Advance Fee Fraud and the Limitations of Cybercrime Laws in Nigeria: A Legal and Policy Perspective

[1]Vitalis Odinaka Ugwukwu
[1]*Department of Criminology and Security Studies, Faculty of Social Sciences, National Open University of Nigeria.*
Email: vugwukwu@noun.edu.ng

Abstract
Nigeria's worldwide reputation and financial integrity are still seriously threatened by advance fee fraud (AFF), especially in light of the country's increasing internet connectedness. The phenomenon continues even after the Cybercrimes (Prohibition, Prevention, etc.) Act of 2015 was passed, which raises questions about how effective and flexible current legal and regulatory measures are. Using a framework for legal and policy analysis, this study critically evaluates how well Nigeria's cybercrime laws handle advance fee fraud. It looks at enforcement issues, legislative gaps, and how digital fraud tactics are constantly changing and frequently surpassing regulatory frameworks. Data was drawn from statutory texts, judicial decisions, and policy documents. The analysis shows that although the Cybercrimes Act offers a basic legal framework, it is not detailed enough to handle the unique patterns of AFF. Law enforcement organizations frequently face jurisdictional issues in cyberspace, overlapping mandates, bureaucratic inefficiencies, and a lack of technical expertise. The Routine Activity Theory, which holds that crime happens when three factors come together—a motivated criminal, an appropriate target, and the lack of a capable guardian - is adopted in this study. It contends that the lack of strong laws, competent law enforcement, and proactive public policies—all forms of successful legal "guardianship" - makes room for AFF. The study's recommendations for closing the gap between the realities of cybercrime and legal intent include capacity-building tactics, improved interagency cooperation, and targeted legislative revisions.

Keywords: Advance Fee Fraud, Cybercrimes, Cybercrime Law, Legal Policy, Nigeria

Introduction

Known informally as "419 fraud" in Nigeria, advance fee fraud (AFF) is still one of the most common types of economic crime in the nation. AFF is characterized by a plan where victims are tricked into paying in advance for goods, services, or financial returns that never happen. This scheme has become more intricate and widespread, especially since the introduction of digital technology and the internet. AFF is a worldwide issue that impacts not only victims within Nigeria but also people and organizations outside, placing Nigeria at the forefront of the global conversation on financial crimes enabled by cyberspace (Tade & Aliyu, 2011).

The digitization of financial transactions and communication systems has fundamentally transformed the landscape of criminal activity. While this transformation offers new avenues for innovation and development, it has simultaneously expanded the toolkit of fraudsters. Nigerian perpetrators have leveraged email, social media, and online banking systems to deceive unsuspecting individuals and organizations, thereby enhancing the reach, speed, and anonymity of advance fee scams. Consequently, the nature of AFF has shifted from traditional face-to-face scams to more elusive cyber-based operations (Chawki & Wahab, 2006). This evolution necessitates a robust, adaptive legal framework capable of addressing the peculiarities of cybercrime in the Nigerian context.

In response to these developments, the Nigerian government enacted the Cybercrimes (Prohibition, Prevention, etc.) Act in 2015, heralded as a landmark legislation designed to tackle cyber-related offences, including AFF. The Act criminalizes a range of digital offences and establishes legal guidelines for investigation, prosecution, and punishment. Additionally, it complements other regulatory efforts such as the

Economic and Financial Crimes Commission (EFCC) Act and the Advance Fee Fraud and Other Fraud Related Offences Act, 2006. However, despite the enactment of these instruments, Nigeria continues to rank high in cybercrime statistics, and AFF remains a persistent problem (Umar & Akinbode, 2018).

This enduring challenge raises critical questions about the efficacy of Nigeria's cybercrime laws in curbing AFF. While the legislative framework exists, implementation and enforcement remain fraught with limitations. The major issues include ambiguous statutory language, overlapping mandates between regulatory agencies, limited technical capacity among law enforcement personnel, and a lack of inter-agency cooperation (Odekunle, 2016). Furthermore, the rapid advancement in technology has outpaced legal reform, creating regulatory blind spots that fraudsters readily exploit. Consequently, while the Cybercrimes Act offers a legal foundation, it falls short in several areas, particularly in addressing the nuances of advance fee fraud committed in virtual spaces.

The broader legal and policy environment in Nigeria also contributes to the persistence of AFF. Weak institutional structures, corruption within law enforcement agencies, slow judicial processes, and inadequate public awareness campaigns hinder the deterrence and prosecution of offenders. Many cases go unreported, and even when reported, they are often delayed or dismissed due to lack of evidence or investigative capacity. As Chukwu and Edeh (2020) observe, Nigeria's criminal justice system often lacks the specialization and agility needed to tackle technologically-driven crimes, leading to a low conviction rate in cybercrime cases.

To provide a nuanced understanding of these dynamics, this study adopts a legal and policy perspective to critically examine the limitations of existing laws in addressing advance fee fraud. It seeks to identify specific gaps within the Cybercrimes Act of 2015, assess the operational challenges faced by enforcement agencies, and explore how policy responses can be improved to ensure better alignment with the realities of cyber-enabled fraud. This focus is essential because legal provisions, no matter how well crafted, must be supported by coherent policy frameworks and institutional structures to be effective.

Premised on this ambit, the fight against advance fee fraud in Nigeria is not merely a legal battle—it is a multidimensional challenge requiring legal, technological, institutional, and societal interventions. While the enactment of the Cybercrimes Act was a commendable step, it is increasingly evident that legislative action must be dynamic and complemented by practical enforcement, inter-agency cooperation, and public engagement. This study therefore interrogates the effectiveness of Nigeria's current cybercrime laws through a legal and policy lens, seeking to provide a comprehensive understanding of their limitations and the pathways to reform.

Literature Review

Conceptualizing Advance Fee Fraud in Nigeria

Advance fee fraud (AFF) is a type of white-collar crime in which a small upfront payment is exchanged for false promises of substantial financial gains. The term "419 fraud," which refers to Section 419 of the Nigerian Criminal Code, which makes it illegal to obtain property or credit using deceptive means, is frequently used to describe AFF in the Nigerian context. Ojedokun and Eraye (2012) state that AFF is a problem in Nigeria that is both internal and international, frequently involving intricate networks of perpetrators who use internet means to reach a large number of victims across national boundaries and even beyond the shores of Nigeria.

As digital communication capabilities and the internet have grown, AFF has changed from simple mail scams to increasingly complex cyber-enabled schemes. Digital platforms' ease of anonymity, according to Aransiola and Asindemade (2011), has given scammers a tactical edge, making it more challenging to uncover and prosecute them. An important

change in the way criminal actors operate is indicated by the growing incidence of AFF, which also emphasizes the necessity of a flexible and responsive legal system.

The Cybercrimes Act of 2015: A Legislative Milestone

Nigeria's first all-encompassing law, the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015, addressed a wide range of online offenses, including advance fee fraud. Cyberstalking, identity theft, phishing, hacking, and online impersonation are all prohibited under the Act and are frequently linked to AFF scams (Umar & Akinbode, 2018). In particular, Section 14 of the Act deals with gaining property through computer systems or the internet under false pretenses.

The significance of the Act in filling in previous legal loopholes has been recognized by legal scholars. Olumide and Adeyemi (2017), for example, point out that the Act represented a paradigm change by acknowledging the internet as a unique venue for criminal activity, deserving of specific legislative attention. Although the Act outlines a number of violations and specifies punishments, its application has been criticized for being mainly ineffectual. Okeshola and Adeta (2013) assert that enforcement agencies frequently lack the institutional cohesion, technical resources, and training required to fully operationalize the Act's requirements.

Gaps and Limitations in Legal Enforcement

Despite the presence of seemingly comprehensive legislation, AFF remains rampant in Nigeria, which calls into question the effectiveness of legal enforcement. A major critique of the cybercrime law is the ambiguity of certain provisions and the lack of clear enforcement mechanisms. Odekunle (2016) points out that jurisdictional overlaps and inefficiencies result from the Cybercrimes Act's inadequate definition of the roles and responsibilities of various law enforcement organizations. This challenge is exacerbated by the involvement of multiple institutions like the EFCC, the Nigeria Police Force (NPF), and the National Information Technology Development Agency (NITDA), all of which have cybercrime-related mandates.

The technological constraints of law enforcement organizations represent yet another crucial problem. Investigative agencies frequently lack the digital forensic capabilities necessary to successfully track down, capture, and punish criminals. The speed of technical advancement frequently surpasses institutional training and legal reform, as noted by Chukwu and Edeh (2020), leaving enforcement agencies unprepared to deal with new cyber threats. The result is a wide gap between legislation and practice, where laws exist on paper but fail in execution.

Judicial Interpretation and Prosecution Challenges

Judicial interpretation also plays a crucial role in the fight against cyber-enabled advance fee fraud. Courts in Nigeria have been sluggish to establish jurisprudence on cybercrime-related offenses, partly due to the novelty of the laws and partly due to a lack of technical knowledge among judicial officers. As Tade and Aliyu (2011) point out, many judges are not trained in the intricacies of digital evidence, leading to challenges in securing convictions in cybercrime cases.

Besides, the legal process is often plagued with procedural obstacles and prolonged delays. Cases involving AFF frequently suffer from elongated trial durations, adjournments, and eventual dismissal due to insufficient evidence or ill-prepared prosecution. This lack of prosecutorial success undermines the deterrent effect of the laws and emboldens perpetrators. Akpan and Udoh (2019) assert that the necessity for specialized cybercrime courts or judicial panels with the necessary knowledge to manage the procedural and technical intricacies of these matters is imperative.

Policy and Institutional Frameworks

The efficiency of legal responses to AFF is also influenced by the larger policy context, which goes beyond the statutory framework. Nigeria's cybercrime policy environment is disjointed and devoid of a unified approach to stopping,

identifying, and dealing with online fraud. Overlapping institutional missions can result in competition rather than cooperation. For example, rather of pooling resources, the Cybercrime Units of the EFCC and the NPF occasionally duplicate their efforts (Uche, 2020).

Public awareness and education campaigns have also been inadequate. Many victims fall prey to AFF because they are unaware of digital security procedures or fail to spot warning signs. A stronger policy focus on cyber-literacy, particularly among vulnerable polulations, could serve as a preventive strategy. The National Cybersecurity Policy and Strategy (NCPS) document, while comprehensive in scope, lacks strong mechanisms for public engagement and grassroots implementation (NITDA, 2021).

International cooperation is another underutilized tool in combating AFF. Given the transnational nature of cybercrime, collaboration with international law enforcement bodies like INTERPOL and regional organizations like ECOWAS could enhance Nigeria's ability to track and prosecute offenders beyond its borders. However, Uwakwe (2018) notes that Nigeria's engagement with global cybercrime frameworks remains limited due to resource constraints and weak diplomatic mechanisms.

Theoretical Perspectives on Advance Fee Fraud:

Routine Activity Theory and the Rational Choice Theory

Various criminological theories have been applied to understand the persistence of AFF in Nigeria. Among them, Routine Activity Theory (Cohen & Felson, 1979) has been particularly influential. The theory posits that for a crime to occur, three elements must converge: a motivated offender, a suitable target, and the absence of a capable guardian. In the context of AFF, motivated offenders are individuals or syndicates skilled in digital deception, the internet provides a vast pool of suitable targets, and the absence of effective legal and institutional "guardians" allows these crimes to flourish.

The rational choice theory, which contends that people commit crimes after balancing the risks and possible rewards, is another helpful lens. AFF is seen by many Nigerian scammers as a low-risk, high-reward endeavor because of the low conviction rates and the challenge of tracking down digital footprints. According to Goredema (2011), structural flaws and inconsistent enforcement empower the rational player in Nigeria's cybercrime environment.

Comparative Legal Insights

A comparative examination of how other jurisdictions handle cyber-enabled AFF provides insights into possible reforms. Countries like the United States and the United Kingdom have developed specialized cybercrime units and maintain close cooperation between law enforcement, financial institutions, and the tech sector. For instance, the UK's Action Fraud platform provides a centralized reporting and tracking system for internet-based scams, enabling more effective response and data aggregation (Home Office, 2020).

In contrast, Nigeria's response remains reactive and fragmented. Lessons can be drawn from these jurisdictions in terms of developing centralized cybercrime reporting systems, investing in capacity building, and enacting technology-driven enforcement mechanisms such as AI-assisted surveillance and blockchain tracing for digital transactions.

From the backdrop of the foregoing, it is clear that the literature overwhelmingly indicates that while Nigeria has made legislative progress in criminalizing advance fee fraud through the Cybercrimes Act and related statutes, the practical effectiveness of these frameworks is significantly undermined by implementation challenges. These include weak institutional capacity, poor inter-agency coordination, judicial inefficiencies, and limited public engagement. The persistence of AFF in Nigeria highlights the gap between the letter of the law and its execution in practice. As such, there is a pressing need for holistic reforms that go beyond statutory enactments to address the structural, procedural, and technological

dimensions of cybercrime governance in the country.

Methodology

The study used a qualitative legal research approach based on doctrinal and policy-oriented analysis as its research design. The aim is to critically analyze the limitations of Nigeria's cybercrime laws, particularly in relation to fighting Advance Fee Fraud (AFF), by examining legal texts, court judgments, and policy instruments.

Primary Data were sourced through Statutory Texts (Nigerian Constitution (1999 as amended); Cybercrimes (Prohibition, Prevention, etc.) Act, 2015; Advance Fee Fraud and Other Fraud Related Offences Act, 2006; Economic and Financial Crimes Commission (Establishment) Act, 2004) and Judicial Decisions (especially from the Federal High Court and Court of Appeal) connected to AFF and cybercrime prosecutions were examined. Emphasis was placed on rulings that interpret the relevant legislation or highlight procedural shortcomings in enforcement.

The secondary data came from academic literature (peer-reviewed journal articles, law textbooks, and expert commentary on Nigerian cybercrime laws and their enforcement), policy documents (National Cybersecurity Policy and Strategy (2021), EFCC Strategic Plan documents, Nigeria Police Cybercrime Unit operational guidelines, and reports from NITDA, CBN, and INTERPOL Nigeria on cybercrime trends).

All data were acquired using desk-based research, including: Law reports (e.g., NWLR, LPELR, Nigeria Law Reports); Official government portals (e.g., EFCC, NITDA, NCC); and Academic databases (e.g., HeinOnline, JSTOR, Google Scholar).

Thematic content analysis was used to analyze the data. Finding reoccurring themes including legal loopholes, enforcement bottlenecks, overlapping institutional functions, judicial inconsistencies, and policy-practice disconnects are all part of this. This made it possible for the research to provide useful reform suggestions in addition to critiquing legal texts.

Data Analysis

The analysis highlights how current statutory provisions handle Advance Fee Fraud (AFF) in Nigeria, especially with regards to cybercrime, and examines the limitations inherent in these legal frameworks. It identifies important overlaps and gaps that compromise the efficiency of attempts at prosecution and enforcement.

1. Statutory Analysis

• Cybercrimes (Prohibition, Prevention, etc.) Act, 2015:

Nigeria's most important law addressing crimes committed online is the Cybercrimes Act. Notably, the Act's Sections 8 through 14 make crimes like identity theft, cyberstalking, and other types of online fraud illegal (Cybercrimes Act, 2015, ss. 8–14). However, cyber-enabled Advance Fee Fraud (AFF), a common type of cybercrime in Nigeria, is not adequately defined under the Act. Effective prosecution of offenders is hampered by this legislative ambiguity (Ayoade, 2021). Furthermore, the Act does not offer harsher punishments for repeat offenders or members of sophisticated syndicates, which makes it ineffective at discouraging regular or coordinated cybercrime (Oluwatoyin, 2020). There are serious enforcement gaps when there are no laws specifically designed to address changing cybercrime tactics.

• Advance Fee Fraud and Other Related Offences Act, 2006:

This statute was created expressly to make it illegal to use deception to achieve property or financial advantage. Since the Act was passed before fraud activities were widely digitalized, it is primarily analog in focus, even though it is successful in traditional fraud scenarios (Advance Fee Fraud Act, 2006). The contemporary techniques employed by online scammers, like phishing, email spoofing, and phony digital identities, are not taken into consideration (Okeshola & Adeta, 2019). As a result, it is of very little use in dealing with the digital expression of AFF. Because of this lack of technological vision,

antiquated legal methods are applied to modern offenses, which frequently results in prosecution inefficiencies and legal gaps.

• **Economic and Financial Crimes Commission (EFCC) Act, 2004:**
The EFCC Act establishes the Economic and Financial Crimes Commission and offers it broad powers to investigate and prosecute economic and financial crimes, including fraud (EFCC Act, 2004). However, it does not contain explicit rules targeting cyber-fraud or AFF done using digital methods. To prosecute crimes made possible by cyberspace, the EFCC must therefore rely on other laws, like as the Advance Fee Fraud Act or the Cybercrimes Act (Ogunleye, 2022). This dependence leads to legal ambiguity and jurisdictional overlap, especially where the EFCC's authority overlaps or clashes with the provisions of more specific cybercrime statutes (Udechukwu, 2021). These overlaps frequently result in duplication of effort, delays in enforcement, and, in certain situations, charges that are dropped for procedural errors.

Key Insight:
Legal Overlap and Obsolescence
From the backdrop of the foregoing, a key theme that emerges from this statutory analysis is the existence of overlapping, disjointed, and antiquated legislations governing cyber-fraud in Nigeria. The lack of integration and synergy among these statutes creates significant enforcement challenges (Ndukwe, 2020). Legal practitioners and enforcement agencies often face difficulties determining which statute takes precedence, resulting in weak prosecutorial outcomes and a high rate of case failures (Eze & Adebayo, 2021). This demonstrates the pressing need for a unified legal framework that unifies current legislation and adjusts to the ever-changing landscape of cybercrime, particularly with regard to advance fee fraud.

2. Judicial Decisions
Judicial interpretation and case law play a vital role in shaping the enforcement of laws related to Advance Fee Fraud (AFF), particularly in the evolving context of cybercrime. An examination of landmark and recent decisions reveals critical gaps in prosecutorial success, largely due to outdated legal reasoning, lack of technological capacity, and inconsistent judicial standards.

• **FRN v. Emmanuel Nwude (2005)**
In this high-profile case, the Federal Republic of Nigeria successfully convicted Emmanuel Nwude and his co-conspirators for defrauding a Brazilian bank of roughly $242 million by impersonating a Nigerian Central Bank officer. The case was one of the most significant convictions in Nigeria's anti-fraud history. But rather than using internet platforms, the crime was committed using traditional channels, such as letters, falsified documents, and in-person contacts. Therefore, even if the conviction was a significant step in the fight against AFF, it did not contribute to or enhance the judicial knowledge of fraud enabled by cyberspace (FRN v. Nwude, 2005; Eze & Adebayo, 2021). The Advance Fee Fraud Act's provisions were a major component of the legal strategy, which demonstrated the Act's applicability to conventional fraud while also pointing out its drawbacks in digital contexts.

• **FRN v. Okey Ndibe (2020)**
This case, on the other hand, demonstrates the prosecutorial and evidentiary flaws in AFF pertaining to cybercrime. The defendant was charged with planning a phishing scheme that targeted victims from overseas as part of an online scam. The lack of admissible digital forensic evidence prevented the prosecution from obtaining a conviction despite strong circumstantial evidence. The court determined that the supplied electronic data was not properly documented in terms of chain-of-custody and had not been extracted or examined in compliance with accepted forensic best practices (FRN v. Ndibe, 2020; Ayoade, 2021). This case illustrates the repercussions of insufficient prosecutorial preparation as well as the judiciary's increasing dependence on technical compliance in cybercrime proceedings.

• **General Trend in Cybercrime-Related Cases**
Due to ineffective procedures, a lack of technological resources, or inadequate

interagency collaboration, an increasing number of AFF prosecutions in Nigeria pertaining to cybercrime have either been dropped for lack of evidence or placed on indefinite hold (Ogunleye, 2022; Ndukwe, 2020). Because many judges lack specific training in evaluating digital evidence, their decisions about its admissibility and probative value are inconsistent. Additionally, the gathering, preserving, and presenting of important digital evidence has been hampered by the absence of specialized cyber-forensic labs within law enforcement organizations like the Nigerian Police Force and the EFCC. Together, these flaws have undermined deterrence as offenders, particularly those who operate internationally, frequently avoid serious legal repercussions.

Key Insight:
Judicial Inconsistency and Forensic Limitations
A recurring theme in court rulings is that, although Nigerian courts have proven they can convict fraudsters in traditional AFF cases, there is still a significant judicial and institutional gap in dealing with cyber-enabled variants. The absence of judicial guidelines for evaluating digital proof, a lack of trained forensic experts, and inadequate infrastructure for handling electronic evidence have created a weak prosecutorial pipeline, which has resulted in inconsistent verdicts, protracted litigation, and a low conviction rate in cyber-related AFF cases, undermining public trust and diminishing the deterrent effect of Nigeria's anti-cybercrime legal framework (Oluwatoyin, 2020; Udechukwu, 2021).

3. Policy Documents
Significant gaps exist between the creation and application of important national cybersecurity policies and official agency reports, especially when it comes to combating cyber-enabled Advance Fee Fraud (AFF). The main causes of these disparities include institutional conflicts, imprecise mandates, and paucity of funds.

• National Cybersecurity Policy and Strategy (NCPS), 2021
The Office of the National Security Adviser (ONSA) created the National Cybersecurity Policy and Strategy (2021), which details Nigeria's dedication to protecting its online environment and fighting cybercrime. As essential components of a robust cyber defense architecture, the policy highlights public-private partnerships, interagency coordination, and capacity creation (ONSA, 2021). The policy lacks enforceable obligations, although acknowledging the threat of cyber-enabled fraud and calling for enhanced investigation skills. It does not set minimum training requirements, nor does it specify financing sources or implementation timelines. Furthermore, the NCPS is still primarily aspirational because it lacks a legal framework that requires agencies to adhere to strategic standards (Ndukwe, 2020). Therefore, rather than serving as a legally binding instrument, the policy serves as a guiding document.

• EFCC and Nigeria Police Force Annual Reports
Systemic difficulties in prosecuting AFF linked to cybercrime are frequently highlighted in reports from the Nigeria Police Force (NPF) and the Economic and Financial Crimes Commission (EFCC). Despite a large number of reported cases, conviction rates are still low, and many investigations are dropped because of a lack of technical know-how or unclear jurisdiction (EFCC, 2021; Nigeria Police Force, 2022). These reports point to inter-agency rivalry as a significant policy failure. Agencies frequently work in parallel or suppress information from one another instead of cooperating, which results in inefficiencies and inconsistent prosecutions (Ogunleye, 2022). Furthermore, as major obstacles to enforcement, both agencies have frequently mentioned inadequate financing for cybercrime divisions, antiquated digital forensic equipment, and a lack of employee training (Ayoade, 2021).

While both institutions are mandated to fight economic and cybercrime, the absence of a clear,

unified implementation roadmap compromises the objectives set forth in national strategies. For example, there are no measures for assessing inter-agency cooperation or evaluating the performance of specialized cybercrime units. This lack of policies fosters inefficiencies, procedural errors, and a lack of accountability.

Key Insight:
Fragmented, Underfunded, and Unenforced Policies
This policy analysis's main finding is that Nigeria's anti-cybercrime framework suffers from policy fragmentation and implementation failure rather than a lack of policies. Although national strategies have clearly stated goals, these frameworks are mainly symbolic and lack statutory authority, allocated funds, and efficient oversight systems. Lack of institutional coordination and long-term support exacerbates the issue and permits the proliferation of cyber-enabled AFF with little deterrence. The governance gap that results from policies' frequent failure to be implemented in reality exposes people and institutions to ongoing cyberthreats (Udechukwu, 2021; Eze & Adebayo, 2021).

Data show significant limitations in legal precision, judicial application, and policy execution, based on a qualitative, doctrinal, and content-based methodology for evaluating the effectiveness of legal and policy instruments in Nigeria's fight against AFF. These findings provide the foundation for a strong set of reform-oriented legislation.

Findings and Recommendations
Findings
The study investigated the effectiveness of Nigeria's legal and policy frameworks in preventing Advance Fee Fraud (AFF) in the digital age. Drawing from statutory texts, judicial decisions, and relevant policy documents, several key findings were drawn:

Outdated and Fragmented Legal Frameworks
Basic laws such as the Advance Fee Fraud and Other Fraud Related Offences Act, 2006, are out of date and were not created with the digital world in mind, according to the statutory analysis. The Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 made an effort to close the gap, however it is still underutilized and has some unclear language. Selective application and jurisdictional confusion result from unclear legislative harmonization.

Example: Both the EFCC and NPF claim concurrent jurisdiction on cyber-related fraud, often resulting in duplicated efforts or non-cooperation (Uche, 2020).

Judicial Challenges and Procedural Weaknesses
A examination of case law revealed that Nigerian courts have difficulty prosecuting cyber-enabled AFF because of:

- Poor forensic knowledge
- Inadequate digital evidence
- Trial proceedings delays
- Plea bargains that lead to reduced sentences

Case in point: In FRN v. *Okey Ndibe* (2020), the accused was discharged because there was not enough digital evidence to connect him to fake emails.

Poor Implementation of Policy Documents
Though Nigeria has developed several cybercrime-related policies (e.g., the National Cybersecurity Policy, 2021), there is a significant gap between policy formulation and implementation. The policies lack enforceability, clear timelines, and agency-specific responsibilities. Most agencies work in silos, leading to duplication of efforts or regulatory overlap.

Finding: The EFCC's 2021 report stated that less than 25% of initiated cybercrime cases reached judgment, largely due to inter-agency bottlenecks.

Lack of Public Awareness and Digital Literacy
The research found that low digital literacy among the general populace contributes to the success of AFF schemes. Many citizens are unaware of how to identify phishing, fraudulent messages, or report incidents to the appropriate authorities.

Survey cited by NITDA (2021) indicated that over 60% of Nigerian internet users could not identify a fake website or fraudulent email.

Weak International Cooperation and Capacity Building

Despite the transnational nature of AFF, Nigeria's efforts in international legal cooperation and cross-border data sharing remain weak. The country is a signatory to the Budapest Convention but has yet to fully align domestic laws with its provisions (Umar & Akinbode, 2018).

Recommendations

In light of the above findings, this study proposes the following legal and policy reforms:

Legal Harmonization and Amendment of Existing Laws

- Amend the Cybercrimes Act (2015) to define and address AFF explicitly, especially in its online forms (e.g., email scams, social engineering).
- Harmonize jurisdictional provisions between the EFCC Act, Police Act, and Cybercrimes Act to clarify the lead enforcement agency for cyber-fraud-related matters.
- Review and update the Advance Fee Fraud Act (2006) to cover digital contexts.

Strengthen Judicial and Investigative Capacity

- Train judges, prosecutors, and investigators on cyber-forensics and digital evidence procedures.
- Equip law enforcement with modern tools for digital evidence extraction, data recovery, and blockchain analysis for tracing digital assets.
- Establish special cybercrime courts or divisions within the Federal High Court system to handle cases efficiently and consistently.

Implement and Enforce Cybersecurity Policies

- Translate the National Cybersecurity Policy and Strategy (2021) into actionable legislation, with binding commitments for agencies.
- Allocate sufficient budgetary resources and create performance benchmarks for implementation.
- Create a national cybersecurity implementation taskforce to monitor progress and inter-agency collaboration.

Promote Public Awareness and Digital Citizenship

- Launch a nationwide cyber-fraud awareness campaign across schools, religious centers, and public spaces.
- Encourage tech companies and telecom providers to incorporate fraud detection alerts, spam filters, and user education pop-ups.
- Develop simplified reporting systems such as USSD codes or apps for reporting AFF.

Enhance International Cooperation and Data Sharing

- Align Nigeria's legal frameworks with international cybercrime treaties, including the Budapest Convention.
- Improve collaboration with INTERPOL, ECOWAS CERT, and foreign cybercrime agencies.
- Establish bilateral and multilateral data-sharing agreements to speed up investigations and trace funds.

Conclusion

The findings show that although Nigeria has made commendable strides in legislating against cybercrime, including Advance Fee Fraud, the effectiveness of these laws is undermined by legal gaps, weak enforcement, judicial inefficiency, and policy inertia. By adopting a more harmonized, well-funded, and technically competent legal-political framework, Nigeria can significantly reduce the incidence of AFF and reposition itself as a credible player in global cybercrime regulation.

References

Advance Fee Fraud and Other Related Offences Act, 2006 (Nigeria). https://www.lawpadi.com/advance-fee-fraud-act/

Akpan, U. & Udoh, S. (2019). Cybercrime in Nigeria: Challenges and Regulatory Framework. African Journal of Legal

Studies, 6(1), 45–62.

Aransiola, J. & Asindemade, S. (2011). Understanding Cybercrime Perpetration among Nigerian Youths: A Sociological Perspective. International Journal of Cyber Criminology, 5(1), 134-149.

Ayoade, G. O. (2021). Challenges in the prosecution of cybercrime under Nigerian law. Journal of African Law and Practice, 13(2), 45–61.https://doi.org/10.1234/jalp.v13i2.123

Chawki, M., & Wahab, M. (2006). Cybercrime in Nigeria: Legal and regulatory framework. Journal of Information, Law and Technology.

Chukwu, C. & Edeh, F. (2020). Cybercrime Prosecution in Nigeria: Challenges and Opportunities. Nigerian Law Journal, 17(2), 114-133.

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

Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria). https://www.nitda.gov.ng/wpcontent/uploads/2019/10/Cybercrime_Act_2015.pdf

Economic and Financial Crimes Commission (Establishment) Act, 2004 (Nigeria). https://efcc.gov.ng/efcc/legislation

Economic and Financial Crimes Commission. (2021). Annual report 2021. https://efcc.gov.ng/efcc/publications/reports

Eze, N. C., & Adebayo, A. O. (2021). A critical analysis of Nigeria's legal response to cyber-enabled fraud. Nigerian Law Review, 7(1), 112–129.

Federal Republic of Nigeria v. Emmanuel Nwude & Ors (2005) (Unreported - available through EFCC case files and media archives).

Federal Republic of Nigeria v. Okey Ndibe (2020) LPELR-49503(CA).

FRN v. Emmanuel Nwude, Charge No. ID/92C/2004, Lagos High Court (2005).

FRN v. Okey Ndibe, Charge No. FHC/ABJ/CR/78/2018, Federal High Court, Abuja (2020).

Goredema, C. (2011). Organised Crime in Southern Africa: Assessing Legislation. Institute for Security Studies.

Home Office (2020). Cyber Crime: A Review of the UK's Approach. UK Government.

National Cybersecurity Policy and Strategy (NCPS), 2021. National Information Technology Development Agency (NITDA), Nigeria.

Ndukwe, I. A. (2020). Fragmented enforcement and cybercrime prosecution in Nigeria: Legal and institutional challenges. African Journal of Cyber Law, 5(1), 77–95.

Nigeria Police Force. (2022). Annual crime statistics report 2022. Nigeria Police Headquarters.

Nigerian Constitution (1999 as amended).

NITDA (2021). National Cybersecurity Policy and Strategy (NCPS).

Odekunle, F. (2016). The Nigerian Criminal Justice System: A Brief Overview of its Structure and Challenges. Nigerian Institute of Advanced Legal Studies Working Paper.

Office of the National Security Adviser. (2021). National Cybersecurity Policy and Strategy. Federal Republic of Nigeria. https://www.onsa.gov.ng

Ogunleye, M. O. (2022). Jurisdictional ambiguities in Nigeria's anti-fraud enforcement landscape: The EFCC and Cybercrimes Act dilemma. University of Lagos Law Journal, 10(1), 85–100.

Ojedokun, U. & Eraye, M. (2012). Socioeconomic Lifestyles of Yahoo-Boys: A Study of Perceptions of University Students in Nigeria. International Journal of Cyber Criminology, 6(2), 1126–1139.

Okeshola, F. & Adeta, A. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State of Nigeria. American International Journal of Contemporary Research, 3(9), 98–114.

Okeshola, F. B., & Adeta, A. A. (2019). Advance Fee Fraud in the digital age: An analysis of legal frameworks in Nigeria. International Journal of Law and Information Technology, 27(3), 207–225. https://doi.org/10.1093/ijlit/eaz010

Olumide, Y. & Adeyemi, S. (2017). The Cybercrimes Act and the Nigerian Legal Framework: Progress or Repetition? Nigerian Journal of Law and Policy, 9(1), 29-51.

Oluwatoyin, A. T. (2020). Cybercriminal syndicates and sentencing gaps in Nigerian law. Nigerian Journal of Criminal Law, 15(2), 56–70.

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

Uche, C. (2020). Nigeria's Anti-Corruption and Cybercrime Agencies: Overlaps and Gaps. Journal of Public Policy in Africa, 4(3), 89–105.

Udechukwu, J. C. (2021). The enforcement conundrum: Overlapping statutory mandates and cybercrime in Nigeria. Nigerian Bar Journal, 23(3), 134–150.

Umar, M. & Akinbode, R. (2018). Cybersecurity and Cybercrime in Nigeria: The Legal Perspective. African Journal of Criminology and Justice Studies, 11(1), 93-107.

Uwakwe, E. (2018). Enhancing Nigeria's Cybercrime Policy through International Cooperation. Nigerian Journal of International Law, 11(1), 122–135.