contains several lacunae that hinder its efficiency and effectiveness.[93] First, SCUML lacks statutory prosecutorial powers.[94] It depends entirely on the EFCC to prosecute offences, which often delays enforcement.[95] While this separation of roles ensures legal coherence, it also weakens SCUML's deterrent effect since non-compliant entities perceive enforcement as indirect.[96] Second, the Unit's administrative subordination to the EFCC raises questions about its institutional independence.[97] Although SCUML performs a regulatory role distinct from the EFCC's investigative function, its operational budget and staffing are controlled by the Commission, potentially creating bureaucratic bottlenecks.[98] Third, SCUML's jurisdiction is limited to DNFBPs, leaving a regulatory vacuum in informal economic sectors such as peer-to-peer (P2P) transactions, cryptocurrency trading, and unregistered real estate intermediaries.[99] This exclusion undermines comprehensive AML/CFT coverage.[100] Fourth, the Money Laundering Act does not provide explicit sanctions for professional bodies that fail to enforce AML compliance within their sectors, leaving SCUML reliant on persuasion rather than compulsion.[101] Fifth, there is inadequate inter-agency data integration between SCUML, EFCC, and NFIU.[102] Data sharing remains largely manual and episodic, contrary to FATF Recommendation 31, which requires real-time cooperation and information exchange among competent authorities.[103] Sixth, SCUML lacks a digital compliance infrastructure for online registration and automated risk assessment.[104] This limits its ability to monitor large numbers of DNFBPs efficiently and detect complex laundering patterns involving multiple intermediaries.[105] Seventh, the Act is silent on whistle-blower protection and corporate liability within DNFBPs.[106] Without legal safeguards for compliance officers, whistleblowing within non-financial institutions remains minimal, reducing transparency.[107]

Globally, jurisdictions such as the United Kingdom, Singapore, and South Africa operate robust DNFBP oversight models.[108] The UK's Financial Conduct Authority (FCA) and Her Majesty's Revenue and Customs (HMRC) directly regulate DNFBPs, ensuring strong penalties for non-compliance.[109] Similarly, Singapore's Suspicious Transaction Reporting Office (STRO) and South

[89] SCUML Annual Compliance Report (2023).
[90] SCUML–ICAN–NBA–REDAN MoU (2022).
[91] Ibid.
[92] Money Laundering (Prevention and Prohibition) Act 2022, passim.
[93] Ibid, s 17(2).
[94] Ibid.
[95] Ibid.
[96] Ibid, s 17(3).
[97] SCUML Annual Report (2023).
[98] FATF Mutual Evaluation Report (2022).
[99] Ibid.
[100] Money Laundering (Prevention and Prohibition) Act 2022, passim.
[101] FATF Recommendation 31 (2021).
[102] Ibid.
[103] SCUML Annual Compliance Report (2023).
[104] Ibid.
[105] Money Laundering (Prevention and Prohibition) Act 2022, s 17.
[106] Ibid.
[107] FATF DNFBP Supervision Models (2020).
[108] HMRC, *DNFBP Supervision Report* (2021).
[109] STRO (Singapore) Annual Review (2022); South Africa FIC Annual Report (2021).

Africa's Financial Intelligence Centre (FIC) provide digitized risk-based monitoring frameworks integrated with their national FIUs.[110] Nigeria's SCUML, though aligned with international models, remains less technologically developed and institutionally dependent.[111] To achieve parity with global standards, SCUML must enhance its regulatory independence, digital infrastructure, and statutory clarity.[112]

The Special Control Unit Against Money Laundering (SCUML) plays a vital intermediary role in Nigeria's anti-financial crime system by bridging the gap between financial regulation and criminal prosecution.[113] Through its oversight of DNFBPs, SCUML ensures that non-bank sectors do not become conduits for money laundering and terrorism financing.[114] However, SCUML's effectiveness is constrained by its lack of prosecutorial autonomy, limited jurisdiction, and inadequate technological integration.[115] To strengthen its impact, Nigeria should: Amend the Money Laundering Act to grant SCUML quasi-prosecutorial authority for administrative sanctions; Digitize DNFBP registration and reporting systems; Establish a national inter-agency AML data-sharing platform; and Expand SCUML's jurisdiction to include emerging high-risk sectors such as cryptocurrency and real estate investment platforms.[116] Such reforms would reinforce SCUML's role as a cornerstone of Nigeria's AML/CFT regime, enhance EFCC's prosecutorial efficiency, and solidify Nigeria's compliance with global financial integrity standards.[117]

6. Conclusion and Recommendations

In conclusion, the increasing incidence of cybercrime in Nigeria poses serious threats to the nation's economy, security, and global reputation. Institutions such as the Economic and Financial Crimes Commission, the Nigeria Police Force, and the Independent Corrupt Practices and Other Related Offences Commission play vital roles in investigating, prosecuting, and preventing cybercrime-related offences. Their efforts, supported by legal frameworks such as the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, have contributed significantly to the fight against internet-based crimes in the country. However, the evolving nature of cyber threats requires continuous improvement in institutional capacity, legal mechanisms, and collaborative efforts both locally and internationally. Strengthening these institutions, enhancing technological capabilities, and promoting public awareness will ultimately ensure a more effective response to cybercrime and contribute to the protection of Nigeria's digital space and financial systems.

In view of the increasing prevalence and complexity of cybercrime in Nigeria, it is necessary to adopt effective measures that will strengthen the capacity of relevant institutions to investigate and prosecute cybercrime-related offences. Although agencies such as the Economic and Financial Crimes Commission and other law enforcement bodies have made considerable efforts in combating cybercrime, several improvements are still required to enhance their effectiveness. The following recommendations are therefore proposed:

(i) Strengthening Inter-Agency Collaboration
(ii) Capacity Building and Specialized Training
(iii) Improvement of Legal and Regulatory Frameworks
(iv) Establishment of Specialized Cybercrime Courts
(v) Public Awareness and Education
(vi) Strengthening International Cooperation
(vii) Provision of Adequate Funding and Technological Resources

[110] FATF Mutual Evaluation Report on Nigeria (2022).
[111] Ibid.
[112] Money Laundering (Prevention and Prohibition) Act 2022, s 17.
[113] Ibid.
[114] Ibid.
[115] SCUML Reform Proposal (2024 Draft Bill).
[116] Transparency International, *Global AML Review* (2023).
[117]