

THE TRANSNATIONAL THREAT OF FRAUD TO NATIONAL SECURITY: FROM NIGERIA TO THE UNITED KINGDOM



August 2025

TABLE OF CONTENTS

Table of Contents	i
List of Abbreviations	ii
Executive Summary	01
Introduction	03
Background	08
Methodology and Research Design	10
Typologies and Patterns of Transnational Fraud in the Southern Region of Nigeria	11
Socioeconomic and Political Drivers of Fraud in Nigeria	18
Implications for National and International Security	20
Law Enforcement and Intelligence Collaboration: Opportunities and Challenges	22
Policy Recommendations	28
Deterrents Implementation	30
Conclusions	31
References	32
Appendices	37
Contributors	39

LIST OF ABBREVIATIONS

01. BEC: Business Email Compromise
02. CAFEi: Consumer Awareness and Financial Enlightenment Initiative
03. EFCC: Economic and Financial Crime Commission
04. FIU: Financial Intelligence Unit
05. ICC: International Criminal Court
06. ICPC: Independent Corrupt Practices and other Related Offences Commission
07. INTERPOL: International Criminal Police Organisation
08. KYC: Know-Your-Customer
09. MLATs: Mutual Legal Assistance Treaties
10. MOU: Memoranda of Understanding
11. NCA: National Crime Agency
12. NFIB: National Fraud Intelligence Bureau
13. NPF: Nigeria Police Force
14. PEPs: Politically Exposed Persons
15. UK: United Kingdom
16. UN: United Nations
17. SFO: Serious Fraud Office

Executive Summary



Caption: EFCC arrests soldier, 26 others for alleged internet fraud in Lagos

Source: <https://dailypost.ng/2020/08/17/efcc-arrests-soldier-26-others-for-alleged-internet-fraud-in-lagos-photos>

While the broader issue of fraud originating from Nigeria has been widely studied, much of the existing literature fails to analyse the problem by specific regions or to explore the various states driving this criminal activity in detail. Most research treats Nigeria as a single source of fraud, neglecting to investigate the state-level dynamics, regional specialisations, and social and economic institutions that underpin these criminal organisations. This study explores the growing transnational issue of fraud and its implications for national security, focusing particularly on the relationship between Nigeria's southern states, like Lagos, Oyo, Ogun, Ondo, Delta, and Edo, and the United Kingdom. Although fraud has traditionally been viewed as a financial or economic crime, the increasing depth, scale, and sophistication of fraud networks have elevated it to a serious threat to security. These networks utilise digital technology, exploit lax legal enforcement, and benefit from socioeconomic vulnerabilities to carry out a wide range of scams against individuals, corporations, and public institutions in the UK and globally. This research analyses the patterns, typologies, enablers, and security implications of transnational fraud, highlighting the Nigeria-UK connection. It identifies common types of fraud such as cybercrime, Business Email Compromise (BEC), romance scams, sextortion, identity theft, and money laundering, recognising them both as economic crimes and strategic threats. These activities undermine digital and financial infrastructure, erode public trust in institutions, and, in some instances, fund organised crime groups like terrorists.

This study adopts a multidisciplinary approach, drawing on criminology, international relations, and political economy to examine the nexus between fraud and security. It uses legal analysis and media reports to investigate how and why fraud occurs in various Southern Nigerian states, as well as how its consequences spread across borders. The study also reveals how socioeconomic and technological enablers, such as youth joblessness, technological knowledge gaps, cultural glorification of fraud, insufficient institutional monitoring, and cryptocurrency misuse, contribute to the emergence and sustainability of these criminal networks in Southern Nigeria. In many southern Nigerian communities, internet fraud has become normalised, if not glorified, creating an environment in which crime is encouraged, and enforcement is frequently opposed or undermined.

Although both countries have enacted legislation and established anti-fraud agencies, Nigeria's enforcement remains limited by scarce resources, judicial delays, and corruption. Meanwhile, the UK has stronger prosecution capabilities. Still, it often faces challenges due to a lack of cooperation or capacity on the Nigerian side, particularly when it comes to tracking suspects or recovering stolen assets. The study leverages law enforcement expertise to shed light on the hierarchical structures behind these crimes, the gaps that impede effective investigations, and areas requiring focus to contain these offences. Given the scope and gravity of the issue, the study concludes that fraud is no longer a minor or isolated crime, but a significant security threat that demands high-level attention within both national and international security frameworks. Ultimately, this research aims to provide data-driven insights to aid policymakers, security agencies, development partners, and international actors in developing coordinated and effective responses to the escalating threat of transnational fraud between Nigeria and the United Kingdom.



Caption: Nigeria Detains 127 Internet Fraud Suspects in Night Clubs; Guests Say it was Brutal.

Source: <https://www.occrp.org/en/news/nigeria-detains-127-internet-fraud-suspects-in-night-clubs-guests-say-it-was-brutal>

The Transnational Threat of Fraud to National Security: From Nigeria to the United Kingdom

INTRODUCTION

Fraud has shifted from being treated as an isolated financial nuisance to becoming a high-impact, transnational threat to national security. In the United Kingdom, fraud now accounts for over 40% of all reported crime, with UK Finance¹ estimating £1.17 billion lost to confirmed cases in 2023 across nearly 3 million incidents. In 2024, authorised push-payment (APP) fraud losses remained just over £450 million despite a 20% fall in case numbers, the lowest since 2021, showing that fraudsters are consolidating into fewer, more targeted, and higher-value attacks. Reported losses to romance scams in 2024 stood at approximately £99.4m². Most of these scams are cyber-enabled, often beginning on social and messaging platforms before being routed into the UK's fast payment infrastructure.

Southern Nigeria, especially Lagos, Ogun, Oyo, Edo, Delta, and Ondo, has become a consistent hotspot for these threat patterns. The types of fraud linked to these states include business email compromise (BEC), romance fraud, sextortion, identity theft, crypto-investment scams, and the recruitment of money mules in the UK. This geographical focus is intentional; it stems from a mix of digital access, technical skills, youth unemployment, and deeply embedded social norms that, in some communities, normalise or even celebrate fraud.

1. <https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024>

2. <https://www.which.co.uk/news/article/romance-fraud-hit-99.4m-in-2024-here-are-7-signs-youre-dating-a-scammer-avu9z2G7yuCh>

A Changing Criminal Landscape

Historically, “419” advance-fee fraud and unsophisticated phishing have defined Nigeria as a hub for fraud. Over the past decade, these crimes have evolved into sophisticated, multi-layered operations capable of targeting and exploiting victims worldwide. Recent enforcement operations illustrate this shift. In December 2024³, Nigeria’s Economic and Financial Crimes Commission (EFCC) raided the “Big Leaf Building” in Victoria Island, Lagos, detaining 792 suspects, including 148 Chinese and 40 Filipinos, in a seven-storey “call-centre” used for romance and crypto-investment scams targeting overseas victims. According to the EFCC, all floors were equipped with high-end computers; investigators recovered 500 SIM cards; and recruits underwent a two-week induction on how to impersonate foreign females in online chats. There have been no convictions, and public communication on the ongoing case is sparse.

Such operations blur the lines between cybercrime, organised crime, and human trafficking. In several cases, recruits, both Nigerian and foreign nationals, have been deceived with fake job offers, trapped in debt bondage, and coerced into running scam scripts. This mirrors the “fraud factory”⁴ model seen in parts of Southeast Asia, underscoring that not all participants in these networks are willing offenders; some do not have a choice.



3. <https://www.efcc.gov.ng/efcc/news-and-information/news-release/10584-efcc-bursts-syndicate-of-792-cryptocurrency-investment-romance-fraud-suspects-in-lagos-arrests-193-chinese-arabs-filipinos-others>

4. <https://news.sky.com/story/they-fall-in-love-with-me-inside-the-fraud-factories-driving-the-online-scam-boom-13234505>

The Nigeria–UK Fraud Connection

The UK is an appealing target for Nigeria-connected fraud networks for multiple reasons. First, the UK features high digital adoption and near-instant payment systems that enable funds to be transferred quickly, often before a victim recognises they have been scammed. Second, the UK's sizeable Nigerian diaspora, most of whom are law-abiding, can be exploited for cultural familiarity, language, and local knowledge in laundering operations. Third, gaps in regulation and procedures for cross-border cooperation mean that even when UK victims report fraud linked to Nigeria, Mutual Legal Assistance Treaty (MLAT) processes can take months or years, allowing suspects to destroy evidence or flee. Finally, some cyberfraud narratives in West Africa incorporate a colonial grievance logic, where targeting Western victims is reframed as a form of economic and historical revenge. This does not excuse the wrongdoing, but it offers insight into how fraud is sometimes rationalised as wealth redistribution or self-reparation in contexts marked by past exploitation.

Research shows that some online fraudsters in West Africa rationalise their actions as a form of reparative justice or wealth reclamation due to colonial exploitation. In interviews conducted by academics Suleman Lazarus and colleagues⁵, offenders—especially those involved in romance scams—explicitly invoked historical colonial injustice. They framed their acts as correcting centuries of extraction by Western powers, suggesting that targeting Western victims was a symbolic act of retrieving wealth taken from their ancestors. This narrative allows them to neutralise guilt and stigmatise Western victims as part of a broader reparative narrative.

These dynamics create an asymmetric enforcement environment. In the UK, law enforcement agencies such as the National Crime Agency (NCA) and the City of London Police's National Fraud Intelligence Bureau (NFIB) possess advanced investigative tools but have limited jurisdiction overseas. In Nigeria, the EFCC, police cybercrime units, and the National Financial Intelligence Unit (NFIU) face issues of under-resourcing, political interference, and heavy caseloads that hinder or prevent prosecutions. Although there have been joint successes, like INTERPOL/Group-IB's "Operation Falcon"⁶ which disrupted Nigeria-linked BEC crews, systemic cooperation remains inconsistent.

5. https://eprints.lse.ac.uk/126900/1/Fraud_as_Legitimate_Retribution_for_Colonial_Injustice_Neutralization_Techniques_in_Interviews_with_Police_and_Online_Romance_Fraud_Offenders.pdf



Caption: Sample image of a sextortion threat

Source: AI photo generated on Freepik

From Romance Fraud to Sextortion

Another evolving dimension is the overlap between romance scams and sextortion. Fraud “academies” or “Hustle Kingdoms” in Nigeria have been documented training recruits to run both types of schemes, sometimes escalating from one to the other within the same victim relationship. In a typical pattern, a scammer invests weeks or months building trust through online romance, then requests intimate images or videos. Once obtained, these materials become leverage for sextortion demands, which can be repeated or resold to other criminals. UK law enforcement has warned of increasing sextortion harms, including suicides among young victims, leading to calls for social media platform accountability and potential extraditions for overseas perpetrators.

6. <https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group>



WHY THIS REPORT?

This study focuses on the Nigeria–UK fraud nexus to fill a gap in current literature. Many reports treat Nigerian fraud as a single, nationwide phenomenon without breaking down the distinct regional ecosystems, typologies, and enablers that shape its transnational impact. By examining the southern states most frequently linked to UK-targeting scams, this report identifies patterns, organisational structures, and socio-economic drivers that must be addressed to disrupt these crimes effectively.

The analysis draws on multiple sources: industry loss data (UK Finance), law-enforcement briefings (EFCC, NCA, INTERPOL), academic studies on cybercriminal networks, and credible media reporting. It also incorporates direct quotes and case snapshots to illustrate the human impact and operational realities of fraud networks. This combination of quantitative and qualitative evidence is intended to help policymakers, practitioners, and international partners design targeted interventions that address both the symptoms and root causes of transnational fraud.

BACKGROUND

The socioeconomic characteristics and current history of Nigeria provide numerous indications as to why fraud has thrived. The country is frequently regarded as a major example of the economic idea of the 'paradox of abundance', which describes the tendency of nations with abundant resources outside the Western world to descend into poverty, violence, and corruption⁷. The commercialisation of oil in post-independence Nigeria provided an unparalleled incentive for the proliferation of fraudulent practices, as the economy was awash with petrodollars, which were considered part of a national cake to be divided⁸. Before then, the legend of Prince Modupe⁹, a fraudster active in the 1930s and 1940s, involved impersonating royalty and courting gullible correspondents in the U.S., at some point even appearing at the San Francisco Opera House in 1947 under false titles. In the mid-1940s, Nigeria also saw the emergence of the *Wayo Tricksters*¹⁰ alongside these highly successful "princes." They were financial scammers who sold victims boxes of blank paper, promising that, with the application of a particular chemical, these sheets would turn into valid currency. Consequently, it is clear from the preceding that fraud in Nigeria predates the advent of electronic payments or internet-enabled transactions, which are central to cashless policies.

Therefore, fraud, which was previously considered a criminal or commercial offence, has undergone significant changes in scope and effect over the last two decades. With the growth of digital globalisation and increasing connectivity, fraud has evolved into an organised, international industry with far-reaching consequences for national security¹¹. Nigeria, Africa's most populous country and largest economy, is at the heart of this phenomenon. It has achieved global recognition as both a source and a hub of different types of fraud, most notably cyber-enabled fraud such as Business Email Compromise (BEC), romance scams, identity theft, advance-fee schemes, money laundering, and, more recently, cryptocurrency-based fraudulent transactions¹².

This threat is most obvious in the nation's southern states. These states, including Lagos, Ogun, Oyo, Ondo, Delta, and Edo, have emerged as fraud hotspots, fuelled by a complex interplay of socioeconomic issues, governmental negligence, and the unfettered expansion of digital subcultures that celebrate criminal brilliance. Our Key Informant Interview (KII) respondent from the Economic and Financial Crimes Commission (EFCC) says,

7. Okorie, C., Udoh, E., & Bassey, O. B. (2023). Mirroring the developmental challenges of oil-rich Nigeria within the context of resource curse/Dutch disease and paradox of plenty. *TIJER—International Research Journal*, 10(4), 818-834.

8. Tade, O., & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology*, 64(16), 1717-1740.

9. <https://pmnewsnigeria.com/2019/09/18/419-cases-other-scams-in-nigeria-date-back-to-the-1930>

10. <https://thenativemag.com/nigerian-rappers-cybercrime/>



In the southern states, particularly Lagos, Delta, Edo, and Rivers, Business Email Compromise (BEC) remains the dominant typology. These areas host a large concentration of international business operations and maritime trade, making corporate communication a prime target for interception and invoice manipulation. Romance scams are also highly prevalent, especially among younger operators who leverage social media to target emotionally vulnerable victims abroad, predominantly in the UK and North America. Ponzi schemes surface periodically, often tied to charismatic promoters promising unrealistic returns in crypto or agriculture. The prevalence is driven by a combination of high youth unemployment, social validation of sudden wealth, and the proliferation of online communities where these techniques are shared and refined.



The cultural dimension of fraud in these regions is also worth noting. The phenomenon of 'Yahoo Yahoo' – a colloquial name for internet fraud, and its ritualistic version 'Yahoo Plus', indicates a societal shift in value systems, where illegal achievement is frequently glorified in music, cinema, and social media¹³. These narratives radicalise marginalised young people, who perceive fraud as a method to achieve social mobility, respect, and money. While these actions are sometimes disregarded as acts of individual lawlessness, their sheer magnitude, systemic roots, and transnational parts pose severe dangers to state stability and international collaboration¹⁴.

The United Kingdom has emerged as a prime target for such fraudulent activities. Millions of pounds have been lost by British people, corporations, and organisations because of Nigerian-based schemes. Fraudsters use digital platforms, social media, online payment systems, and even cryptocurrency to commit these crimes while remaining mostly anonymous and beyond the purview of UK law enforcement¹⁵. The implications of cross-border fraud go beyond financial losses. They damage societal confidence in institutions, destroy diplomatic trust between Nigeria and the United Kingdom, and enable criminals who use fraud earnings to fund organised crime. This study seeks to bridge current gaps in scholarship by providing a region-specific analysis that connects fraudulent conduct to larger national and worldwide security concerns.

11. Ayemere, I. (2025). The impact of globalization on national security in Nigeria. *African Journal of Social Issues*, 8(1), 145-157.

12. Soares, A. B., Lazarus, S., & Button, M. (2025). Love, lies, and larceny: One hundred convicted case files of cybercriminals with eighty involving online romance fraud. *Deviant Behavior*, 1-24.

13. Nwobodo, R. E. (2024). A Critical Examination of 'Yahoo-Yahoo' among Nigerian Youths as a Breach of African Culture and Values. *International Journal of Religious and Cultural Practice*, 9(2), 1-1.

14. Oluku, O., & Ene, W. R. P. (2024). The Social Support Systems of Yahoo Yahoo Business in Nigeria. *Journal of Social Theory and Research (JOSTAR)* Volume, 4(1).

15. Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2024). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, 27(3), 364-387.

Methodology and Research Design

The study employed a descriptive and exploratory research design, which is suitable for investigating contemporary social and criminal issues, such as international fraud. This approach enables a systematic examination of emergent patterns, causal linkages, and institutional responses. The study focused on fraud in Nigeria's southern area, which includes six significant states: Lagos, Ogun, Oyo, Ondo, Edo, and Delta. These states were chosen due to their well-documented reputations as cybercrime hotspots, high levels of internet penetration, urban density, and concentration of young people involved in fraud. A comprehensive review of peer-reviewed journal articles and books on fraud, transnational crime networks, and national security was conducted. Official publications from the EFCC, ICPC, INTERPOL, the UK Home Office, and the National Cyber Security Centre were also analysed. Consequently, the empirical approach adopted aims to thoroughly explore the patterns, typologies, enablers, and security implications of transnational fraud in Nigeria and the United Kingdom.

This study also employed a qualitative approach using Key Informant Interviews (KIIs) to collect in-depth insights from experienced law enforcement and regulatory officials directly involved in detecting, investigating, and prosecuting transnational fraud involving Nigeria and the United Kingdom. Participants were mainly recruited from the Economic and Financial Crimes Commission (EFCC), cross-border fraud operatives, the Nigeria Police Force (Anti-Cybercrime Unit), and representatives from Immigration, Customs, and Financial Intelligence Units. The selection criteria for respondents included a minimum of five years' operational experience in fraud investigation or prevention, along with prior involvement in at least one cross-border fraud case involving the UK.

Semi-structured interview guides were created for each agency type, comprising open-ended, thematic questions on fraud typologies, operational constraints, inter-agency cooperation, and strategic priorities. Interviews were conducted in English, lasted between 35 and 50 minutes, and were recorded with permission. Officers were guaranteed randomisation of responses to ensure honest participation in the study.

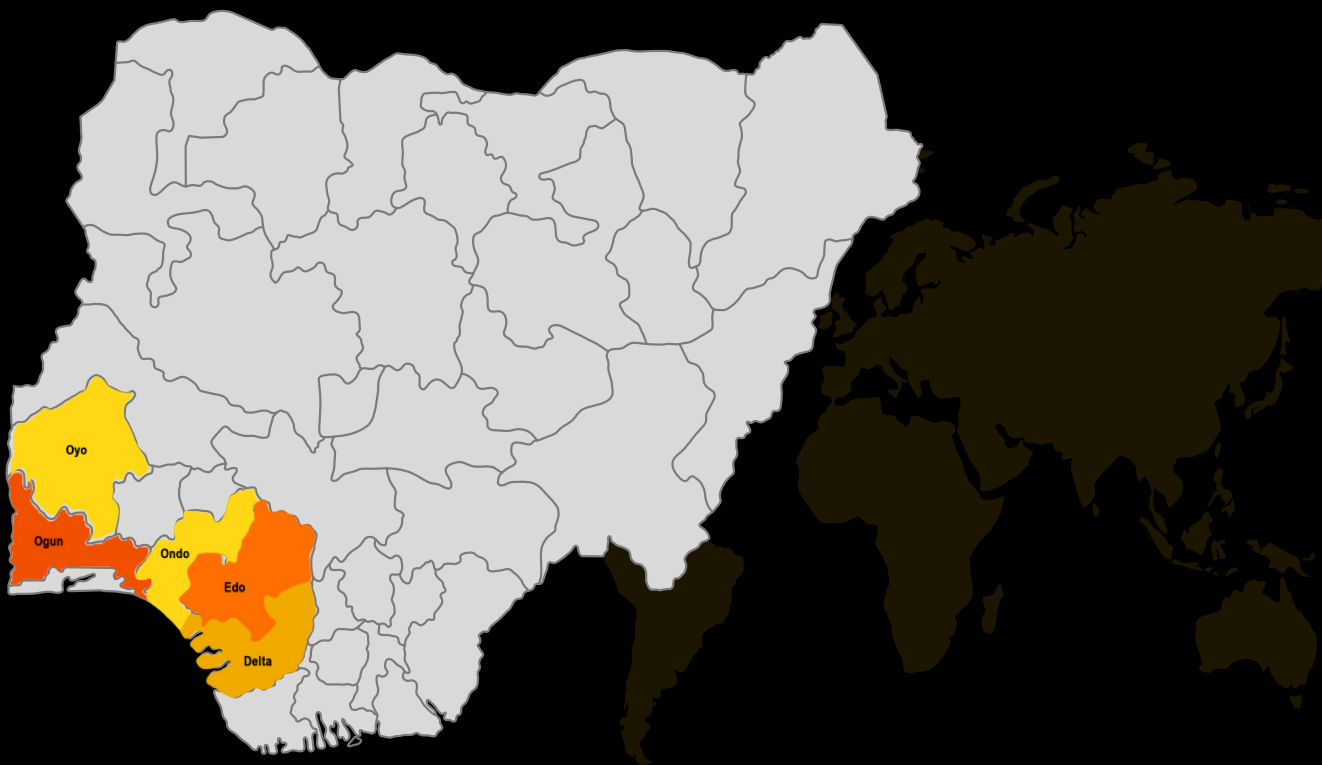
For analysis, the responses were transcribed and analysed using thematic coding. Codes were developed both inductively (emerging from the data) and deductively (based on the interview guide) and organised under key themes such as fraud typologies, operational constraints, collaboration, impact cases, and strategic recommendations.

On the receiving end, the study focused on the United Kingdom as the main target country, highlighting its vulnerability to Nigeria-based fraud. Peer-reviewed journal articles and books on fraud, transnational crime networks, and national security were examined in detail. Official publications from the EFCC, ICPC, INTERPOL, the UK Home Office, and the National Cyber Security Centre were also reviewed. As a result, the empirical approach selected for this study aims to thoroughly analyse the patterns, typologies, enablers, and security implications of transnational fraud in Nigeria and the United Kingdom.

Typologies and Patterns of Transnational Fraud in the Southern Region of Nigeria

Southern Nigeria, which includes states such as Lagos, Oyo, Ogun, Ondo, Delta, and Edo, has become a major hotspot for sophisticated fraudulent activities with direct links to the United Kingdom. Ogundele et al¹⁶ argue that the region's strategic location, high population density, rising urbanisation, expanding internet infrastructure, and huge population of unemployed youth make it a good ground for fraud cartels. Advance fee fraud, often known as '419' in Nigeria, is one of the most well-known and longstanding types of fraud. This sort of fraud involves deceptive communication, which is commonly through email, social media, or messaging apps. It offers the victim a huge amount of money in exchange for upfront payments to 'push' the process¹⁷.

Ayodeji¹⁸ asserts that while previously characterised by badly written emails and unprofessional tactics, 419 scams have become increasingly professional and convincing, using fake web pages and cloned identities. For example, scammers act as British troops, physicians, or successful expatriates on online dating platforms to emotionally persuade victims and vulnerable



16. Ogundele, A. T., Awodiran, M. A., Idem, U. J., & Anwana, E. O. (2023). Cybercrime activities and the emergence of yahoo boys in Nigeria. 2023 International Conference On Cyber Management And Engineering (CyMaEn).

17. Onwudiwe, I. D. (2017). Transnational crimes: The case of advanced fee fraud in Nigeria. In Pan-African issues in crime and justice (pp. 99-120). Routledge.

18. Ayodeji, I. A. (2024). Fraud Detection and Prevention in the Nigerian Financial Industry [Walden University].

UK nationals into sending money¹⁹. When trust is developed, they use delicate claims about medical emergencies, visa issues, or legal bills to collect money.

This issue is closely connected to romance fraud, often called sextortion when sexual blackmail is involved. This type of deception has surged in southern Nigeria, where groups of young men frequently impersonate women or wealthy professionals online to lure unsuspecting individuals into intimate digital interactions. According to Cross et al²⁰, victims are emotionally manipulated into giving money and sharing obscene images or videos, which are then used to blackmail them. Another prevalent form is Business Email Compromise (BEC), targeting UK businesses by hacking their email systems, monitoring communications, and ultimately sending fraudulent orders to divert money to criminal accounts²¹. Criminals often impersonate company executives or trusted partners to deceive financial departments. Identity theft and document fraud also have severe consequences. Fraudsters from southern Nigeria have enhanced their ability to clone identities in the UK. Jabeen et al²² argue that passports, bank account details, and National Insurance numbers are common pieces of personal data obtained by fraudsters. These identities are then used to open bank accounts in the UK, apply for loans or benefits, or create fake online profiles to perpetrate further fraud. Numerous cases have involved Nigerian nationals or diaspora members in the UK being implicated in passport fraud, residency scams, and illegal naturalisation schemes, often involving fake marriage certificates, birth documents, and immigration papers²³.

The view of the KII respondents across the various agencies posits that transnational fraud is a complicated and constantly changing phenomenon. Technological advancements and a lack of coordination and foresight among agencies allow criminals to shapeshift and drive fraudulent transactions. Within the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force (NPF) Anti-Cybercrime Unit, and several border and financial regulatory bodies, Business Email Compromise (BEC) emerges as the most prevalent and financially damaging form of fraud. This aligns with the loss figures reported by the FBI (2023) and the UK's National Crime Agency (2024). The EFCC highlights the widespread occurrence of BEC in the bustling international trade centres of southern Nigeria, while the Police draw attention to its growing technical sophistication, which now includes vendor compromise and multi-stage money laundering. Respondents reveal that offenders are not only diversifying their methods but are also blending romance scams with fake crypto "investments." They also speak to a rise in sextortion cases.

According to David²⁴, illegal cash movements and money laundering are also important forms of transnational fraud with a large presence in southern Nigeria. The Nigeria Financial Intelligence Unit (NFIU) spoke about the strategies criminals use to evade detection.

19. Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, 3, 100044.

20. Cross, C., Holt, K., & Holt, T. J. (2023). To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud. *Criminology & Criminal Justice*, 17488958221149581.

21. Lazarus, S. (2025). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "black Axe" confraternity. *Deviant Behavior*, 46(4), 456-480.

22. Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. *Spectrum of engineering sciences*, 3(1), 143-161.



We routinely detect frequent small-value remittances structured to avoid reporting thresholds, use of third-party accounts for high-risk transfers, and undeclared high-value goods shipped as "personal effects"



As a significant worldwide financial hub, the United Kingdom frequently serves as both a target and a conduit for such unlawful transactions. Money laundering is the process of connecting fraudulent proceeds in Nigeria to the UK's financial system. Maishanu²⁵ asserts that Southern Nigerian scammers frequently funnel cash through a web of shell businesses, offshore accounts, and crypto wallets before injecting them into the UK economy through real estate purchases, luxury goods acquisitions, or investment portfolios. Properties in places including London, Manchester, and Birmingham have been linked to politically exposed persons (PEPs) and alleged fraudsters from Nigeria, many of whom utilise proxies or front businesses to hide ownership²⁶. Also, an often-overlooked trend of deception is the trafficking of individuals from Southern Nigeria to the UK under false pretences, mainly for domestic work, sex trade, or other types of modern slavery²⁷. Victims are given legitimate prospects but instead become indebted and exploited. In reality, some victims are forced to engage in fraudulent acts themselves, such as creating bank accounts, working as money mules, or stealing data²⁸. The Police Cyber Crime Unit respondent said,



Over the past two years, I have seen three dominant streams, and Business Email Compromise (BEC) still remains the highest loss category. It has evolved from classic invoice interception to vendor email compromise and account takeover, utilising OTP phishing kits and SIM swap facilitation. Secondly, Romance scammers are now grooming victims into fake crypto dashboards or forex apps. Actors run longer playbooks, using small early payouts to build trust before the final cash out. Thirdly, sextortion is increasing daily, especially fast-cycle cases via Instagram, Snapchat, and WhatsApp. I have seen two patterns trending: (a) minors/young adults lured into explicit video chats; (b) AI-manipulated images used to threaten disclosure. The harm is acute and time-sensitive.



Furthermore, fraudulent investment schemes and Ponzi operations aimed at Nigerians or dual citizens living in the UK exploit their connections and longing for home to defraud them.

23. Vargas, V. M. (2019). The new economic good: Your own personal data. An integrative analysis of the Dark Web. Proceedings of the International Conference on Business Excellence.

24. David, T. (2018). The adequacy and efficacy of anti-money laundering legislations within the context of electronic banking and informal remittance systems in developing countries with particular reference to Nigeria and South Africa University of London].

Hierarchical Structure in Nigeria to UK Financial Fraud

There is increasing evidence of organised, hierarchical syndicates behind various types of fraud. For instance:

- **Silver Terrier:** An Interpol-identified BEC syndicate comprised of over 400 distinct actors/groups, collectively responsible for thousands of attacks globally. It suggests a sophisticated, multi-tier structure coordinating BEC fraud.
- **“Yahoo Boys”** network: A loosely organised collective that openly shares scripts and techniques for romance scams, sextortion²⁹, deepfake-based impersonations, and BEC operating across social media, messaging platforms, and document-sharing sites like Scribd. These groups function as hubs for training and coordination.
- **Hustle Kingdoms:** The LSE “Scoping Study on Fraud Centres³⁰” documents the existence of “fraud centres” (e.g., call centres or “Hustle Kingdoms”) in Nigeria acting as structured training, recruitment, and operational hubs for a range of scams.

Although a rigid command hierarchy, such as a corporation, isn't universally documented, a clear layered system exists, ranging from trainers and script distributors to technical support and operators, particularly in BEC, romance fraud, and sextortion networks. These parts of a well-oiled criminal enterprise are often referred to or identified in slang based on the type of criminal activity, their role, or hierarchy.

Silver Terrier

Silver Terrier is a mature and complex Nigerian-based BEC syndicate that traces its roots back to around 2014, emerging as exponents of email fraud evolved from traditional “419” scams. By 2018, Unit 42 (Palo Alto Networks) identified over 300³¹ individual threat actors or groups linked to nearly half a million BEC attacks, using 15 distinct commodity malware tools, including Agent Tesla and DarkComet³². By 2019, that network had expanded to over 480 groups, launching up to 245,637³³ attacks in a single month, with annual losses approaching US\$5 billion across 2018 to 2020. Structurally, SilverTerrier operates with loosely hierarchical cells, with separate teams for lead generation, victim communication, and money-flow management. It also leveraged widely available malware priced as low as USD 12–69. Despite their agility, there have been some law enforcement breakthroughs.

25. Maishanu, M. M. (2024). Unveiling the Digital Revolution: Cryptocurrency, Blockchain, and the Future of Finance.

26. Garside, S. M. (2016). Corruption and money laundering: international asset recovery from politically exposed persons in the UK, Nigeria, Russia and China Norwegian University of Life Sciences, Ås].

27. Olayiwola, P. (2024). Tackling Modern Slavery or Worsening Vulnerability? UK's Modern Slavery Agenda in Nigeria. *International Criminology*, 1-9.

28. Igbinomwanhia, O. G. (2021). Human Trafficking and Poverty in South-south Nigeria.

29. <https://www.thesun.ie/news/14579938/sextortion-scams-blackmail-vulnerable-brits-catfish-yahoo>

30. https://www.researchgate.net/publication/386618459_Scoping_Study_on_Fraud_Centres_Ghana_India_and_Nigeria?

In 2022, INTERPOL³⁴ said a 10-day joint operation between men of the NPF Cybercrime Police Unit, INTERPOL's National Central Bureau (NCB) and private partners, dubbed Falcon II, led to the arrest of 11 suspects based in Lagos and Asaba, Delta State. Preliminary analysis of their activities revealed more than 800,000 potential victims' domain credentials and linked the group to attacks on more than 50,000 targets.

In the U.S., Nigerians extradited from the UK have received sentences; one individual in 2024 was sentenced to five years in prison³⁵ along with nearly US \$5 million in restitution, emphasising both the scale and transnational reach of these networks.

Lagos also has a large population of tech-savvy youth, some of whom utilise their skills for nefarious ends³⁶. The proximity to banking headquarters, embassies, telecommunications corporations, and financial organisations makes complex fraud operations easier to conduct, as staging, which is a crucial component of schemes like BEC, is easier to achieve. Following Lagos is Oyo state, notably the city of Ibadan, which has emerged as a breeding ground for youth-led fraud, fuelled by the high number of tertiary schools and a surplus of unemployed graduates³⁷. While fraud schemes in Oyo might not always attain the level of complexity found in Lagos, they are frequently based around low-tech but high-impact frauds, including online romance fraud, SIM card swapping, email phishing, and lottery scams³⁸. In some cases, ritualistic practices are thought to "strengthen" fraud or ensure that victims comply with false requests³⁹.

In recent years, Ogun State has transformed from a peaceful border state to a bustling centre of digital fraud. Cities like Abeokuta, Ijebu-Ode, and Sagamu have become identified with high rates of internet frauds, particularly those targeting foreigners⁴⁰. Ogun's proximity to Lagos provides criminals with access to advanced internet infrastructure and escape routes. Ogun is notably known for romance scams and advance fee fraud (419), which are frequently enabled through dating apps and social media platforms⁴¹. Some communities in the state have accepted cyber fraud as a valid source of survival. Bah⁴² asserts that the state is also becoming a cryptocurrency transaction hub, where fraud revenues are turned into digital currencies for storage or cross-border movement, making Ogun a critical node in transnational financial fraud chains. While not as well-known as Lagos or Ogun, Ondo State is a growing fraud hotspot. Ipinlaye⁴³ argues that cities like Akure and Owo are seeing an increase in fraud and digital frauds, which are largely perpetrated by young men with university degrees and some computer skills. A growing pattern in Ondo is the use of local online marketplaces and classified websites to commit fraud⁴⁴. While these frauds may appear insignificant, they contribute significantly to digital risk and can act as a breeding ground for more advanced fraud behaviour.

31. <https://unit42.paloaltonetworks.com/silverterrier-2019-update/>

32. <https://upcommons.upc.edu/server/api/core/bitstreams/2ce7eb68-04a5-4f11-9ae8-09b06f607216/content>

33. <https://unit42.paloaltonetworks.com/silverterrier-nigerian-business-email-compromise/>

34. <https://www.icirnigeria.org/npf-interpol-bust-cybercrime-syndicate-targeting-over-50000-victims/>

35. <https://cyberscoop.com/nigerian-man-sentenced-to-5-years-for-role-in-bec-operation/>

Furthermore, Delta state, notably the city of Warri, is notorious for its active participation in sextortion scams and email-based money fraud. Many fraudulent activities target overseas victims. These scams typically entail emotional manipulation, blackmail, and requests for money once intimate information is obtained through deception⁴⁵. Beyond sextortion, Delta has a growing number of young cybercriminals who specialise in money mule operations, account takeover fraud, and illicit online dating schemes⁴⁶. Edo State has long been recognised for its participation in international human trafficking, but in recent years, it has also become a centre for transnational fraud⁴⁷, specifically sextortion, false immigration services, and impersonation frauds. Benin City, the state capital, boasts various fraud rings that operate call centres, scam schools, and digital hubs where young people are taught the skill of internet manipulation⁴⁸.

Hence, it is crucial to recognise that fraud in southern Nigeria is not monolithic. It is shaped by the unique socioeconomic circumstances, technological infrastructure, and criminal cultures of each state. Furthermore, beyond financial loss, these scams undermine public trust in digital platforms, destabilise financial institutions, and feed other crimes such as terrorism, drug trafficking, and human smuggling through the funds that are generated⁴⁹. There are also societal losses like reduced entry and higher visa costs to countries for Nigerians, inaccessible local and foreign loans, increased prejudice within and beyond Africa, and a weakening of Nigeria's image in the comity of nations. In both Nigeria and the United Kingdom, national security is under threat not only from the direct financial consequences of fraud, but also from its capacity to damage institutions, undermine the rule of law, and distort governance and international relations.

The Intersectionality of Fraud: Romance Scams and Sextortion

Romance scams and sextortion are increasingly connected within Nigeria-related fraud activities targeting the UK. These crimes often form a continuum: beginning with online romance to establish trust and intimacy, which then leads to requesting personal details or explicit images that can be later used for coercion. Open-source investigations and academic research show that “hustle academies⁵⁰” in West Africa train recruits in both types of fraud, often using the same victim as multiple sources of exploitation. After gaining emotional trust, the shift to sextortion, including threatening to release intimate material unless money is paid, is a common tactic, with operators trained to change tactics based on victim responses. Often, the appearance of a romance scam is an indication that sextortion will occur. In some instances, some victims suffer both: increased requests for financial support in the name of a relationship which they fall for. When the victim tires of sending resources, sextortion begins.

36. Agbeyangi, A., Makinde, A., & Odun-Ayo, I. (2024). Nigeria's ICT and Economic Sustainability in the Digital Age. arXiv preprint arXiv:2401.03996.

37. Ogundele, A. T., Awodiran, M. A., Idem, U. J., & Anwana, E. O. (2023). Cybercrime activities and the emergence of yahoo boys in Nigeria. 2023 International Conference On Cyber Management And Engineering (CyMaEn).

38. Akanle, O., & Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, Characterization and Strategies. *International Journal of Cyber Criminology*, 13(2).

39. Ojedokun, U. A., & Ilori, A. A. (2021). Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria. *International Journal of Criminal Justice*, 3(1), 99-122.

40. Adetoro, N. (2010). Internet utilisation and abuses in selected cybercafes in Ogun State, Nigeria. *African Journal of Library, Archives and Information Science*, 20(1), 19-28.

41. Aborisade, R. A., & Adedayo, S. S. (2021). 'Catch me if you can': the myth and reality of criminals' use of juju to evade arrest from the Nigeria police. *Police Practice and Research*, 22(1), 74-89.

The Guardian⁵¹ reports that “Yahoo boys” have deliberately evolved from early email-based scams into romance phishing and sextortion as smartphone ownership and social media use increased in Nigeria. Similarly, WIRED’s investigation⁵² into scammer communities found that playbooks, scripts, and tutorial videos for both scam types are shared across Facebook, Telegram, TikTok, and YouTube, making it easy for newcomers to learn the transition from romance to sexual blackmail. Academic work by Cross and Holt published in *Criminology & Criminal Justice*⁵³ supports this link, showing that sextortion often develops within existing romance-fraud relationships, exploiting the emotional leverage and private content gathered during the initial grooming phase.

This overlap has significant implications for prevention and victim support. Treating romance fraud and sextortion as separate offences misses the fluid way in which offenders operate. Interventions that disrupt the romance stage, such as stronger identity checks on dating apps, platform-level monitoring for scam scripts, and early law-enforcement engagement, can also prevent escalation into sextortion. At the same time, dismantling training hubs and “hustle academies” that coach offenders in both techniques is critical. Public awareness campaigns and cross-border intelligence sharing should explicitly address this pipeline, equipping potential victims and front-line responders to recognise early warning signs before emotional manipulation becomes blackmail.

42. Bah, A. (2022). Blockchain technology and international money transfers into the Nigerian Remittance market.

43. Ipinlaye, A. (2022). Cybercrime's Toll on Education: Unravelling the Academic Fallout of Internet Fraud among Students.

44. Adebayo, A. A., & Kekere, A. I. (2016). Electronic commerce in Nigeria: The exigency of combatting cyber frauds and insecurity. *JL Pol'y & Globalization*, 47, 159.

45. Adebayo, D. O., Julius, E., & Fasasi, L. (2019). Incidence of Yahoo-Plus activities among in-school adolescents in Delta State, Nigeria. *Global Journal of Guidance and Counselling in Schools: Current Perspectives*, 9(1), 14-23.

46. Button, M., Gilmour, P. M., Hock, B., Jain, T., Jespersen, S., Lazarus, S., . . . Sabia, J. (2024). Scoping Study on Fraud Centres: Ghana, India and Nigeria.

47. Otolde, L. E. (2019). Nature and management of human trafficking: The Nigerian Edo people's experience. In *Crime, Law and Society in Nigeria* (pp. 123-157). Brill.

48. Wariboko, O. P. C., & Nwanyanwu, F. C. (2024). The Dark Side of Connectivity: A Socio-Ethical Exploration of Internet Fraud and Nigerian Youth. *Agidigbo: ABUAD Journal of the Humanities*, 12(1), 89-104.

49. Asiri, A. M. (2024). Corruption and Transnational Organized Crime in the Middle East and North Africa St. Thomas University].

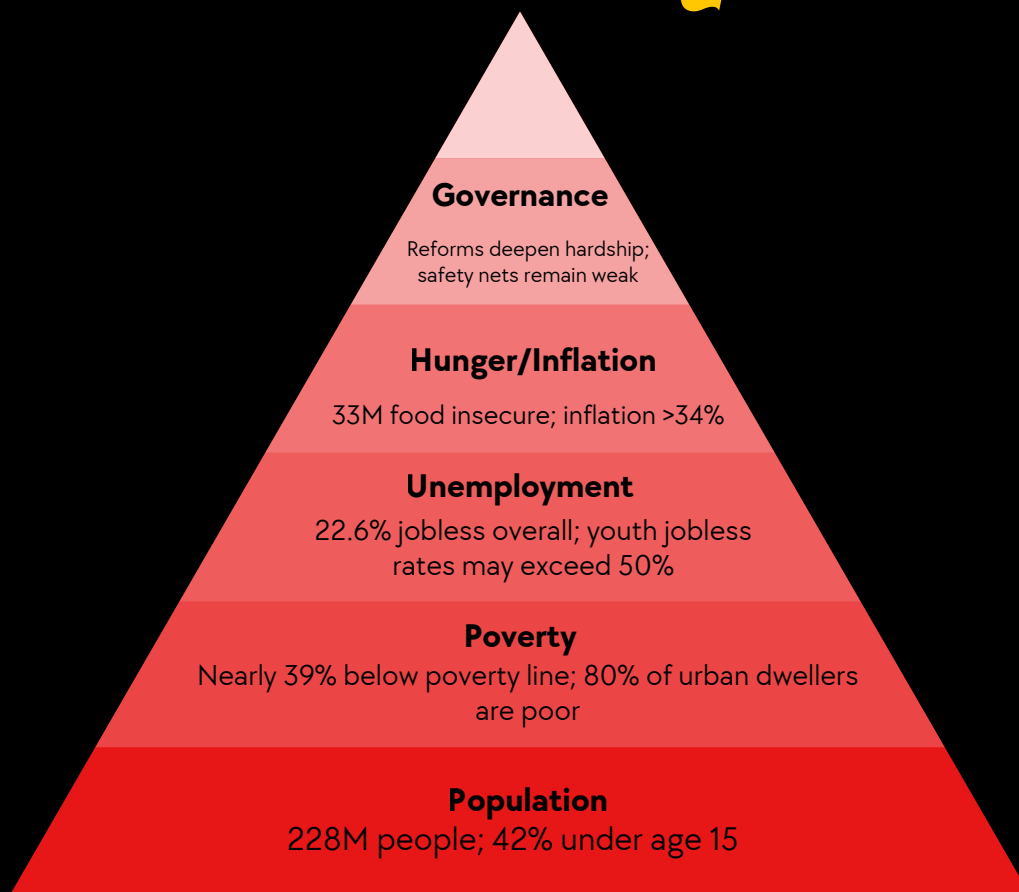
50. <https://ontarget.cmaustralia.edu.au/hustle-academies-west-africas-online-scammers-are-training-others-in-fraud-and-sextortion>

51. <https://www.theguardian.com/uk-news/article/2024/aug/21/how-west-africas-online-fraudsters-moved-into-sextortion>

52. <https://www.wired.com/story/yahoo-boys-scammers-facebook-telegram-tiktok-youtube/>

53. <https://journals.sagepub.com/doi/10.1177/17488958221149581>

Socioeconomic and Political Drivers of Fraud in Nigeria



One of the major causes of fraud in Nigeria is widespread poverty and a high youth unemployment rate. According to Umoh⁵⁴, with almost 60% of the population living below the poverty line and millions of young people unable to find meaningful job, the temptation of fraud becomes not only economic but also existential. The Southern part of Nigeria is home to some of the most urbanised and densely inhabited states; nonetheless, the contradiction of prosperity amidst poverty is evident⁵⁵. While these locations house oil refineries, seaports, tech hubs, and industrial centres, economic disempowerment among youths continues, offering a fertile field for illicit business⁵⁶. Many young people in areas such as Lagos, Benin City, Warri, and Ibadan turn to fraud as a quick and profitable way to avoid unemployment. Furthermore, a sizable segment of the community increasingly idolises people who have amassed wealth and position through illegal means. Lazarus⁵⁷ argues that the rise of 'Yahoo boys' in music, fashion, and social media underscores the creation of a subculture that associates deception with intelligence, innovation,

54. Umoh, E. (2025). Unemployment as a Driver of Crime: Exploring the Roles of Poverty, Youth Restiveness, and Effectiveness of Government Interventions in Emerging Economies. Unemployment as a Driver of Crime: Exploring the Roles of Poverty, Youth Restiveness, and Effectiveness of Government Interventions in Emerging Economies (February 12, 2025).

55. Rivera-Williams, J. (2025). A Multiple Perspective Analysis on Urban Poverty in Developing Nations: A Case Study on Nigeria, Colonial Implications, and Modern-Day Outcomes.

56. Ballard, B. B. (2023). The Petroleum Industry and Economic Empowerment of Young Adults in Nigeria's Niger Delta Region [Walden University].

and rebellion against a failed system. Peer influence is essential in this sense. Flashy lifestyles, fancy automobiles, trendy clothing, and lavish parties are signs of success that attract young people into the criminal underground⁵⁸. In many cases, these fraudsters are protected or even lauded by their communities, reinforcing the culture of impunity.

Perhaps the most devastating driver of fraud in Nigeria is the cooperation of political leaders, as well as the weaponisation of fraudulent proceeds in political processes. In other cases, Adebani and Obadare⁵⁹ contend that criminals utilise the wealth obtained from scams to support political campaigns, gain influence, or secure appointments. In contrast, politicians protect fraudsters in exchange for loyalty and financial support during elections. This connection between fraudsters and political actors is visible in the Southern region, where local power brokers frequently retain links with significant figures in fraud circles⁶⁰. Nigeria has seen a rapid increase in mobile phone and internet penetration, particularly among youth. Smartphones and affordable data plans have enabled even rural communities to access global platforms like Facebook, WhatsApp, Telegram, and dating websites, which are commonly utilised by fraudsters⁶¹. While this digital transition has growth potential, it also reduces the barrier to entry for online fraud. Adedoyin⁶² asserts that free courses, fraud templates, and hacking tools are easily accessible online. In Nigeria, digital literacy is frequently focused on access and consumption rather than cybersecurity, leaving both criminals and victims exposed online.

The failure of law enforcement to successfully detect, investigate, and prosecute fraud contributes considerably to its spread. In Nigeria, institutions such as the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force suffer staffing, training, financing, and digital forensics constraints. In Southern Nigeria, where fraud is both prevalent and adaptive, law enforcement's reactive approach is insufficient to match the magnitude and sophistication of fraud operations. The POLCCU respondent said,

“Our main constraints fall into five categories: Firstly, Time to data (cross-border evidence): Mutual Legal Assistance and platform disclosure windows are slow compared to how quickly offenders erase logs and move funds. Secondly, Forensics capacity: We have strong initial triage capabilities, but our specialist cloud and mobile forensics are limited, especially in rapid extraction at scale and handling password-bypassed devices. Thirdly, Financial tracing: We depend on bank compliance teams, but real-time freezing across multiple fintechs is inconsistent; mule networks exploit this gap. Fourthly, Human resources and tooling: There is a shortage of trained cyber analysts, and link analysis is highly sought after. Finally, Legal/judicial throughput: Cyber dockets are behind conventional cases; some prosecutors and courts require greater familiarity with digital evidence chains (hashing, log integrity, cloud subpoenas).”

In addition, corruption in the police and judiciary hinders accountability. Cases are regularly delayed or rejected, suspects are released without indictment, and high-profile fraudsters frequently avoid prosecution due to political ties or bribes.

57. Lazarus, S. (2018). Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. *Criminology, Crim. Just. L & Soc'y*, 19, 63.

58. Onwughalu, V. C. (2023). The Works and Lifestyles of Nigerian Celebrities as Drivers of Crimes Amongst the Youth and Young People. *ANSU Journal of Arts And Social Sciences*, 10(2), 114-130.

59. Adebani, W., & Obadare, E. (2011). When corruption fights back: democracy and elite interest in Nigeria's anti-corruption war. *The Journal of Modern African Studies*, 49(2), 185-213.

60. Reurink, A. (2019). Financial fraud: A literature review. Contemporary topics in finance: A collection of literature surveys, 79-115.

61. Agbeyangi, A., Makinde, A., & Odun-Ayo, I. (2024). Nigeria's ICT and Economic Sustainability in the Digital Age. *arXiv preprint arXiv:2401.03996*.

62. Adedoyin, A. D. (2023). A study of the impact of technology on cybercrime in the public and private sectors in Nigeria University of Portsmouth].

Implications for National and International Security

Fraud has become a critical issue in modern society, posing substantial threats to national security due to several key aspects that have evolved with the increasing reliance on technology and the interconnectivity of the global information network. The multinational aspect of the fraud, which originated in Nigeria's southern area and targeted the United Kingdom, has far-reaching ramifications for both countries' national security.

It is critical to highlight that the ramifications of fraud on the Nigerian economy are substantial, with the country incurring financial setbacks of up to \$550 million in 2020 alone⁶³. While commercial banks in Nigeria lost US\$39 million due to fraud, Nigeria's Consumer Awareness and Financial Enlightenment Initiative (CAFEi) declared that fraud will cost the economy \$6 trillion by 2030, both domestically and internationally⁶⁴. These ramifications affect many aspects of the economic landscape. Businesses and individuals often face the brunt of illegal activity. When firms incur losses, it naturally leads to a decline in revenue⁶⁵. This domino effect subsequently leads to reduced tax collections, which restricts the government's fiscal capacity to allocate expenditures into critical public sectors, particularly those concerned with security and defence⁶⁶.

Fraud also generates revenue for larger criminal enterprises. Proceeds from fraudulent activities are frequently laundered through sophisticated international routes and reinvested in other types of organised crime, including drug trafficking, arms smuggling, and human trafficking⁶⁷. In some cases, these monies are used to assist extremist and insurgent groups, especially in conflict-prone areas of West Africa⁶⁸. For instance, in 2022, the United States Department of the Treasury's Office of Foreign Assets Control (OFAC)⁶⁹ found six Nigerians guilty of establishing a Boko Haram cell in the United Arab Emirates to raise funds and provide material assistance to it. There is also evidence that small-scale fraud, like illicit profiteering, is also employed to generate income for terrorist activity⁷⁰. While there is limited direct evidence linking UK-based fraud revenues to terrorist organisations, intelligence sources imply that inadequate financial surveillance and illicit financial flows provide chances for terror financiers to use transnational fraud networks⁷¹. The Financial Action Task Force 2013 report on Terrorist Financing in West Africa also alludes to methods by which extremist groups structure and harness financial flows, including irregular and criminal channels.

Fraud also causes considerable reputational harm to both countries, albeit in different ways. Nigeria's recurrent link with fraud has resulted in widespread stereotyping and diplomatic friction. According to Aleyomi⁷², Nigerian citizens, especially young men from the southern region, often face increased scrutiny while requesting for visas, undertaking foreign business or

63. Adisa, O. T. (2023). Impact Of Cybercrime And Cybersecurity On Nigeria's National Security.

64. Ojolo, T. L. (2020). A Criminological Investigation Into The Lived Experiences Of Cybercrime Perpetrators In Southwest Nigeria University Of Kwazulu-Natal, Howard College].

65. Bressler, M. S., & Bressler, L. (2019). Frauds, Embezzlers, Thieves, And Other Bad Actors: How Criminals Steal Your Profits And Put You Out Of Business. *Global Journal Of Accounting & Finance (Gjaf)*, 3(1).

66. Laufer, W. S. (2006). *Corporate Bodies And Guilty Minds: The Failure Of Corporate Criminal Liability*. University Of Chicago Press.

67. Levi, M. (2015). Money For Crime And Money From Crime: Financing Crime And Laundering Crime Proceeds. *European Journal On Criminal Policy And Research*, 21, 275-297.

68. Kar, D., & Spanjers, J. (2017). Transnational Crime And The Developing World. *Global Financial Integrity*, 53, 53-59.

69. <https://home.treasury.gov/news/press-releases/jy0678>

transactions, or seeking academic or economic opportunities overseas. Innocent Nigerians in the diaspora frequently endure the burden of such backlash, facing more scrutiny, discrimination, and reduced possibilities for integration.

The increased sophistication of fraudsters operating between Nigeria and the United Kingdom puts key infrastructure at danger. Government systems, banking platforms, health databases, and electoral technology are vulnerable to infiltration by people attempting to corrupt or destroy public services⁷³. In the UK, cases of fraud have surged in the wake of greater digital transactions, remote work, and decentralised data storage, especially during and after the COVID-19 outbreak⁷⁴. Fraud also promotes social polarisation and insecurity. Ukachukwu and Naetor⁷⁵ assert that areas where fraud is rampant are frequently caught in cycles of crime, leading to disengagement from education, formal employment, and civic involvement.

This not only destabilises local economies but also creates conditions for intergenerational insecurity. Fraud-prone communities often become locked in cycles of crime because the lure of quick, illicit income overshadows long-term investments in education or formal employment. Young people in these areas may drop out of school or avoid seeking legitimate work, believing fraud offers faster rewards. Over time, this reduces civic participation, weakens trust in institutions, and deprives local economies of skilled labour. The result is a form of intergenerational insecurity, where children grow up in environments where crime is normalised and opportunities for lawful advancement are limited.

Fraud associated with Nigeria, particularly online scams, has significant social repercussions that go beyond financial loss, affecting Nigerians' mobility, financial inclusion, and international reputation. Persistent stereotypes⁷⁶, such as the “Nigerian Prince” scam, cause visa officers to scrutinise applicants more closely and lead immigration authorities to adopt stricter fraud checks, resulting in delays and perceived barriers to travel. In 2025, the U.S. embassy in Nigeria warned that individuals involved in visa fraud or falsifying documents could face lifetime bans⁷⁷ or criminal prosecution; measures that disproportionately affect genuine applicants from Nigeria.

Domestically, fraudulent practices undermine local financial systems and limit access to formal loans; meanwhile, an Oxford-member study called “Nigeria’s Fraud Reality” found a serious disconnect between global perceptions of Nigeria as a fraud hub and factual data, noting that such biases impose “systematic barriers” on Nigerian citizens, businesses, and economic development; weakening trust, restricting capital access, and tarnishing Nigeria’s standing internationally.

71. Ryder, N. (2024). To Report Or Not To Report? An Analysis Of The Relationship Between Defence Against Terrorism Financing Suspicious Activity Reports And Fraud In The United Kingdom. In *Financial Crime, Law And Governance: Navigating Challenges In Different Contexts* (Pp. 169-202). Springer.

72. Aleyomi, M. B. (2020). Nigeria's Image Crisis: Drivers, Efforts And Prospects. *African Identities*, 18(1-2), 217-232.

73. Adedoyin, A. D. (2023). A Study Of The Impact Of Technology On Cybercrime In The Public And Private Sectors In Nigeria University Of Portsmouth].

74. Levi, M., & Smith, R. G. (2022). Fraud And Pandemics. *Journal Of Financial Crime*, 29(2), 413-432.

75. Ukachukwu, C. C., & Naetor, V. M. (2020). Value Deficiency, Employment Generation And Crime Among Youths In Nigeria: An Overview. *Asian Research Journal Of Arts & Social Sciences*, 11(2), 13-24.

76. <https://businessday.ng/news/article/stereotyping-how-nigeria-can-reclaim-global-reputation/>

77. <https://businessday.ng/world/article/us-embassy-issues-lifetime-ban-warning-for-visa-fraudsters-in-nigeria/>

Law Enforcement and Intelligence Collaboration: Opportunities and Challenges

In an increasingly interconnected world, fraud has evolved into a global criminal operation that easily crosses borders and countries. However, recognising the threat fraud poses to national security and to eradicate it, the Nigerian government has made several attempts to curb the phenomenon in society, including the enactment of laws such as the Cybercrimes Act of 2015, the Economic and Financial Crimes Commission (EFCC) Act, the Advance Fee Fraud and Other Fraud-Related Offences Act, and the recently updated Money Laundering (Prevention and Prohibition) Act of 2022. Similarly, the United Kingdom functions under an established and targeted legislative framework, including the Fraud Act 2006, the Computer Misuse Act, the Proceeds of Crime Act, and the Serious Crime Act, among others. Some of the maximum penalties for crimes under these pieces of legislation include:



a. Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (and amendments)

- Computer-related fraud: up to 7 years' imprisonment, ₦5 million fine, or both.
- Unlawful system access (hacking, unauthorised use): up to 7 years' imprisonment or ₦7 million fine or both.
- Phishing, spreading malware, impersonation: up to 3 years' imprisonment, ₦1-₦5 million fine, or both.

b. Advance Fee Fraud and Other Fraud-Related Offences Act, 2006

- Advance-fee fraud and similar offences: 7 to 20 years' imprisonment, no option of fine.

c. EFCC (Establishment) Act (2004)

- Establishes EFCC's investigative and forfeiture powers. It does not itself prescribe penalties, but empowers EFCC to enforce underlying offences such as fraud, money laundering, etc.

d. Money Laundering (Prevention and Prohibition) Act, 2022

- Offenders (individuals or corporate bodies) can face imprisonment for 5 to 10 years and/or fines (e.g. ₦1 million or twice the transaction value), depending on the specific violation.

According to Muller⁷⁸, before the enactment of the Cybercrimes Act of 2015, the Economic and Financial Crimes Commission (EFCC) Act was in existence to prosecute those who committed cybercrime in the country. The Economic and Financial Crimes Commission (Establishment) Act of 2004 established the Economic and Financial Crimes Commission (EFCC), which is an agency charged with investigating and prosecuting economic and financial crimes such as advance fee fraud (commonly known as 419), computer credit card fraud, illegal charge transfers, contract scam, fraudulent entrenchment of negotiable instruments, among others⁷⁹. The EFCC is the authorised financial intelligence unit (FIU) in Nigeria, responsible for coordinating the numerous institutions involved in the fight against money laundering, as well as enforcing all laws related to economic and financial crimes in Nigeria⁸⁰. The major legislation governing cybercrime in Nigeria is the Cybercrime (Prohibition, Prevention, and Other Provisions) Act of 2015. This Act includes measures for the prohibition, prevention, detection, response, investigation, and prosecution of cybercrime in Nigeria⁸¹. It also established the National Cybersecurity Fund, which is a pool of money used to implement the terms of the Act⁸².

78. Muller, S. R. (2022). Digital Forensic Readiness Of Cybercrime Investigating Institutions In Nigeria: A Case Study Of The Economic And Financial Crimes Commission (Efcc) And The Nigeria Police Force.

79. Bello, P., Matthew, F., & Cosmas, A. O. (2022). The Role Of Economic And Financial Crime Commission (Efcc) In Combating Corruption In Nigeria. *Musamus Journal Of Public Administration*, 5(1).

80. Nwambuko, T. C., Uchegbue, B. C., & Ifedi, F. O. (2022). Financial Crimes Control In Nigeria: An Assessment Of The Economic Financial Crimes Commission (Efcc). *Caritas Journal Of Management, Social Sciences And Humanities*, 1(1).

The Money Laundering (Prohibition) Act of 2011, as revised in 2022, offers a legislative framework for fighting money laundering, which is commonly associated with fraud⁸³. Esoimeme⁸⁴ avers that this Act obligates financial institutions to establish internal control mechanisms to prevent money laundering. The Criminal Code Act and the Penal Code Act have provisions that criminalise fraud-related acts like unauthorised access to computer systems, cyber stalking, and identity theft⁸⁵. The two acts are important components of Nigerian legislation that provide measures for pursuing fraud. Nigeria's efforts to combat international crime have been bolstered by cooperation with international agencies such as the International Criminal Court, the United Nations, and Interpol⁸⁶. Interpol offers tools and venues for global information exchange⁸⁷. Interpol's key advantage is that it has global reach through its large membership and a constitution that maintains its neutrality. Indeed, extradition requests, intelligence sharing, and combined operations to apprehend transnational criminals are impossible without such collaboration.

In the United Kingdom, agencies such as the National Crime Agency (NCA), the City of London Police's National Fraud Intelligence Bureau, the Serious Fraud Office (SFO), and Action Fraud collaborate in a coordinated and intelligence-driven manner⁸⁸. The UK's Fraud Review emphasised the need to strengthen cross-sector information sharing and gave major coverage to issues of information, intelligence, and data sharing⁸⁹. Since the publication of the Fraud Review, the necessity for and commitment to enhanced collaboration and exchange of information and intelligence between companies and agencies has been consistently emphasised as a core pillar in several official initiatives for combatting fraud⁹⁰.

However, both Nigeria and the United Kingdom have at times struggled to maintain momentum in anti-fraud partnership. Mihus⁹¹ argues that changes in administration, altering diplomatic agendas, or competing national interests can disrupt previously agreed-upon plans. Memoranda of understanding (MOUs) on intelligence cooperation, for example, can be signed but inadequately implemented or quietly abandoned due to a lack of follow-up⁹². In Nigeria, successive administrations have repeatedly replaced anti-corruption leadership, resulting in policy discontinuities and decreased institutional memory⁹³. In the United Kingdom, concerns such as Brexit, immigration control, and counterterrorism have frequently taken precedent over fraud enforcement, diverting resources and attention away from the Nigerian fraud threat⁹⁴. This is in addition to the fact that cross-border enquiries frequently involve official requests under Mutual Legal Assistance Treaties (MLATs), which can take months or even years to process⁹⁵. Speaking on these delays, the EFCC said,

81. Izevbuwa, O. G., & Ngwoke, R. A. (2022). Combating The Menace Of Cybercrime In Nigeria: A Review Of The Cybercrime (Prohibition, Prevention Etc) Act 2015 And Other Legislations. *Jl Pol'y & Globalization*, 119, 1.

82. Nwabachili, C. O., & Nnoyelu, C. V. (2025). Legality Or Otherwise For The Imposition Of Cyber Security Levy In Nigeria. *Nnamdi Azikiwe University Journal Of International Law And Jurisprudence*, 16(1), 195-210.

83. Olujobi, O. J., & Yebisi, E. T. (2023). Combating The Crimes Of Money Laundering And Terrorism Financing In Nigeria: a Legal Approach For Combating The Menace. *Journal Of Money Laundering Control*, 26(2), 268-289.

84. Esoimeme, E. E. (2017). The Nigerian money laundering (prevention and prohibition) bill, 2016: a critical appraisal. *Journal of Money Laundering Control*, 20(1), 79-88.

85. Egbo, D. (2022). A Critical Analysis Of The Law Regulating Cybercrimes In Nigeria. Available at SSRN 5136457.

86. OKEBUGWU, G. C. (2024). The Role Of International Protective Mechanisms Incurbing Transnational Crimes. *Pplrunlaw Review*, 3(1).

87. Abiodun, T. F., & Abioro, T. (2020). Roles and challenges of international criminal police organization (Interpol) in investigation of crimes and maintenance of global security. *Research Journal of social science and management*, 10(3), 12-34.

88. Button, M. (2021). Hiding behind the veil of action fraud: The police response to economic crime in England and Wales and evaluating the case for regionalization or a National Economic Crime Agency. *Policing: A Journal of Policy and Practice*, 15(3), 1758-1772.

89. Watson, C. (2017). Information And Intelligence Sharing In The Fight Against Fraud And Intellectual Property Crime: Challenges And Strategies For Professional Practice University Of Portsmouth].



As far as I am concerned three reforms are crucial: Faster access to digital evidence from foreign-based tech companies. Current Mutual Legal Assistance Treaty (MLAT) processes are too slow for time-sensitive cybercrime cases. Secondly, specialised cybercrime courts with judges trained in digital evidence admissibility, to reduce case backlog and avoid acquittals on technical grounds. Lastly, stronger asset recovery legislation to allow for quicker freezing and repatriation of fraud proceeds from overseas jurisdictions. Without disrupting the financial incentive, convictions alone won't have a deterrent effect.



These bureaucratic roadblocks hinder proactive cooperation and foster a sense of inefficiency or unwillingness to act. According to Eshemo-Omo and Obieshi⁹⁶, in the UK, there is a rising concern about the timeliness of Nigerian responses to legal requests, and Nigerian authorities frequently blame a lack of capacity or overly onerous documentation requirements from British partners. These bottlenecks impede rapid asset freezing, suspect apprehension, and forensic analysis, providing fraud networks a key time advantage to destroy evidence or vanish.

In conversations with KII respondents, operational constraints continue to emerge as a common hindrance to the effective prevention and investigation of crime. The NPF discusses them in terms of evidentiary latency, particularly emphasising the sluggish pace of cross-border data requests and the limited capabilities for advanced digital forensics. Similarly, the EFCC is advocating for legal reforms to expedite the process of acquiring evidence from abroad and to enhance the judicial understanding of cybercrime cases. Our respondent said,



Our unit's intelligence feeds into active investigations every week. The challenge is not in generating intelligence, but in data-sharing bottlenecks. Barriers include inter-agency rivalry, lack of unified cybercrime databases, and varying security clearance levels that delay dissemination. Furthermore, certain foreign agencies are reluctant to share real-time intelligence unless a formal request is routed through diplomatic channels. This delay often gives suspects enough time to move assets or wipe devices.



90. Gilbert, M., & Wakefield, A. (2018). Tackling Fraud Effectively In Central Government Departments: A Review Of The Legal Powers, Skills And Regulatory Environment Of Uk Central Government Counter Fraud Teams. *Journal Of Financial Crime*, 25(2), 384-399.

91. Mihus, I. (2025). Fraud Hunters Around The World: Fighting Deception In Different Countries. *Socio-Economic Relations In The Digital Society*, 2(56), 115-123.

92. Lubin, A. (2025). Shades Of Legal Nuance: A Functional Analysis Of Intelligence Doubletalk. *Indiana Legal Studies Research Paper No.*

93. Kalama, J. T. (2018). Anti-Corruption War In Nigeria: Reflections On Present And Past Administrations (1999-2018). *International Institute For Policy Review And Development Strategies*, Nigeria+ 234 8174380445, + 234 767021763, 153.

94. Nawaz, M., & Ebner, J. (2016). The Eu And Terrorism: Is Britain Safer In Or Out? *Quilliam*.

95. Delorme, T. (2024). Mutual Legal Assistance, a Mechanism Enabling The Prosecution Of Transnational Organised Crime: Barriers And Solutions. *Sorbonne Doctoral Law Review-Revue Doctorale De Droit De La Sorbonne*, 7(1).

96. Eshemo-Omo, I. P., & Obieshi, E. (2024). A Comparative Analysis of Non-Judicial Remedies for Administrative Acts in Nigeria and the United Kingdom. *AGORA Int'l J. Jurid. Sci.*, 18, 183.

Other agencies also share these concerns, albeit indirectly, pointing out that data-sharing bottlenecks stemming from incompatible formats, delays in clearance, and legal hurdles hinder the real-time interception of funds and goods. This observation aligns with regional studies on intelligence silos within West African law enforcement (Okeshola & Adeta, 2022).

Financial crime investigation and prosecution are typically viewed as underfunded areas of UK law enforcement operations. Financial crime does not appear in the government's crime objectives, and only one force, the City of London Police, incorporates this sector in its organisational priority⁹⁷. The reasons why the UK has been unable to address this issue may originate from the collaborative failure of government, law enforcement, and business to enlighten the public about the true cost of financial crime⁹⁸. It is difficult to make the argument for more law enforcement resources, harsher imprisonment, or higher investment in anti-fraud measures if the problem is not widely understood. In Nigeria, authorities such as the Economic and Financial Crimes Commission (EFCC), the Nigeria Police Force (NPF), and the National Financial Intelligence Unit (NFIU) face chronic underfunding, insufficient personnel training, poor digital forensic skills, and antiquated equipment⁹⁹. Investigations are often hampered by logistical constraints, lack of inter-agency coordination, and political interference¹⁰⁰. In the Southern part of Nigeria, the hotspots for fraud, the lack of proper investigative infrastructure makes these institutions reactive rather than proactive¹⁰¹.

Do Criminal Sanctions Deter Crime?

Deterrence theory holds that punishment discourages crime if the risk of being caught is high, the penalty is known and severe, and enforcement is swift. However, meta-studies show that certainty of punishment tends to matter more than severity alone. In Nigeria, scholars have found that the low conviction rates, weak prosecutions, and slow court processes significantly reduce both individual and general deterrent effects. For instance, research shows that the quality of prosecution moderates any deterrent impact: strong forensic evidence alone doesn't deter fraud unless cases are effectively prosecuted and result in real convictions.

Studies across financial crime contexts indicate that simply raising maximum penalties (e.g., longer prison terms) doesn't effectively deter repeat fraudsters or prospective offenders, especially when actual enforcement is rare or perceived as unlikely.

97. Levi, M. (2008). Policing fraud and organised crime. *Handbook of Policing*, 522-552.

98. Gilmour, P. M. (2021). Exploring the barriers to policing financial crime in England and Wales. *Policing: A Journal of Policy and Practice*, 15(2), 1507-1521.

99. Aliyu, M. M. (2022). Challenges to investigation and prosecution of corruption cases in Nigeria. *AFJCLJ*, 7, 24.

100. Ayodeji, G. I. (2018). Illicit Financial Flows, Insecurity and Challenges of Governance in Nigeria. *Studies in Politics and Society*, 271.

101. Obidimma, E. O., & Ishiguzo, O. (2023). Cybercrime Investigation and Prosecution in Nigeria: The Critical Challenges. *AFJCLJ*, 8, 30.

102. <https://eprints.lse.ac.uk/126338/1/Fraud-Scoping-Study-for-publication-2024.pdf>

In Nigeria, sanctions often lack visibility; cases drag on or are dropped, and prominent fraudsters face little consequence. In a 2024 scoping study conducted by the London School of Economics¹⁰² and Itad, researchers found that legal and institutional deficiencies such as judicial delays, difficulty in gathering evidence, and inconsistent enforcement significantly weaken the deterrent value of fraud prosecutions in Nigeria. Interviews with practitioners and reformed offenders revealed that this unpredictability not only undermines confidence in the system but also creates a perverse incentive, particularly among marginalized youth, who view fraud as a lower-risk pathway compared to formal employment. Evidence from restorative justice models¹⁰³ emphasises that community-based condemnation, loss of reputation, and pressure from family or moral norms can disrupt reoffending more effectively than imprisonment or fines, particularly in low-trust settings.

Despite these hurdles, there is evidence of development. Nigeria's recent efforts to tighten its anti-money laundering regime and expand the capabilities of the NFIU are encouraging. Furthermore, initiatives like Operation Falcon, a combined endeavour between Nigerian and UK law enforcement agencies targeting cybercriminals, show the possibilities of bilateral cooperation¹⁰⁴. To be effective, collaboration requires a conscious and ongoing effort to develop institutional trust, harmonise legal procedures, engage in capacity building, and foster inclusive international collaborations. Most crucially, both Nigeria and the United Kingdom must prioritise anti-fraud operations as vital components of their national and global security agendas, rather than simply as law enforcement issues.

103. <https://pmc.ncbi.nlm.nih.gov/articles/PMC4744856/>

104. Nwafor, I. E. (2024). Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps. *African Journal of Legal Studies*, 16(3), 249-270.

Policy Recommendations

Transnational fraud between Nigeria and the United Kingdom is a complex danger that necessitates an equally complex solution. To effectively counteract the patterns and impacts of this problem, the following recommendations are made:

- The Nigerian government should initiate youth-centred employment and entrepreneurship programmes, especially in the southern region. Emphasis should be on developing skills in ethical technology use, digital entrepreneurship, and innovation. Conditional cash transfers, vocational training, and microfinancing for online businesses can help redirect potential fraud recruits toward legitimate digital economies.
- Nigeria and the United Kingdom must urgently enhance their cybersecurity infrastructure, especially in prevention, detection, and response. Nigeria's federal and state governments, particularly in high-risk areas like Lagos, Ogun, and Edo, should invest in digital forensics laboratories, cyber command centres, and real-time threat monitoring systems. These measures will enhance law enforcement's ability to detect, track, and disrupt fraudulent networks.
- Both countries should modernise their fraud and cybercrime laws. Nigeria's Cybercrimes Act (2015), although important, requires revision to address contemporary issues such as cryptocurrency fraud, deepfake technologies, and social engineering. Legal cooperation agreements, especially the examination of mutual legal assistance treaties (MLATs), should be updated to enable quicker evidence sharing and collaborative investigations.
- Law enforcement cooperation between Nigeria and the United Kingdom should be formalised through the creation of a permanent joint task force dedicated to transnational cybercrime. This team should comprise digital crime experts, financial intelligence analysts, prosecutors, and diplomatic representatives.

- As cryptocurrency continues to play a significant role in laundering criminal proceeds, Nigeria should enforce Know-Your-Customer (KYC) compliance, transaction monitoring, and registration for all crypto exchanges operating within its borders. The UK should enhance its oversight of cross-border cryptocurrency transactions, especially those originating from blacklisted jurisdictions.
- Nigeria's anti-fraud organisations, including the EFCC and NFIU, require ongoing investment in personnel training, equipment, and operational independence. In the United Kingdom, Action Fraud, the National Crime Agency (NCA), and local police forces should collaborate more closely to prevent duplication and enhance case management efficiency.
- Nigeria and the United Kingdom should develop secure, real-time systems for intelligence sharing. These systems should facilitate the swift exchange of digital evidence, provide alerts on emerging fraud typologies, and support collaborative analysis of criminal networks.
- Awareness programs in Nigeria should emphasise both the dangers of fraud and its legal consequences. Campaigns in the United Kingdom should focus on educating the public, especially the elderly and vulnerable groups, about the warning signs of scams such as romance fraud and phishing. Schools, religious institutions, and community organisations in both countries can play vital roles in spreading information on fraud prevention.



Deterrents Implementation

1. Increase the certainty of detection and conviction

- Improve investigative capacity and forensic resources (digital tools, mobile money tracing, SIM-swap detection).
- Prioritise high-profile prosecutions and convictions that are publicised widely, thereby amplifying the perceived risk. Vicarious deterrence¹⁰⁵ via visible punishment of prominent perpetrators strengthens general deterrence effects¹⁰⁶.
- Ensure swift judicial proceedings rather than long delays (“celerity”).

2. Publicise cases and court outcomes

- Use media campaigns to highlight successful convictions, asset seizures, and prison sentences.
- Reports and enforcement bulletins that mention location, value, individuals, legal citations, and sentencing.

3. Expand alternative sanctions

- Nigeria currently does not fully utilise tools such as unexplained wealth provisions (except in Lagos State) or corporate failure-to-prevent-fraud offences. Broader adoption could help deter fraud networks and complicit professionals¹⁰⁷.
- Civil and administrative sanctions (e.g., disbarment, professional exclusion) are also visible and immediate.

4. Combine criminal sanctions with soft deterrents

- Social and internal sanctions, such as community-based stigma, family pressure, moral norms, or public shaming, often have a more substantial deterrent effect than formal legal punishments alone, especially for fraud-related offences where the emotional guilt is powerful¹⁰⁸.
- Increase public awareness campaigns and educational messaging on the harms of fraud and the consequences of convictions.

5. Target networks, not just individuals

- Recognise the interconnected nature of fraud gangs. Sanctions against the organisation, call centres, leadership, and financiers send more effective signals. Utilise asset forfeiture, criminal confiscation, and disruptive litigation to weaken the group's capacity.

6. Leverage international partnerships

- Joint operations (e.g., EFCC-INTERPOL or EFCC-NCA) can accelerate extraditions and create high-visibility outcomes, demonstrating that cross-border cooperation effectively deters scammers who believe they're shielded indoors.

105. https://www.researchgate.net/publication/270634989_The_Deterrence_Effects_of_Vicarious_Punishments_on_Corporate_Financial_Fraud

106. <https://globalinvestigationsreview.com/guide/the-guide-monitorships-archived/third-edition/article/the-academic-perspective/>

107. <https://sas-space.sas.ac.uk/6701/1/Adetunji%2C%20A%20-%20IALS%20-%202017.pdf?>

108. <https://pmc.ncbi.nlm.nih.gov/articles/PMC4744856/>

CONCLUSION

Fraud, previously viewed as a nonviolent and isolated crime, has evolved into a sophisticated, transnational security issue with ramifications that span borders, economies, and political systems. The globalisation of transportation, communications, and finance has benefited not only legitimate businesses but also professional criminals, allowing them to organise transnationally¹⁰⁹. As this study has shown, the transactional relationship between fraud networks operating in Nigeria, notably in the Southern region, and their equivalents or facilitators in the United Kingdom is a key source of insecurity in the twenty-first century.

In Nigeria, poor institutions, widespread corruption, youth unemployment, and socioeconomic disparity provide fertile ground for the expansion of fraudulent practices among those striving to raise their level of living. These processes are amplified in the Southern region by historical marginalisation, urban poverty, and an informal economy based on digital opportunism. Meanwhile, in the United Kingdom, fraud originating from Nigeria, especially in the form of cyber scams, identity theft, and property laundering, has hampered law enforcement functions and contributed to the hardening of immigration policies, racial profiling, and public resentment against African diasporic communities¹¹⁰.

Criminal sanctions can deter fraud but only when supported by effective enforcement, high visibility, and public awareness of the risks. Nigeria's current gaps in prosecution, delays, and low conviction rates weaken any deterrent effect. Greater certainty, speed, transnational cooperation, and innovative sanctions (e.g., anti-money laundering laws, corporate liability, and measures addressing unexplained wealth) are more likely to reduce the volume of fraud.

Therefore, the study's overriding conclusion is that fraud, particularly in its international dimensions, should be reframed as a strategic security problem that necessitates coordinated, preventive, and intelligence-driven countermeasures. Furthermore, a comprehensive solution must address the socioeconomic factors that drive fraud. In Nigeria, particularly in the southern region, this entails investing in education, job development, youth empowerment, and computer literacy to minimise the attractiveness of false money. Combating transnational fraud between Nigeria and the United Kingdom is about more than just law enforcement; it's about national and human security, institutional reform, and geopolitical integrity.

109. Kar, D., & Spanjers, J. (2017). Transnational crime and the developing world. *Global Financial Integrity*, 53, 53-59.

110. Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.

111. Agbeyangi, A., Makinde, A., & Odun-Ayo, I. (2024). Nigeria's ICT and Economic Sustainability in the Digital Age. *arXiv preprint arXiv:2401.03996*.

REFERENCES

- Abiodun, T. F., & Abioro, T. (2020). Roles and challenges of international criminal police organisation (Interpol) in investigation of crimes and maintenance of global security. *Research Journal of social science and management*, 10(3), 12-34.
- Aborisade, R. A., & Adedayo, S. S. (2021). 'Catch me if you can': the myth and reality of criminals' use of juju to evade arrest from the Nigeria police. *Police Practice and Research*, 22(1), 74-89.
- Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2024). Emotional and financial costs of online dating scam: A phenomenological narrative of the experiences of victims of Nigerian romance fraudsters. *Journal of Economic Criminology*, 3, 100044.
- Adebanwi, W., & Obadare, E. (2011). When corruption fights back: democracy and elite interest in Nigeria's anti-corruption war. *The Journal of Modern African Studies*, 49(2), 185-213.
- Adebayo, A. A., & Kekere, A. I. (2016). Electronic commerce in Nigeria: The exigency of combatting cyber frauds and insecurity. *JL Pol'y & Globalization*, 47, 159.
- Adebayo, D. O., Julius, E., & Fasasi, L. (2019). Incidence of Yahoo-Plus activities among in-school adolescents in Delta State, Nigeria. *Global Journal of Guidance and Counseling in Schools: Current Perspectives*, 9(1), 14-23.
- Adedoyin, A. D. (2023). A study of the impact of technology on cybercrime in the public and private sectors in Nigeria University of Portsmouth].
- Adetoro, N. (2010). Internet utilisation and abuses in selected cybercafes in Ogun State, Nigeria. *African Journal of Library, Archives and Information Science*, 20(1), 19-28.
- Adisa, O. T. (2023). The impact of cybercrime and cybersecurity on Nigeria's national security.
- Agbeyangi, A., Makinde, A., & Odun-Ayo, I. (2024). Nigeria's ICT and Economic Sustainability in the Digital Age. *arXiv preprint arXiv:2401.03996*.
- Agbiboa, D. E. (2016). *Frontiers of Urban Survival Everyday Corruption and Precarious Existence in Lagos*. University of Oxford (United Kingdom).
- Akanle, O., & Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, Characterisation and Strategies. *International Journal of Cyber Criminology*, 13(2).
- Aleyomi, M. B. (2020). Nigeria's image crisis: Drivers, efforts and prospects. *African Identities*, 18(1-2), 217-232.
- Aliyu, M. M. (2022). Challenges to investigation and prosecution of corruption cases in Nigeria. *AFJCLJ*, 7, 24.
- Asiri, A. M. (2024). *Corruption and Transnational Organized Crime in the Middle East and North Africa*. St. Thomas University].
- Ayemere, I. (2025). The impact of globalisation on national security in Nigeria. *African Journal of Social Issues*, 8(1), 145-157.
- Ayodeji, G. I. (2018). Illicit Financial Flows, Insecurity and Challenges of Governance in Nigeria. *Studies in Politics and Society*, 271.
- Ayodeji, I. A. (2024). *Fraud Detection and Prevention in the Nigerian Financial Industry* Walden University].
- Bah, A. (2022). Blockchain technology and international money transfers into the Nigerian Remittance market.

- Ballard, B. B. (2023). The Petroleum Industry and Economic Empowerment of Young Adults in Nigeria's Niger Delta Region Walden University].
- Bello, P., Matthew, F., & Cosmas, A. O. (2022). The role of Economic and Financial Crime Commission (EFCC) in combating corruption in Nigeria. *Musamus Journal of Public Administration*, 5(1).
- Bressler, M. S., & Bressler, L. (2019). FRAUDS, EMBEZZLERS, THIEVES, AND OTHER BAD ACTORS: HOW CRIMINALS STEAL YOUR PROFITS AND PUT YOU OUT OF BUSINESS. *Global Journal of Accounting & Finance (GJAF)*, 3(1).
- Button, M. (2021). Hiding behind the veil of action fraud: The police response to economic crime in England and Wales and evaluating the case for regionalisation or a National Economic Crime Agency. *Policing: A Journal of Policy and Practice*, 15(3), 1758-1772.
- Button, M., Gilmour, P. M., Hock, B., Jain, T., Jespersen, S., Lazarus, S., . . . Sabia, J. (2024). Scoping Study on Fraud Centres: Ghana, India and Nigeria.
- Cross, C., Holt, K., & Holt, T. J. (2023). To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud. *Criminology & Criminal Justice*, 17488958221149581.
- David, T. (2018). The adequacy and efficacy of anti-money laundering legislations within the context of electronic banking and informal remittance systems in developing countries with particular reference to Nigeria and South Africa University of London].
- Delorme, T. (2024). Mutual Legal Assistance, a mechanism enabling the prosecution of Transnational Organised Crime: barriers and solutions. *Sorbonne Doctoral Law Review-Revue Doctorale de droit de la Sorbonne*, 7(1).
- Egbo, D. (2022). A Critical Analysis Of The Law Regulating Cybercrimes In Nigeria. Available at SSRN 5136457.
- Eshemo-Omo, I. P., & Obieshi, E. (2024). A Comparative Analysis of Non-Judicial Remedies for Administrative Acts in Nigeria and the United Kingdom. *AGORA Int'l J. Jurid. Sci.*, 18, 183.
- Esoimeme, E. E. (2017). The Nigerian money laundering (prevention and prohibition) bill, 2016: a critical appraisal. *Journal of Money Laundering Control*, 20(1), 79-88.
- Eyo, I., & Okebugwu, G. C. (2024). Analysis of fundamental challenges in the combat of transnational crimes. *International Journal of Research and Innovation in Social Science*, 8(4), 1297-1318.
- Garside, S. M. (2016). Corruption and money laundering: international asset recovery from politically exposed persons in the UK, Nigeria, Russia and China Norwegian University of Life Sciences, Ås].
- Gilbert, M., & Wakefield, A. (2018). Tackling fraud effectively in central government departments:
A review of the legal powers, skills and regulatory environment of UK central government counter fraud teams. *Journal of Financial Crime*, 25(2), 384-399.
- Gilmour, P. M. (2021). Exploring the barriers to policing financial crime in England and Wales. *Policing: A Journal of Policy and Practice*, 15(2), 1507-1521.
- Gundur, R., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., & Mejía, D. D. (2021). Evaluating criminal transactional methods in cyberspace as understood in an international context.
- Igbinomwanhia, O. G. (2021). Human Trafficking and Poverty in South-south Nigeria.
- Ipinlaye, A. (2022). Cybercrime's Toll on Education: Unravelling the Academic Fallout of Internet Fraud among Students.
- Izevbuwa, O. G., & Ngwoke, R. A. (2022). Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention etc) Act 2015 and Other Legislations. *JL Pol'y & Globalization*, 119, 1.

- Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. *Spectrum of engineering sciences*, 3(1), 143-161.
- Kalama, J. T. (2018). ANTI-CORRUPTION WAR IN NIGERIA: REFLECTIONS ON PRESENT AND PAST ADMINISTRATIONS (1999-2018). *INTERNATIONAL INSTITUTE FOR POLICY REVIEW AND DEVELOPMENT STRATEGIES, NIGERIA*+ 234 8174380445,+ 234 767021763, 153.
- Kar, D., & Spanjers, J. (2017). Transnational crime and the developing world. *Global Financial Integrity*, 53, 53-59.
- Laufer, W. S. (2006). *Corporate bodies and guilty minds: The failure of corporate criminal liability*. University of Chicago Press.
- Lazarus, S. (2018). Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. *Criminology, Crim. Just. L & Soc'y*, 19, 63.
- Lazarus, S. (2025). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "black Axe" confraternity. *Deviant Behavior*, 46(4), 456-480.
- Levi, M. (2008). Policing fraud and organised crime. *Handbook of Policing*, 522-552.
- Levi, M. (2015). Money for crime and money from crime: Financing crime and laundering crime proceeds. *European Journal on Criminal Policy and Research*, 21, 275-297.
- Levi, M., & Smith, R. G. (2022). Fraud and pandemics. *Journal of Financial Crime*, 29(2), 413-432.
- Lubin, A. (2025). *Shades of Legal Nuance: A Functional Analysis of Intelligence Doubletalk*. Indiana Legal Studies Research Paper No.
- Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2024). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organised Crime*, 27(3), 364-387.
- Maishanu, M. M. (2024). *Unveiling the Digital Revolution: Cryptocurrency, Blockchain, and the Future of Finance*.
- Mihus, I. (2025). FRAUD HUNTERS AROUND THE WORLD: FIGHTING DECEPTION IN DIFFERENT COUNTRIES. *Socioeconomic relations in the digital society*, 2(56), 115-123.
- Muller, S. R. (2022). Digital Forensic Readiness of Cybercrime Investigating Institutions in Nigeria: A Case Study of the Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force.
- Nawaz, M., & Ebner, J. (2016). *The EU and Terrorism: Is Britain Safer In or Out?* Quilliam.
- Nwabachili, C. O., & Nnoyelu, C. V. (2025). Legality or otherwise for the imposition of cyber security levy in Nigeria. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence*, 16(1), 195-210.
- Nwafor, I. E. (2024). Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps. *African Journal of Legal Studies*, 16(3), 249-270.
- Nwambuko, T. C., Uchegbue, B. C., & Ifedi, F. O. (2022). Financial Crimes Control in Nigeria: an Assessment of the Economic Financial Crimes Commission (EFCC). *Caritas Journal of Management, Social Sciences and Humanities*, 1(1).

- Nwobodo, R. E. (2024). A Critical Examination of 'Yahoo-Yahoo' among Nigerian Youths as a Breach of African Culture and Values. *International Journal of Religious and Cultural Practice*, 9(2), 1-1.
- Nwoke, C. (2023). Regulatory Framework for Alternative Investments in Nigeria. Available at SSRN 4825269.
- Obidimma, E. O., & Ishiguzo, O. (2023). Cybercrime Investigation and Prosecution in Nigeria: The Critical Challenges. *AFJCLJ*, 8, 30.
- Ogundele, A. T., Awodiran, M. A., Idem, U. J., & Anwana, E. O. (2023). Cybercrime activities and the emergence of yahoo boys in Nigeria. 2023 International Conference On Cyber Management And Engineering (CyMaEn),
- Ojedokun, U. A., & Ilori, A. A. (2021). Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria. *International Journal of Criminal Justice*, 3(1), 99-122.
- Ojolo, T. L. (2020). A criminological investigation into the lived experiences of cybercrime perpetrators in southwest Nigeria University of KwaZulu-Natal, Howard College].
- OKEBUGWU, G. C. (2024). THE ROLE OF INTERNATIONAL PROTECTIVE MECHANISMS INCURBING TRANSNATIONAL CRIMES. *PPLRUNLAW REVIEW*, 3(1).
- Okorie, C., Udoh, E., & Bassey, O. B. (2023). Mirroring the developmental challenges of oil-rich Nigeria within the context of resource curse/Dutch disease and paradox of plenty. *TIJER-International Research Journal*, 10(4), 818-834.
- Olayiwola, P. (2024). Tackling Modern Slavery or Worsening Vulnerability? UK's Modern Slavery Agenda in Nigeria. *International Criminology*, 1-9.
- Olujobi, O. J., & Yebisi, E. T. (2023). Combating the crimes of money laundering and terrorism financing in Nigeria: a legal approach for combating the menace. *Journal of Money Laundering Control*, 26(2), 268-289.
- Oluku, O., & Ene, W. R. P. (2024). THE SOCIAL SUPPORT SYSTEMS OF YAHOO YAHOO BUSINESS IN NIGERIA. *Journal of Social Theory and Research (JOSTAR) Volume*, 4(1).
- Onogwu, P. G., & Lawal, O. (2024). THE NEXUS BETWEEN CORRUPTION AND RESOURCE THEFT: IMPLICATIONS FOR NATIONAL SECURITY IN RESOURCE-RICH NATIONS. *The American Journal of Political Science Law and Criminology*, 6(11), 42-51.
- Onwudiwe, I. D. (2017). Transnational crimes: The case of advanced fee fraud in Nigeria. In *Pan-African issues in crime and justice* (pp. 99-120). Routledge.
- Onwughalu, V. C. (2023). The Works and Lifestyles of Nigerian Celebrities as Drivers of Crimes Amongst the Youth and Young People. *ANSU Journal of Arts And Social Sciences*, 10(2), 114-130.
- Otoide, L. E. (2019). Nature and management of human trafficking: The Nigerian Edo people's experience. In *Crime, Law and Society in Nigeria* (pp. 123-157). Brill.
- Reurink, A. (2019). Financial fraud: A literature review. *Contemporary topics in finance: A collection of literature surveys*, 79-115.
- Rivera-Williams, J. (2025). A Multiple Perspective Analysis on Urban Poverty in Developing Nations: A Case Study on Nigeria, Colonial Implications, and Modern-Day Outcomes.
- Ryder, N. (2024). To report or not to report? An analysis of the relationship between defence against terrorism financing suspicious activity reports and fraud in the United Kingdom. In *Financial Crime, Law and Governance: Navigating Challenges in Different Contexts* (pp. 169-202). Springer.

- Soares, A. B., Lazarus, S., & Button, M. (2025). Love, lies, and larceny: One hundred convicted case files of cybercriminals with eighty involving online romance fraud. *Deviant Behavior*, 1-24.
- Tade, O., & Adeniyi, O. (2020). Dimensions of electronic fraud and governance of trust in Nigeria's cashless ecosystem. *International Journal of Offender Therapy and Comparative Criminology*, 64(16), 1717-1740.
- Ukachukwu, C. C., & Naetor, V. M. (2020). Value Deficiency, Employment Generation and Crime among Youths in Nigeria: An Overview. *Asian Research Journal of Arts & Social Sciences*, 11(2), 13-24.
- Umoh, E. (2025). Unemployment as a Driver of Crime: Exploring the Roles of Poverty, Youth Restiveness, and Effectiveness of Government Interventions in Emerging Economies. Unemployment as a Driver of Crime: Exploring the Roles of Poverty, Youth Restiveness, and Effectiveness of Government Interventions in Emerging Economies (February 12, 2025).
- Vargas, V. M. (2019). The new economic good: Your own personal data. An integrative analysis of the Dark Web. *Proceedings of the International Conference on Business Excellence*,
- Wariboko, O. P. C., & Nwanyanwu, F. C. (2024). The Dark Side of Connectivity: A Socio-Ethical Exploration of Internet Fraud and Nigerian Youth. *Àgídìgbo: ABUAD Journal of the Humanities*, 12(1), 89-104.
- Watson, C. (2017). Information and intelligence sharing in the fight against fraud and intellectual property crime: challenges and strategies for professional practice [University of Portsmouth].

APPENDIX 1

Nigeria: History, People and Culture

Nigeria's cultural and political identity draws from some of the most influential precolonial states in Africa. The Nok civilisation (c. 1500 BC–500 AD), known for its terracotta art, is one of the earliest complex societies in Sub-Saharan Africa and influenced later regional cultures. The medieval period, powerful kingdoms had emerged, including the Benin Empire, famed for its bronze artistry and administrative sophistication, and the Yoruba city-states of Ife and Oyo, which developed advanced political systems and cultural traditions. In the north, the Kanem-Bornu Empire and later the Sokoto Caliphate (established in 1804 by Usman dan Fodio) became major Islamic powers and centres of trade, education, and governance.

The modern Nigerian state was created in 1914 when the British merged the Southern and Northern Protectorates. Colonial administrators employed indirect rule, relying on traditional rulers in the north and restructured chiefs in the south, which both preserved and distorted indigenous systems. Economic priorities under colonialism focused on cash crops and resource extraction, laying foundations for uneven development. Nigeria became formally independent on 1 October 1960, with a federal structure recognising the diversity of its regions. Post-independence, the country faced political turbulence including military coups and a devastating civil war (1967–1970), yet it retained its status as one of Africa's most strategically significant states).

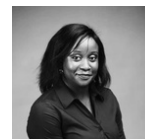
Nigeria is the most populous country in Africa, with an estimated 230 million people in 2025. It is also one of the youngest populations globally, with more than 50 percent under the age of 15. Nigeria is home to more than 250 ethnic groups and over 500 languages, with the Hausa-Fulani, Yoruba, and Igbo constituting the three largest groups. Despite its immense oil and gas wealth, Nigeria grapples with challenges of poverty, unemployment, and insecurity, while also driving Africa's largest economy, contributing over USD 477 billion to GDP in 2022. This blend of rich history, cultural diversity, and economic importance makes Nigeria central to understanding both the opportunities and risks of West Africa.

APPENDIX 2

Terminology Associated with Fraud in Nigeria

- **Azah/aza/house/ile:** Bank account
- **BM:** Blackmail
- **Bombing:** The practice of messaging large numbers of online accounts to find potential victims.
- **Bread:** money
- **Cash out:** Money successfully gotten from a scam.
- **Client:** The target/victim of the scam (often pronounced without the 't').
- **Format:** The schematics of the job (This is the comms or script that consists of replies and convincing quotes to deceive people).
- **Grinding:** chatting with a potential victim.
- **Hustle Kingdom (HK):** A hostel where recruits are trained, loyalties are obtained, and victims are targeted
- **Kpaco:** credit/bank cards/gift cards
- **Mama:** Target female (mostly for romance fraud)
- **Maye/maga/mugu:** client that is either supposed to be scammed or who is making the deposit
- **Jonzing:** This is used when a prospect/target victim has discovered the pranks of the yahoo boys but pretends to play along.
- **Leaf/paper:** Cheque/ money order/cashier's check
- **Loader:** the person running the operation or someone skilled at loading stolen credit cards into accounts or payment systems.
- **Picker:** the person needed to withdraw money from the bank or cash a gift card
- **442:** Percentage of takings for a job. It means 40% for the people who do the work, 40% for the account receiving the funds, and 20% for the middlemen. It derives from football speak.
- **Taxo:** Tax refund fraud (primarily used in the US)

CONTRIBUTORS



Dr Andrew Agbo-Madaki is an Adjunct Professor of Cybersecurity and Intelligence Engineering at the Ontario College of Technology. He holds a PhD in Security & Strategic Studies (with a focus on Cyber Warfare), an MSc in Computer Forensics (specialisation in Cybersecurity), and a BSc in Sociology (with a focus on criminology and sentencing patterns in lower courts). Andrew is responsible for the World Bank's Cybersecurity Capability Building for Africa research, as well as Communications for the World Bank SEEFOR project and UNICEF's funded research, CASTLE, on securing schools in Nigeria, among other National projects. Andrew was the Head of Operations at the Nigeria Emergency Coordination Centre, where he was responsible for coordinating the Humanitarian Development Peace Nexus. He currently provides capacity-building services to several government agencies, including the National Counter Terrorism Centre (NCTC), the Federal High Court, the Nigeria Police Force (NPF), the Nigerian Maritime Administration and Safety Agency (NIMASA), and the National Crime Agency UK, among others.

Ms Chioma Agwuegbo is a communications for development expert, researcher, and feminist advocate whose work sits at the intersection of gender, technology, and human rights. She is the Executive Director of TechHerNG, a social impact organisation she founded to help women and girls access, understand, and use technology safely. Her research portfolio combines academic inquiry with applied, evidence-based advocacy, shaping conversations on digital rights, technology-facilitated gender-based violence (TFGBV), and feminist solidarity in Africa. Her educational background enhances her applied research; she is currently pursuing a doctoral degree in Development Communication, with a focus on feminist responses to technology-mediated violence and discourse ethics. She holds an MA in Social Media, examining how digital tools can both advance and threaten democratic participation. She has a first degree in Mass Communication. Chioma has researched TFGBV in West Africa for Equality Now, young feminist movements in West Africa for the Ford Foundation, led civic space mapping for the Joint Civic Defence Fund, and produced research for DFID, the MacArthur Foundation, among others. Chioma is a 2024 Ford Global Fellow and Transform Norms Fellow, and sits on the Boards of PLAN International Nigeria and WACSI Nigeria.

Dr Fola Aina is a Political Scientist and international security analyst. He is currently a lecturer in the Political Economy of Violence, Conflict and Development, Department of Development Studies, School of Oriental and African Studies (SOAS), University of London, United Kingdom. He completed a second master's degree in African studies at the University of Oxford, having earlier obtained a Masters' degree in International Development Policy from Seoul National University, South Korea. He holds a doctorate in Leadership Studies, with a focus on security and development, from King's College London, United Kingdom. His research interests encompass peace, security, and development, as well as leadership in national security policy decision-making, military operations, international security, grand strategy, terrorism, insurgency, and extremism. A recipient of multiple awards, including the prestigious General Lamine Cissé Young Researcher Award by Partners West Africa/Geneva Centre for Security Sector Governance, and the Hans. J Morgenthau Fellowship on Grand Strategy, awarded by the Notre Dame International Security Centre, University of Notre Dame. His works have been published in several reputable international peer-reviewed journals, including African Security, Armed Forces & Society, amongst others.

