Economic and Financial Crimes Commission and the fight against internet fraud in Nigeria

Kalu, Ebei Kingsley

Department Of Political Science And Diplomacy, University Of Nigeria, Nsukka

Abstract

Internet fraud, popularly known in Nigeria as "Yahoo-Yahoo," has grown from a peripheral nuisance into a threat that shapes the country's economic performance, banking stability, and international reputation. This article re-examines the role of the Economic and Financial Crimes Commission (EFCC) in combating internet fraud in Nigeria, updating the evidentiary base to 2025 to capture the effect of recent legal reforms, notably the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024. Guided by Deterrence Theory and a time-series research design, the study relies on documentary sources, EFCC annual disclosures, Nigeria Inter-Bank Settlement System (NIBSS) fraud reports, Nigeria Data Protection Commission (NDPC) briefings, and the United States Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) reports, analysed through qualitative content analysis. The findings show that the EFCC's technological capacity, including the Integrated Intelligence and Investigation System (I-24/7), forensic laboratories, and biometric surveillance tools, has improved detection and prosecution, with convictions rising from 103 in 2015 to a record 4,111 in 2024 and recoveries exceeding ₦364.6 billion in the same year. However, the study finds that the EFCC's regulatory framework continues to rely overwhelmingly on reactive, force-based interventions, mass arrests and raids, rather than preventive, structural reforms, even as internet fraud arrests remained the single largest category of EFCC enforcement action in 2024. The persistence of resource constraints, jurisdictional overlaps with the Nigeria Police Force's Cybercrime Unit and the Nigeria Data Protection Commission, and the socio-economic drivers of youth involvement in cybercrime continue to blunt deterrence. The article concludes that a hybrid strategy combining sustained technological investment, harmonised inter-agency regulation, and socio-economic intervention for at-risk youth is required for durable results, and offers policy recommendations accordingly.

Keywords: Economic and Financial Crimes Commission, internet fraud, cybercrime, Nigeria, deterrence theory, regulatory framework, Cybercrimes Act 2024

Introduction

The internet has transformed global commerce, communication, and governance, but it has also become a vector for economic crime (Longe & Chiemeke, 2006). Nigeria's engagement with the internet, dating to the licensing of the country's first internet service providers in 1996, arrived alongside a parallel and less welcome development: the migration of long-standing advance-fee fraud schemes, historically conducted through letters and telex,

and criminalised under Section 419 of the Nigerian Criminal Code, onto digital platforms (Tade & Aliyu, 2011). Over the following three decades, "internet fraud" broadened to include phishing, identity theft, romance scams, business email compromise, cryptocurrency fraud, and, more recently, artificial-intelligence-enabled deception such as voice cloning (Federal Bureau of Investigation [FBI], 2026).

The reputational and economic costs have been substantial. Nigeria has for years featured among the countries most frequently cited in the FBI's Internet Crime Complaint Center (IC3) annual reports as either a source or a destination of fraudulent wire transfers; in the IC3's 2025 annual report, Nigerian victims alone filed 1,219 complaints, while global cybercrime losses reported to the IC3 reached $20.877 billion, a 26 percent increase over 2024 (FBI, 2026). Domestically, the Nigeria Inter-Bank Settlement System (NIBSS) recorded that financial institutions lost ₦52.26 billion to fraud and cyber-enabled financial crime in 2024, up sharply from ₦17.67 billion in 2023, before falling to roughly ₦25.85 billion in 2025 as banks intensified fraud-detection investment (NIBSS, 2026, as cited in Vanguard, 2026). The Nigeria Data Protection Commission (NDPC) separately estimated that the country experiences over 4,000 cyberattacks weekly and accounts for approximately 45 percent of all reported cybercrime incidents in Africa (NDPC, 2026).

It is against this backdrop that the Economic and Financial Crimes Commission (EFCC), established in 2003 pursuant to the EFCC (Establishment) Act 2004 in response to the Financial Action Task Force's (FATF) blacklisting of Nigeria, has positioned the suppression of internet fraud as a central pillar of its mandate, alongside its historic focus on political corruption and money laundering. Since 2015, and particularly since the appointment of successive EFCC chairmen with an explicit cybercrime remit, the Commission has scaled up mass arrest operations, invested in digital forensics, and, from 2024, operated under an amended legal framework, the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, signed into law on 28 February 2024 (Mondaq, 2024). This study updates and extends an earlier documentary evaluation of the EFCC's performance, incorporating data through 2025, to assess whether the Commission's technological and regulatory interventions have translated into a measurable reduction in internet fraud, or merely into higher volumes of enforcement activity.

Nigeria's anti-cybercrime effort presents an apparent paradox. On one hand, the EFCC now reports record enforcement statistics: 4,111 convictions and over ₦364.6 billion in

recoveries in 2024 alone, the highest in the Commission's twenty-year history (Channels Television, 2025; Vanguard, 2025). On the other hand, internet fraud (2,588 recorded arrests) remained by a wide margin the most common single crime category prosecuted by the EFCC in 2024 (Businessday, 2025), and the EFCC's own chairman has publicly lamented that a majority of Nigerian university students are believed to have some involvement in cybercrime (Leadership, 2025). This suggests that enforcement volume has grown without a commensurate decline in the underlying incidence of the crime. Existing academic literature on the EFCC's anti-fraud performance largely predates the 2024 legal reform and the post-pandemic surge in digitally enabled financial crime, relying on statistics that end around 2019–2021 (see, for example, Idris, 2021; Adebayo, 2021). There is consequently a need to re-examine, with more current data, whether the EFCC's application of technology has genuinely improved detection, and whether its regulatory and enforcement posture, still heavily weighted toward reactive raids and mass arrests rather than preventive regulation, discourages or merely displaces internet fraud. This study addresses that gap by asking two central research questions: (i) Has the EFCC's application of technological solutions improved the detection of cybercrime in Nigeria between 2015 and 2025? (ii) Does the EFCC's regulatory framework rely on the use of force rather than structural prevention in the fight against internet fraud in Nigeria over the same period?

The broad objective of this study is to evaluate the role of the EFCC in combating internet fraud in Nigeria between 2015 and 2025. The specific objectives are to: (i) assess the extent to which the EFCC's technological solutions have improved the detection of cybercrime in Nigeria; (ii) examine whether the EFCC's regulatory framework has encouraged reliance on the use of force rather than preventive regulation in the fight against internet fraud; and (iii) proffer evidence-based recommendations for strengthening the EFCC's institutional response to internet fraud.

Literature Review

Internet fraud, used interchangeably in Nigerian scholarship with "cybercrime" and colloquially termed "Yahoo-Yahoo," refers to the use of internet-connected devices and networks to obtain money, property, or information from victims through deception (Aransiola & Asindemade, 2011; Ibrahim, 2016). It encompasses advance-fee fraud, phishing, identity

theft, romance scams, business email compromise, cryptocurrency-investment fraud, and, increasingly, AI-assisted impersonation (FBI, 2026). Scholars distinguish between "computer-focused" crimes, in which the computer system itself is the target (hacking, malware deployment, denial-of-service attacks), and "computer-assisted" crimes, in which digital tools merely facilitate an otherwise familiar offence such as fraud or theft (Aghatise, 2006; Higgins, 2009). Nigerian internet fraud has historically clustered in the second category, evolving directly from the pre-digital "419" advance-fee scam, though the growing prevalence of business email compromise, ransomware-adjacent extortion, and AI-generated deep-fake impersonation indicates a gradual shift toward more technically sophisticated, computer-focused methods (FBI, 2026).

The Economic and Financial Crimes Commission is Nigeria's primary statutory agency for investigating and prosecuting financial crimes, established by the EFCC (Establishment) Act 2004 in direct response to the Financial Action Task Force's designation of Nigeria as a non-cooperative country in the fight against money laundering. It operates today alongside a wider regulatory ecosystem that includes the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024, the Nigeria Data Protection Act 2023 and its 2025 General Application and Implementation Directive, the Money Laundering (Prevention and Prohibition) Act 2022, the Advance Fee Fraud and Other Related Offences Act 2006, and sector-specific instruments such as the Central Bank of Nigeria's Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions (2022). This multiplicity of overlapping instruments is itself a recurring theme in the literature on Nigeria's anti-fraud architecture, with several commentators noting that institutional proliferation has not always been matched by clear delineation of mandate (Effoduh, 2016; Ogwezzy, 2012).

EFCC's Application of Technological Solutions and Detection of Cybercrime

Technology adoption is widely presented in the literature as central to modern law-enforcement capacity (Saragih & Siahaan, 2016; Purba, 2018). The EFCC has, over the review period, deployed several technological tools in support of detection and investigation. The Integrated Intelligence and Investigation System (I-24/7), developed with international partners, enables real-time financial intelligence gathering and cross-referencing of suspect data (Aderibigbe, 2019). The Commission also operates forensic laboratories for digital evidence recovery from computers, mobile devices, and cloud accounts, and has progressively incorporated biometric identification, leveraging the Bank Verification Number (BVN) and

National Identification Number (NIN) frameworks, into its investigative workflow (Hamu Legal, 2024). These tools featured prominently in a string of large-scale operations between 2024 and 2025: the arrest of 792 suspected internet and investment fraudsters at a single Victoria Island address in December 2024; the arrest of 105 suspects, including four Chinese nationals, in a "hotel review job scam" targeting United Kingdom victims in January 2025; and a series of sting operations across Makurdi, Abuja, and other zonal commands that together accounted for internet fraud remaining the leading category of EFCC arrests in 2024, with 2,588 recorded cases, ahead of general fraud (815) and currency racketeering (168) (Businessday, 2025; EFCC, 2025; Nigerian Observer, 2024).

Comparatively, international cooperation frameworks such as Europol's Joint Cybercrime Action Taskforce (J-CAT) and the United Nations Office on Drugs and Crime's (UNODC) Comprehensive Study on Cybercrime have emphasised that no single national agency can address internet fraud in isolation, given the cross-border movement of funds, mule accounts, and offenders (Europol, 2021; UNODC, 2013). The EFCC's participation in the first-ever Regional Cybercrime Summit for West Africa, convened in October 2024 in partnership with UNODC, the Economic Community of West African States (ECOWAS), and Microsoft, represents a recent step toward this internationally recommended model of cooperative, technology-supported enforcement (Vanguard, 2025). Whether this cooperation translates into sustained joint operations, rather than one-off summitry, remains an open question that this study's documentary sources cannot fully resolve, and is flagged here as an area for further monitoring rather than settled fact.

Despite these gains, the literature and recent commentary converge on the view that detection capacity has not kept pace with the sophistication or scale of the threat. The NDPC reported in 2026 that Nigeria records over 4,000 cyberattacks weekly and that financial losses attributable to cybercrime reached approximately ₦12 billion in 2024 (NDPC, 2026), a figure that sits uneasily alongside NIBSS's considerably higher estimate of ₦52.26 billion in bank-specific fraud losses for the same year (NIBSS, 2026), a discrepancy that itself illustrates the absence of a single, authoritative national cybercrime-loss metric against which EFCC performance can be benchmarked. Purba (2018) and Rahim (2018) had earlier argued that limited human resources, infrastructure, and specialist technical staff constrain law-enforcement agencies in developing countries; this constraint remains visible in Nigeria, where cybercriminals increasingly exploit artificial intelligence for voice cloning and deep-fake-enabled romance and investment scams, a trend the FBI's 2025 Internet Crime Report

associates with more than 22,000 complaints and nearly $900 million in global losses (FBI, 2026) but which Nigerian law-enforcement technology has yet to be systematically evaluated against.

EFCC's Regulatory Framework and Use of Force in the Fight Against Internet Fraud

The EFCC's regulatory architecture rests on the EFCC (Establishment) Act 2004, the Money Laundering (Prevention and Prohibition) Act 2022, the Advance Fee Fraud Act 2006, and, since February 2024, the amended Cybercrimes Act. The 2024 amendment introduced several changes directly relevant to internet fraud enforcement: it mandated the establishment of sectoral Computer Emergency Response Teams (CERTs) and Security Operations Centres, required service providers to retain traffic and subscriber data for two years in line with the Nigeria Data Protection Act 2023, expanded corporate and third-party liability for cybercrime facilitation beyond the financial sector, clarified and operationalised the 0.5 percent National Cybersecurity Levy on electronic transactions, and repealed the earlier, widely criticised Section 48(4) provision permitting passport cancellation for convicted persons (Hamu Legal, 2024; AB Legal Practitioners, 2025; Mondaq, 2024).

Notwithstanding this legislative modernisation, a substantial body of commentary, echoing the "use of force" concern at the centre of this study, holds that enforcement in practice remains dominated by large-scale physical raids and mass arrests rather than the preventive, intelligence-led regulation the amended Act envisions. The EFCC's most publicised actions in 2024–2025, including raids on hotels, estates, and residential compounds in Lagos, Port Harcourt, Abuja, Benin City, and Owerri, typically resulted in the arrest of anywhere from a handful to several hundred suspects at a time, with released statements emphasising the number of suspects apprehended and assets recovered (laptops, vehicles, cash) rather than the disruption of the criminal networks or infrastructure enabling the fraud (Nigerian Observer, 2024; EFCC, 2025). Civil-society and legal commentary has also raised concern that expanded surveillance powers under the 2024 amendment, including interception of communications without a court order in "urgent" cases, and vague statutory language proscribing "false" or "insulting" online content, have occasionally been applied against government critics rather than internet fraudsters, a pattern documented in the arrests of activists Dele Farotimi and Olamide Thomas in late 2024 (NALTF, 2025; Vanguard, 2025). This dual pattern, an intensifying reliance on mass, force-based raids for internet fraud alongside contested use of the same legal instruments against dissent, supports the study's proposition that Nigeria's

regulatory framework has yet to shift decisively from reactive coercion toward preventive, rights-respecting regulation.

Prior Nigerian studies on the EFCC and internet fraud (e.g., Aderibigbe, 2019; Idris, 2021; Adebayo, 2021) were conducted using data that, at the time of writing, extends only to approximately 2019–2021 and therefore could not capture either the 2024 legislative reform or the post-2023 surge in digitally-mediated fraud linked to expanded e-payment volumes, artificial intelligence, and cryptocurrency. This study addresses that temporal gap by incorporating EFCC, NIBSS, NDPC, and FBI/IC3 data through 2025–2026, thereby providing a more current empirical basis for assessing the Commission's performance under the amended legal regime.

Theoretical Framework

This study adopts Deterrence Theory, associated with Beccaria and Bentham and developed in contemporary criminology by Nagin (2013) and Apel and Nagin (2011), as its analytical lens. Deterrence Theory posits that the likelihood of criminal behaviour is inversely related to the certainty, severity, and swiftness of punishment. Applied to internet fraud in Nigeria, the theory generates a testable expectation: as the EFCC's conviction rate, sentence severity, and speed of prosecution rise, the incidence of internet fraud should fall. The theory has, however, been qualified by McMahon, Davidson, and Messier (2021), who argue that deterrence operates differently in cyberspace than in physical criminal contexts because of the perceived anonymity of digital offenders, the low probability of detection relative to physical crime, and the transnational character of much cyber-enabled fraud, all of which weaken the certainty component of deterrence. This qualification is directly relevant to Nigeria, where despite record 2024 conviction numbers, internet fraud arrests simultaneously reached their own record volume, suggesting that increased certainty of punishment for those caught has not yet translated into a broader deterrent effect across the wider population of potential offenders, consistent with the EFCC chairman's own public concern about the scale of youth involvement in cybercrime (Leadership, 2025).

Deterrence Theory is complemented in this study by insights from Routine Activity Theory, which holds that crime occurs at the convergence of a motivated offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979, as applied to cybercrime by Aiken, Bach, Jahera, & Colella, 2018). The rapid expansion of Nigeria's digital economy,

e-payment volumes exceeding ₦1 quadrillion in 2024, fintech adoption growing from 255 companies in January 2024 to 430 by February 2025, and near-universal smartphone-based banking access, has multiplied the pool of "suitable targets" available to offenders, plausibly offsetting gains in guardianship (detection and prosecution capacity) achieved through EFCC technological investment. The two theories together therefore offer a coherent explanation for the study's central empirical puzzle: rising convictions coexisting with a rising, rather than falling, absolute volume of internet fraud arrests.

Methodology

The study adopts a time-series research design, appropriate for evaluating trends and relationships between variables over an extended period (Kerlinger, 1977; Asika, 2009). Data were collected through the documentary method, drawing on secondary sources including EFCC annual and press disclosures, NIBSS fraud reports, NDPC briefings, FBI/IC3 annual reports, Nigerian and international news media, and previously published academic literature (Oguonu & Anugwom, 2014; Bailey, 1994). Data were analysed using qualitative content analysis (Asika, 2006; Sandelowski, 2000), which permits systematic identification of patterns and themes, in this case, trends in arrests, prosecutions, convictions, and asset recovery, and the qualitative characterisation of the EFCC's regulatory posture as either preventive or force-based, across the compiled documentary evidence. The independent variables are the EFCC's application of technological solutions and its regulatory framework; the dependent variable is the detection and management of internet fraud in Nigeria, operationalised through arrest, prosecution, conviction, and recovery statistics. Given the reliance on secondary, largely government-sourced data, the study acknowledges the limitation that official statistics may be shaped by reporting incentives and definitional inconsistencies across agencies (illustrated, for instance, by the divergence between NDPC and NIBSS loss estimates for 2024 discussed above); triangulation across multiple independent sources was used to mitigate this limitation wherever possible.

The documentary sample was purposively bounded to the period 2015–2025/2026, with 2015 selected as a starting point because it coincides with the enactment of Nigeria's first dedicated Cybercrimes Act, and 2025–2026 representing the most recent period for which verifiable EFCC, NIBSS, NDPC, and FBI/IC3 data were publicly available at the time of writing. Priority was given to primary institutional sources (EFCC press releases, NIBSS and NDPC reports, the FBI's IC3 annual report) over secondary media commentary wherever both

were available, with media reports used chiefly to corroborate, contextualise, or supply operational detail (dates, locations, suspect counts) not contained in institutional disclosures. As with any documentary design relying substantially on institutional self-reporting, the study cannot fully rule out the possibility that reported enforcement statistics overstate substantive impact relative to publicity value; this is treated as an interpretive caution throughout the discussion in Section 4 rather than as a fatal design flaw, consistent with the broader methodological literature on the use of official crime statistics (Tombs & Whyte, 2013).

Results and Discussion

Technological Solutions and Detection Outcomes, 2015–2025

Table 1 summarises the trajectory of EFCC conviction outcomes from 2015 to 2024, drawing on figures reported in EFCC disclosures and independent Nigerian media analysis.

Table 1: EFCC Convictions and Asset Recovery, Selected Years (2015–2024)

Year	Convictions	Notable Recovery Data
2015	103	Advance-fee fraud constituted 54% of investigations
2016	194	—
2017	189	—
2018	312	—
2019	1,280	—
2020	976 (COVID-19-affected)	—
2021	2,220	—
2023	3,175	$43.8m and multiple foreign currencies recovered in the reporting year
2024	4,111 (record high)	₦364.6 billion, $214.5 million, and over 750 duplexes/apartments recovered, the largest single-year recovery in EFCC history

Sources: EFCC (2024, 2025); Channels Television (2025); Vanguard (2025); allAfrica (2025).

The upward trajectory in convictions is consistent with expanded technological capacity: the I-24/7 platform, forensic digital-evidence laboratories, and BVN/NIN-linked biometric verification have collectively shortened the investigative cycle from petition to prosecution. Zonal-level data corroborate this: in 2024, Lagos Zonal Directorate alone recorded 685 convictions, followed by Enugu (516), Ibadan (501), and Benin (412), reflecting geographically distributed capacity rather than a single headquarters-driven effort (Vanguard,

2025). The Commission also received 15,724 petitions across all zonal directorates in 2024, indicative of a substantial and rising caseload (Vanguard, 2025).

However, arrest data complicate a simple narrative of technological success. Of all crime categories investigated by the EFCC in 2024, internet fraud accounted for 2,588 arrests, more than three times the number for general fraud (815) and more than fifteen times the number for currency racketeering (168) (Businessday, 2025). This indicates that while detection and prosecution capacity has grown, the underlying rate of internet fraud offending, or at least of apprehension-worthy internet fraud activity, has grown at least as fast, if not faster. The EFCC's own chairman, Ola Olukoyede, has been quoted publicly asserting that a large majority of Nigerian tertiary-education students have some involvement in cybercrime (Leadership, 2025), a claim that, whatever its precise empirical basis, signals institutional concern that detection gains have not been matched by a reduction in the pool of potential offenders.

Financial Intelligence and Transaction Monitoring

Financial intelligence and transaction-monitoring infrastructure sits at the interface between the EFCC, the Central Bank of Nigeria (CBN), and the Nigerian Financial Intelligence Unit (NFIU). The BVN and NIN linkage requirements, reinforced by the 2024 Cybercrimes Amendment Act and CBN implementation circulars, obligate all Tier 1 account holders to complete biometric verification, a measure intended to close the anonymity gap that both enables internet fraud and frustrates its detection (Hamu Legal, 2024). NIBSS transaction-monitoring data show that Nigeria's e-payment volumes crossed ₦1 quadrillion in 2024, alongside a rise in fraud losses from ₦17.67 billion in 2023 to ₦52.26 billion in 2024, a 196 percent increase, before falling by more than half to approximately ₦25.85 billion in 2025 as banks invested in artificial-intelligence-based fraud detection and real-time monitoring, with fraud case counts declining from 70,111 in 2024 to 67,518 in 2025 (Vanguard, 2026). This 2025 decline is one of the more encouraging findings of this update: it suggests that financial-sector-level monitoring investment, rather than EFCC enforcement action alone, has begun to yield a measurable reduction in successful fraud incidents, even as EFCC arrest volumes for internet fraud remained high. The Nigeria Cybersecurity Levy, set at 0.5 percent of the value of electronic transactions by designated businesses under Section 44 of the amended Cybercrimes Act, is intended to fund a National Cybersecurity Fund supporting exactly this kind of monitoring infrastructure, although its implementation was briefly suspended in May

2024 after the House of Representatives directed the CBN to withdraw its initial implementation circular pending clearer guidance (Mondaq, 2024).

Cybercrime Reporting Channels in Nigeria

Nigeria's cybercrime reporting architecture includes the Nigeria Computer Emergency Response Team (NgCERT) Cybercrime Reporting Portal, the Nigeria Police Force Cybercrime Unit hotline, and the EFCC's own Tip-Off platform, each designed to lower the barrier for citizens and institutions to report suspected fraud (NgCERT, 2021; EFCC, 2019). The 2024 Cybercrimes Amendment Act adds a mandatory dimension to this architecture, requiring any person or organisation that detects an intrusion, attack, or disruption to report it to the National CERT or an appropriate sectoral CERT within 72 hours (Hamu Legal, 2024), aligning Nigeria's domestic reporting timeline with international norms such as the European Union's General Data Protection Regulation. Internationally, the FBI's IC3 portal has also become a significant, if indirect, source of intelligence on Nigeria-linked fraud: the IC3's 2025 Annual Report identifies Nigeria among the jurisdictions most frequently associated with the destination of fraudulent wire transfers globally, alongside hubs in East Asia and Latin America (FBI, 2026; Businessday, 2026). The layering of domestic mandatory-reporting obligations with international complaint data such as IC3's offers the EFCC an expanding intelligence base, though the extent to which this expanded intake has been operationally integrated into EFCC casework remains, on the evidence reviewed, unclear and warrants further study.

The Effects of the Regulatory Framework: Arrests, Convictions, and the Persistence of Force-Based Enforcement

Table 2 sets out illustrative EFCC internet-fraud enforcement actions drawn from late 2024 and early 2025, demonstrating the continued centrality of mass, force-based raids to the Commission's operational model even after the 2024 legislative reform.

Table 2: Selected Large-Scale EFCC Internet Fraud Operations, 2024–2025

Date	Location	Suspects Arrested	Notes
November 21, 2024	Makurdi, Benue State	15	Sting operation; identity theft and phishing

November 27, 2024	Makurdi, Benue State	10 convicted	Impersonation of professionals online
December 10, 2024	Victoria Island, Lagos	792	Largest single raid of the period; investment and internet fraud
January 9, 2025	Gudu, Abuja	105 (4 Chinese, 101 Nigerian)	"Hotel review job scam" targeting UK victims

Sources: Nigerian Observer (2024); EFCC (2025); Businessday (2025).

These operations, together with the 4,111 total convictions and ₦364.6 billion in recoveries recorded in 2024 (Channels Television, 2025), represent the EFCC's strongest enforcement year to date. Yet the qualitative character of these actions, coordinated raids on residential compounds, hotels, and event venues resulting in mass arrest, followed by prosecution, supports this study's contention that Nigeria's approach remains predominantly reactive and coercive rather than preventive. This is not to dismiss the deterrent value of visible, well-publicised enforcement; Deterrence Theory would predict some effect from the sheer increase in the certainty and visibility of punishment. But the EFCC's regulatory framework, even as amended in 2024, continues to authorise and reward apprehension over disruption of the criminal business model itself (payment rails, mule-account networks, and the digital infrastructure, VPNs, spoofed identities, and increasingly AI tools, that sustain fraud). Additionally, the amended Act's expanded surveillance and content-moderation provisions have generated controversy over selective or overbroad application against government critics rather than internet fraud suspects (NALTF, 2025), a development that, if it continues, risks diverting institutional and public trust away from the Act's stated anti-fraud purpose.

Cross-institutional coordination remains a further constraint. The EFCC, the Nigeria Police Force Cybercrime Unit, the NDPC, the NFIU, and the CBN each hold overlapping but not fully harmonised mandates over aspects of cyber-enabled financial crime, and, as illustrated by the divergent 2024 loss estimates from NDPC (₦12 billion) and NIBSS (₦52.26 billion), do not yet operate from a single shared evidentiary base (NDPC, 2026; NIBSS, 2026). This fragmentation complicates both the measurement of the EFCC's marginal impact and the design of an integrated national response.

Challenges Facing the EFCC

Several persistent challenges qualify the EFCC's documented gains. First, resource constraints, in staffing, forensic infrastructure, and specialist training, remain a recurring theme in both older (Purba, 2018) and more recent commentary, particularly as offenders adopt artificial intelligence tools that outpace existing detection capability (FBI, 2026). Second, jurisdictional and definitional overlaps among the EFCC, the Nigeria Police, the NDPC, and the NFIU create duplication and gaps in accountability. Third, the transnational character of much internet fraud, evident in the involvement of foreign nationals in Nigeria-based scam operations (for example, the Chinese nationals arrested in the January 2025 Abuja raid) and in the reported deportation of scores of foreign nationals convicted of cyber-related offences (allAfrica, 2025), requires international cooperation that remains uneven. Fourth, the socio-economic drivers of youth involvement in cybercrime, linked in the literature to unemployment and constrained legitimate opportunity (Ojedokun & Eraye, 2012), have not been substantially addressed by an enforcement-first strategy, a concern the EFCC's own leadership has publicly voiced. Finally, the controversial application of expanded surveillance powers under the amended Cybercrimes Act to government critics, rather than fraud suspects, risks eroding the legitimacy that effective deterrence requires (NALTF, 2025).

Discussion: Revisiting the Study's Propositions

Returning to the two propositions advanced in Section 1.5, the evidence assembled above offers partial, rather than unqualified, support for P1 (that technological solutions have improved detection). Convictions and recoveries have risen dramatically in absolute and record-breaking terms, and the 2025 decline in NIBSS-reported bank fraud losses, alongside the fall in fraud case counts from 70,111 to 67,518, is the clearest evidence in the dataset of a genuine, technology-associated improvement in outcomes rather than mere enforcement volume. At the same time, the continued dominance of internet fraud within EFCC arrest statistics, and the absence of a corresponding decline in the number of Nigerians involved in cybercrime as reported anecdotally by the EFCC's own leadership, means P1 cannot be accepted without qualification: detection has improved, but detection is not equivalent to prevention or reduction of the underlying crime rate.

The evidence lends stronger support to P2 (that the regulatory framework continues to privilege the use of force over structural prevention). The operational pattern documented in

Table 2, recurrent mass raids yielding tens to hundreds of arrests per operation, together with the persistence of these methods even after the ostensibly more preventive 2024 legislative reform, and the contested application of expanded surveillance powers against non-fraud-related speech, together indicate that Nigeria's institutional response remains centred on reactive coercion. This is not necessarily an indictment of the EFCC's operational choices given resource and capacity constraints; rather, it reflects the absence, to date, of a fully resourced alternative model built around preventive disruption of criminal infrastructure, financial-sector-level monitoring (of the kind NIBSS data suggest is beginning to work), and socio-economic intervention targeted at the youth population most associated with internet fraud recruitment.

Conclusion

This study set out to re-evaluate the EFCC's technological and regulatory response to internet fraud in Nigeria using data updated through 2025. The evidence shows unambiguous technological and prosecutorial progress: convictions rose from 103 in 2015 to a record 4,111 in 2024, recoveries reached an unprecedented ₦364.6 billion in the same year, and financial-sector fraud losses, after peaking at ₦52.26 billion in 2024, fell by more than half in 2025 as monitoring technology matured. At the same time, internet fraud remained the largest single category of EFCC enforcement activity in 2024, and the Commission's operational model continues to rely predominantly on large-scale, reactive, force-based raids rather than on structural disruption of the criminal infrastructure and socio-economic drivers underlying the crime. Consistent with the qualified version of Deterrence Theory advanced by McMahon, Davidson, and Messier (2021), increased certainty of punishment for apprehended offenders has not yet translated into a demonstrable reduction in the overall incidence of internet fraud in Nigeria. The 2024 Cybercrimes Amendment Act represents a genuine legislative modernisation, but its implementation to date illustrates both the promise of a more preventive, technology-enabled regulatory model and the risk that expanded state powers may be misapplied in ways that undermine public trust.

Recommendations

Based on the foregoing, the study recommends that:

1. The EFCC and allied agencies establish a single, harmonised national cybercrime-loss reporting framework to eliminate the current discrepancies between NDPC, NIBSS, and EFCC statistics and enable accurate performance measurement;

2. Investment in technological capacity be extended beyond detection and forensic recovery toward disruption of the payment and identity infrastructure that sustains internet fraud, including closer real-time integration between EFCC systems and bank/fintech fraud-monitoring platforms;

3. The National Assembly and relevant oversight bodies review the implementation of the 2024 Cybercrimes Amendment Act's surveillance and content-related provisions to ensure they are not applied against legitimate speech in ways that could undermine public confidence in the broader anti-fraud effort;

References

AB Legal Practitioners. (2025). *A review of the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024.* https://abe-lp.com/2025/08/05/a-review-of-the-cybercrimes-prohibition-prevention-etc-amendment-act-2024/

Adebayo, J. (2021). Challenges in the management and disposal of forfeited assets in Nigeria. *Journal of Financial Crime, 28*(2), 547–560. https://doi.org/10.1108/JFC-09-2020-0166

Aderibigbe, T. (2019). The role of technology in combating financial crimes: A case study of the Economic and Financial Crimes Commission (EFCC) in Nigeria. *Journal of Financial Crime, 26*(2), 449–461.

Aghatise, E. J. (2006). Cybercrime definition and investigation: The Nigerian and global perspective. *Computers & Security, 25*(5), 361–363.

Aiken, M., Bach, T., Jahera Jr, J. S., & Colella, A. (2018). The social ecology of cybercrime in Ghana. *Criminology & Public Policy, 17*(3), 605–636.

allAfrica. (2025, August 26). *Nigeria: EFCC deserves praise, not litigation.* https://allafrica.com/stories/202508260539.html

Apel, R., & Nagin, D. S. (2011). Deterrence: A review of the evidence by a criminologist and economist. *Annual Review of Economics, 3*(1), 83–106.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 759–763.

Asika, N. (2006). *Research methodology in the behavioural sciences.* Longman Nigeria.

Asika, N. (2009). *Research methodology: A process approach.* Mukugamu & Brothers.

Bailey, K. D. (1994). *Methods of social research* (4th ed.). Free Press.

Businessday. (2025, January 16). *Internet fraud, currency racketeering, others top EFCC arrests in 2024.* https://businessday.ng/news/article/internet-fraud-currency-racketeering-others-top-efcc-arrests-in-2024/

Businessday. (2026, April 7). *Nigeria flags rising exposure in $20.9bn global cybercrime surge.* https://businessday.ng/technology/article/nigeria-flags-rising-exposure-in-20-9bn-global-cybercrime-surge/

Channels Television. (2025, March 10). *Fighting corruption: EFCC records highest convictions, asset recovery.* https://www.channelstv.com/2025/03/10/fighting-corruption-efcc-records-highest-convictions-asset-recovery/

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Economic and Financial Crimes Commission (EFCC). (2004). *Economic and Financial Crimes Commission (Establishment) Act.*

Economic and Financial Crimes Commission (EFCC). (2019). *EFCC Tip-Off platform.*

Economic and Financial Crimes Commission (EFCC). (2025, January 10). *EFCC arrests four Chinese, 101 others for suspected internet fraud in Abuja.* https://www.efcc.gov.ng/efcc/news-and-information/news-release/10605-efcc-arrests-four-chinese-101-others-for-suspected-internet-fraud-in-abuja

Effoduh, J. A. (2016). The clouds are gathering—cybercrime laws and regulations in Nigeria. *Journal of Internet and Information Systems, 6*(1), 1–10.

Europol. (2021). *Joint Cybercrime Action Taskforce (J-CAT).* https://www.europol.europa.eu/operations-services-and-innovation/eu-regional-taskforces/joint-cybercrime-action-taskforce

Federal Bureau of Investigation. (2026). *Internet Crime Complaint Center (IC3) 2025 annual report.* U.S. Department of Justice.

Hamu Legal. (2024). *Highlights of Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024.* https://hamulegal.com/highlights-of-cybercrimes-prohibition-prevention-etc-amendment-act-2024/

Higgins, G. E. (2009). Cybercrime: An overview of the Federal Computer Fraud and Abuse Statute and related federal criminal laws. *United States Attorneys' Bulletin, 57*(6), 4–15.

Ibrahim, S. (2016). Causes of cybercrime and prevention methods in Nigeria. *International Journal of Computer Applications, 147*(11).

Idris, A. (2021). Successes and challenges of EFCC in Nigeria's anti-corruption crusade. *Unpublished study.*

Kerlinger, F. N. (1977). *Foundations of behavioural research* (2nd ed.). Holt, Rinehart and Winston.

Leadership. (2025, August 25). *EFCC deserves praise, not litigation.* https://leadership.ng/efcc-deserves-praise-not-litigation/

Longe, O. B., & Chiemeke, S. C. (2006). Cyber crime and criminality in Nigeria: What roles are internet access points playing? *European Journal of Social Sciences, 6*(4).

McMahon, S., Davidson, R., & Messier, D. (2021). Deconstructing deterrence in cyberspace. *Philosophy & Technology, 34*(2), 293–312.

Mondaq. (2024). *The Cybercrime (Prohibition, Prevention, etc.) (Amendment) Act 2024.* https://www.mondaq.com/nigeria/security/1701826/the-cybercrime-prohibition-prevention-etc-amendment-act-2024

Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and Justice, 42*(1), 199–263.

Nigeria Data Protection Commission (NDPC). (2026, April). *Presentation at IoT West Africa 2026 conference*, as reported in Vanguard and Worldstage News.

Nigeria Inter-Bank Settlement System (NIBSS). (2026). *Fraud in the Nigerian banking system: 2025 report*, as cited in Vanguard (2026, June).

Nigeria Computer Emergency Response Team (NgCERT). (2021). *Cybercrime reporting portal.* https://www.ngcert.org.ng/cybercrime-reporting-portal/

Nigerian Cybercrime Reform Task Force (NALTF). (2025). *Nigeria's cybercrime reform.* https://naltf.gov.ng/nigerias-cybercrime-reform/

Nigerian Observer. (2024, November 29). *EFCC strengthens fight against internet fraud and financial crimes with major arrests and convictions.* https://nigerianobservernews.com/2024/11/efcc-strengthens-fight-against-internet-fraud-and-financial-crimes-with-major-arrests-and-convictions/

Oguonu, C. N., & Anugwom, E. E. (2014). *Research methods in the social sciences.* Great AP Express Publishers.

Ogwezzy, M. C. (2012). Cybercrime and the proliferation of yahoo addicts in Nigeria. *International Journal of Juridical Sciences, 1*(1), 18–42.

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology, 6*(2), 1001–1013.

Purba, D. (2018). Technological infrastructure and cybercrime enforcement in developing countries. *Journal of Information Technology and Development.*

Rahim, R. (2018). The internet as a tool for transnational cybercrime: Implications for international relations. *Journal of Cyber Policy Studies.*

Sandelowski, M. (2000). Whatever happened to qualitative description? *Research in Nursing & Health, 23*(4), 334–340.

Saragih, R., & Siahaan, D. (2016). The role of information technology in modern society. *Journal of Technology and Society.*

Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860–875.

Tombs, S., & Whyte, D. (2013). Transcending the deregulation debate? Regulation, risk, and the enforcement of health and safety law in the UK. *Regulation & Governance, 7*(1), 61–79.

United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive study on cybercrime.* https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Vanguard. (2025, March 13). *Crackdown on economic, financial crimes: EFCC's landmark cases, recoveries.* https://www.vanguardngr.com/2025/03/crackdown-on-economic-financial-crimes-efccs-landmark-cases-recoveries/

Vanguard. (2025, August 1). *How misuse of Cybercrime Act cost Nigeria N1.1trn in 7 yrs.* https://www.vanguardngr.com/2025/08/how-misuse-of-cybercrime-act-cost-nigeria-n1-1trn-in-7-yrs/

Vanguard. (2026, May 6). *Cybercrime surge hits Nigeria's digital economy as losses hit N12bn annually.* https://www.vanguardngr.com/2026/05/cybercrime-surge-hits-nigerias-digital-economy-as-losses-hit-n12bn-annually/

Vanguard. (2026, June). *Cybercrime still hits Nigeria's digital economy hard.* https://www.vanguardngr.com/2026/06/cybercrime-still-hits-nigerias-digital-economy-hard/