CYBER-ENABLED FINANCIAL CRIME AND DIGITAL FORENSICS: AN ANALYSIS OF ROMANCE SCAM NETWORKS, MULE ACCOUNTS, AND THE ROLE OF FINANCIAL INTELLIGENCE IN NIGERIA

Barrister Adebayo Akinade, dfisn
Deputy President & Chief Executive,
Institute of Security Nigeria
Email: bayoakinade77@gmail.com / bayoakinade@yahoo.co.uk
Date: 28 May, 2026

ABSTRACT

The arrest of Urowhe Diana and Rokibat Oluwasheyi Imoru by the Nigeria Police Force National Cybercrime Center [NPF-NCCC] over an alleged ₦18 million romance scam illustrates the convergence of cyber-enabled fraud, money laundering, and family-based conspiracy. This paper analyses the case within Nigeria's legal and institutional framework, with emphasis on digital forensics, legal records management, information security, and law enforcement strategy. It integrates frameworks from Barrister Adebayo Akinade's works on cybercrime investigations, legal records and data forensics, information security in digital environments, and law enforcement strategies. The analysis is balanced with contributions from Nigerian and foreign scholars on cybercrime, financial intelligence, and investigative practice. The paper argues that effective disruption requires integrated financial intelligence, legally sound digital evidence collection, secure information systems, and coordinated law enforcement operations. Recommendations address legal reform, institutional fusion, capacity building, and public prevention.

Keywords: Romance Scam, Cybercrime, Digital Forensics, Money Laundering, Mule Accounts, NPF-NCCC, NFIU, Law Enforcement Strategy, Nigeria.

1.0 INTRODUCTION

1.1 Background

Romance scams exploit emotional trust to defraud victims across borders. Perpetrators rely on mule accounts, Money Transfer Operators, and rapid fund movement to obscure the money trail. On 28 May 2026, NPF-NCCC announced the arrest of a mother and daughter in connection with an ₦18 million scam involving a victim in Malta.

1.2 Problem Statement

Despite legislative and institutional advances, Nigeria faces challenges in disrupting romance scam networks due to the speed of digital transactions, weaknesses in KYC compliance, gaps in digital forensic capacity, and limited public awareness.

1.3 Aim and Objectives

Aim: To provide a policy and operational analysis of romance scam networks in Nigeria and propose measures to strengthen prevention, detection, and prosecution.

Objectives:

1. Analyse the modus operandi in the NPF-NCCC case.
2. Examine the legal framework governing cybercrime and money laundering in Nigeria.
3. Assess the role of digital forensics, legal records management, and information security in investigation.
4. Evaluate law enforcement strategies and inter-agency coordination.
5. Propose reforms for institutional coordination and public protection.

1.4 Methodology

Case study analysis of the NPF-NCCC press statement, doctrinal legal analysis, and application of investigative and forensic principles from Akinade's works, supplemented with comparative literature from Nigerian and international authors.

2.0 FACTUAL SUMMARY OF THE CASE

NFIU issued an intelligence report on suspected computer-related fraud, identity theft, and money laundering. NPF-NCCC's investigation revealed that Emmanuel Amanfo, currently at large, allegedly conspired with his stepdaughter Rokibat Imoru to open multiple accounts. Funds from a Malta-based victim were received via Money Transfer Operators and direct deposits into Rokibat's accounts, then transferred to an Ecobank account held by her mother, Urowhe Diana. Forensic analysis of digital footprints led to the arrest of the mother and daughter. Investigation is ongoing. Suspects will be charged to court upon conclusion.

3.0 LEGAL FRAMEWORK

3.1 Cybercrimes Act 2015 [as amended]

Sections 14 and 22 criminalize computer-related fraud and identity theft. Sections 38-40 provide for data preservation, access orders, and interception of electronic communications.

3.2 Money Laundering [Prevention and Prohibition] Act 2022

Section 18 criminalizes laundering proceeds of unlawful acts. Section 22 imposes reporting obligations on financial institutions and Money Transfer Operators.

3.3 Evidence Act 2011

Section 84 governs the admissibility of electronic evidence, requiring certification and proper chain of custody.

3.4 Administration of Criminal Justice Act 2015

Governs arrest, detention, and trial procedures, including the handling of electronic evidence.

4.0 DIGITAL FORENSICS, LEGAL RECORDS, AND CRIME TRACKING

4.1 Digital Forensics Framework

Akinade 2019 in Cybercrime Investigations and Digital Forensics for Legal and Security Professionals outlines the forensic process: identification, preservation, examination, analysis, and presentation. The book stresses that "the integrity of digital evidence is compromised the moment it is accessed without proper forensic imaging" [Akinade, 2019a, p. 67].

In the NPF-NCCC case, forensic analysis of digital footprints enabled the linkage of suspects to transaction metadata. Proper chain of custody is essential to ensure admissibility under Section 84 of the Evidence Act.

4.2 Legal Records and Data Forensics

Akinade 2019b in Legal Records, Data Forensics and Crime Tracking Systems for Law Enforcement emphasizes the importance of structured legal records and automated crime tracking systems. The work argues that "integrated records management reduces duplication, accelerates case linkage, and enhances prosecutorial readiness" [Akinade, 2019b, p. 34].

Application to the case requires correlation of bank records, MTO logs, SIM registration data, and device identifiers within a unified case management system.

4.3 Comparative Perspective

Casey 2018 notes that digital evidence without proper documentation is routinely excluded in common law jurisdictions. Levi 2017 highlights that financial crime investigations depend on the ability to reconstruct transaction sequences across institutions.

5.0 INFORMATION SECURITY AND FACILITIES MANAGEMENT IN DIGITAL ENVIRONMENTS

5.1 Secure Information Systems

Akinade 2021 inEnhancing Information Security and Facilities Management in Digital Environments_ identifies secure data storage, access control, and audit trails as critical for maintaining evidence integrity. The author states that "information security failures at the point of data collection undermine the entire investigative process" [Akinade, 2021, p. 89].

5.2 Application to Financial Institutions and MTOs

Banks and MTOs involved in the case must maintain secure transaction logs, implement role-based access, and conduct regular audits to prevent tampering and insider compromise.

5.3 Comparative Perspective

Whitman and Mattord 2021 argue that organizational information security policy must align with legal and evidentiary requirements. The Nigerian Data Protection Act 2023 provides the statutory basis for data protection obligations.

6.0 LAW ENFORCEMENT STRATEGIES, TECHNIQUES, AND TOOLS

6.1 Investigative Strategy

Akinade 2020 inLaw Enforcement Strategies, Techniques and Tools for Crime Investigations and Prevention_ advocates for intelligence-led policing, fusion cells, and proactive disruption of financial crime networks. The author notes that "fusion of cyber, financial, and field intelligence reduces the operational space for organized fraud" [Akinade, 2020, p. 112].

6.2 Operational Tools

Tools include link analysis software, financial tracing platforms, mobile device forensic kits, and open-source intelligence monitoring.

6.3 Inter-Agency Coordination

The case demonstrates the financial intelligence to law enforcement pipeline: NFIU generates Suspicious Transaction Reports, NPF-NCCC conducts digital forensics and arrests. Akinade 2020 recommends a 24/7 Financial Crime Fusion Cell with direct access to NFIU data.

6.4 Comparative Perspective

INL 2021 describes the U.S. Financial Crimes Enforcement Network model, where real-time data sharing between banks and law enforcement enables rapid account freezing. Singapore's Anti-Scam Centre integrates police, banks, and telcos for coordinated response.

7.0 MULE ACCOUNTS AND MONEY LAUNDERING MECHANICS

7.1 Role of Mule Accounts

Family members and associates open accounts to receive and layer funds, reducing direct linkage to the principal offender. Akinade 2019a identifies mule networks as "the human infrastructure of cyber-enabled laundering" [Akinade, 2019a, p. 112].

7.2 Legal Liability

Section 18 of the Money Laundering Act 2022 imposes liability on persons who knowingly facilitate the movement of illicit funds, including mule account holders.

7.3 Detection Indicators

Rapid inflows followed by immediate withdrawals, use of multiple low-balance accounts, and mismatched KYC data.

7.4 Comparative Perspective

FATF 2021 reports that mule networks are a primary method for laundering proceeds of romance and investment scams globally.

8.0 CHALLENGES IN INVESTIGATION AND PROSECUTION

1. **Jurisdictional Complexity:** Victims often reside abroad, requiring mutual legal assistance.
2. **Speed of Transactions:** Funds are moved and withdrawn rapidly, reducing recovery chances.
3. **KYC Weaknesses:** Agent banking and MTO outlets sometimes fail to verify customer identity.
4. **Encryption and Cross-Border Data:** Access to data held outside Nigeria requires MLA processes.
5. **Public Awareness Gap:** Victims and mule account holders often lack awareness of criminal liability.

9.0 RECOMMENDATIONS

9.1 Legal and Policy Reform

1. Amend the Cybercrimes Act to allow 48-hour administrative account freezing pending judicial review.
2. Criminalize the reckless provision of mule accounts with minimum mandatory penalties.
3. Mandate enhanced due diligence for MTO agents handling cross-border transfers.

9.2 Institutional and Operational Reform

1. Establish a 24/7 Financial Crime Fusion Cell within NPF-NCCC with direct NFIU STR access, per Akinade 2020.
2. Create a National Mule Account Registry accessible to regulated entities.
3. Expand NPF-NCCC forensic capacity to include mobile device, cloud, and cryptocurrency analysis, following protocols in Akinade 2019a.
4. Implement integrated crime tracking systems as described in Akinade 2019b.

9.3 Information Security and Records Management

1. Mandate secure audit trails and role-based access for all financial institutions handling high-risk transactions, per Akinade 2021.
2. Conduct regular forensic readiness audits of banks and MTOs.

9.4 Capacity Building and Training

1. Institutionalize forensic and investigative protocols from Akinade 2019a, 2019b, 2020, and 2021 across police, EFCC, and NPF-NCCC training curricula.
2. Conduct quarterly joint exercises with banks, MTOs, and NPF-NCCC on live case simulation.

9.5 Preventive and Public Awareness

1. Launch a national campaign on romance scam red flags and mule account liability.
2. Require transaction warnings at MTO and agent banking points.
3. Integrate cybercrime modules into secondary school civic education.

9.6 International Cooperation

Strengthen mutual legal assistance agreements with jurisdictions where victims reside and participate actively in INTERPOL's Financial Crime Working Group.

10.0 CONCLUSION

Romance scams are organized financial crimes that exploit digital anonymity and weaknesses in KYC and records management. The NPF-NCCC case demonstrates that disruption depends on timely financial intelligence, legally sound digital forensics, secure information systems, and coordinated law enforcement strategy. The works of Barrister Adebayo Akinade provide an integrated framework for evidence integrity, records management, information security, and investigative fusion. Combined with comparative practice from Nigerian and international sources, this framework offers a roadmap for strengthening Nigeria's response to cyber-enabled financial crime.

11.0 REFERENCES

Statutes and Policy Documents

Federal Republic of Nigeria. 2015. Cybercrimes [Prohibition, Prevention, etc.] Act 2015.
Federal Republic of Nigeria. 2022. Money Laundering [Prevention and Prohibition] Act 2022.
Federal Republic of Nigeria. 2011. Evidence Act 2011.
Federal Republic of Nigeria. 2015. Administration of Criminal Justice Act 2015.
Federal Republic of Nigeria. 2023. Nigeria Data Protection Act 2023.
Nigeria Police Force National Cybercrime Center. 2026. Press Statement: NPF-NCCC Arrests Mother and Daughter over ₦18 million Romance Scam. Abuja: NPF-NCCC.
Nigerian Financial Intelligence Unit. 2024. Annual Report on Suspicious Transaction Reporting. Abuja: NFIU.

Works by Barrister Adebayo Akinade

Akinade, A. 2019a. Cybercrime Investigations and Digital Forensics for Legal and Security Professionals. Lagos: Institute of Security Nigeria Press.
Akinade, A. 2019b. Legal Records, Data Forensics and Crime Tracking Systems for Law Enforcement. Lagos: Institute of Security Nigeria Press.
Akinade, A. 2020. Law Enforcement Strategies, Techniques and Tools for Crime Investigations and Prevention. Lagos: Institute of Security Nigeria Press.
Akinade, A. 2021. Enhancing Information Security and Facilities Management in Digital Environments. Lagos: Institute of Security Nigeria Press.

Nigerian and African Authors

Alemika, E.E.O. and Chukwuma, I.C. 2000. Policing and Perceptions of Policing in Nigeria. Lagos: CLEEN Foundation.
Omodunbi, O. 2018. Cybercrime and Cybersecurity in Nigeria. Abuja: NITDA Press.
EFCC. 2023. Guidelines on Investigation of Cyber-enabled Fraud. Abuja: Economic and Financial Crimes Commission.

Foreign Authors and Institutional Sources

Casey, E. 2018. Digital Evidence and Computer Crime. 4th ed. London: Academic Press.
Levi, M. 2017. "Money Laundering Risks and E-Commerce."Trends in Organized Crime, 20, 1-18.

Wall, D.S. 2007. Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press.
Whitman, M.E. and Mattord, H.J. 2021. Principles of Information Security. 7th ed. Boston: Cengage.
FATF. 2021. Money Laundering and Terrorist Financing Red Flag Indicators. Paris: Financial Action Task Force.
INTERPOL. 2023. Global Financial Crime Report. Lyon: INTERPOL.
INL. 2021. Financial Crimes and Money Laundering: A Practitioner's Guide. Washington DC: U.S. Department of State.
Action Fraud UK. 2024. Annual Fraud Report. London: City of London Police.

12.0 FURTHER READINGS

1. UNODC. 2021. Comprehensive Study on Cybercrime. Vienna: United Nations Office on Drugs and Crime.
2. Central Bank of Nigeria. 2024. Circular on Enhanced Due Diligence for Money Transfer Operators. Abuja: CBN.
3. Grabosky, P. 2016. Cybercrime and Cybersecurity: The Global Response. London: Routledge.
4. Nigerian Economic Summit Group. 2024. Trade and Digital Economy Policy Brief*. Lagos: NESG.