CIFILE Journal of International Law (CJIL), Vol. 5, No.9, 1-14 (2024)

Homepage: [*https://www.cifilejournal.com*](https://www.cifilejournal.com)

Print ISSN: 2563-6820
Online ISSN: 2563-3341

Investigating the Laxity of Law Enforcement Authorities Toward Internet Fraud in Nigeria

Damilola John Akinsanya

Nigerian Bar Association, University of Ibadan, Nigeria

(Corresponding Author) damilolaakinsanyajohn@gmail.com

https://doi.org/10.30489/cifj.2023.404862.1073

ARTICLE INFO

Article history:
Receive Date: 09 July 2023
Revise Date: 08 August 2023
Accept Date: 08 September 2023

Keywords:
Internet fraud Laxity Cybercrime
Law Enforcement Authorities
Nigeria

ABSTRACT

The increasing reliance on technology and the volatility of cyberspace have greatly aided the prevalence of internet fraud worldwide. In Nigeria, cybercrime—particularly internet fraud—has become one of the most popular forms of deviance among young people, which continues to pose a significant challenge to law enforcement agencies. While there have been various law enforcement reforms and initiatives to combat the menace, internet fraud continues to thrive. This research article investigates the perceived conviviality of law enforcement personnel with internet fraudsters and how it has contributed to a laxity of law enforcement authorities towards internet fraud. Study findings reveal that there is indeed a laxity of law enforcement actions towards internet fraud due to a plethora of institutional and sociological factors. This study also suggests how security agencies can better approach the internet fraud menace.

Introduction

When the Economic and Financial Crimes Commission (EFCC) was established by the Federal Government of Nigeria twenty years ago, its primary objective was to combat the pervasive corruption prevalent amongst public officeholders in the form of money laundering, misappropriation of public funds, official grafts, and other corrupt activities. However, as information technology gained acceptance in Africa, it became apparent that the commission had other criminal activities to combat—internet frauds.

Internet fraud continues to thrive globally as cyber criminals discover new ways to perpetrate fraud. The continued involvement of fraudsters in criminality is also influenced by the belief that they can get away without being caught, given the anonymity offered by cyberspace (Tan, 2002). In response to the rise in computer-related fraud, the Ghanaian government enacted laws and implemented various enforcement actions to combat internet fraud. One such law is the Electronic Transactions Act 2008, supported by the Data Protection Act 2012 and the Cybercrime Act 2020. Of note, the Cybercrime Act penalizes various forms of internet fraud, like phishing, unauthorized access, malware distribution, and other cyber-attacks. On the side of enforcement, the government established the National Cybersecurity Center in 2018 to coordinate the country's cybersecurity efforts.

In Nigeria, despite the various initiatives implemented by the EFCC as well as several legal and regulatory efforts geared towards combating cybercrime (including the enactment of the Cybercrime (Prohibition, Prevention, Etc.) Act 2015 and the repeal and reenactment of the Evidence Act in 2011), internet fraud continues to defy the efforts of law enforcement authorities to curb its growth. The growing incidence of Internet fraud commission in Nigeria presents many sociological problems. For instance, internet fraudsters' adoption of cyber spiritualism is not unconnected to the rise of ritual killings and organ trafficking in the country (Chukwuka, 2022). Unlike the 2010s, when cybercrime in Nigeria was perpetrated mainly by students in tertiary institutions (Tade, 2013), today, cybercrime, especially internet fraud, has gained acceptance even among uneducated youths—teenagers even—in remote or rural communities.

This study suggests that while there are law enforcement actions against perpetrators of internet fraud in Nigeria in the form of arrests, detention and prosecution, there is still a growing laxity towards internet fraud and fraudsters exhibited in varying degrees by the law enforcement agencies and the Nigerian public. Findings indicate that this conviviality is mainly due to many institutional and sociological factors like internal corruption within law enforcement agencies, cyber-spiritualism, volatility of cyberspace, and socioeconomic realities, amongst other factors. This research paper concludes by proffering holistic suggestions on how security agencies can adequately tackle internet fraud.

Review of Related Literature

The extant bodies of literature on internet fraud in Nigeria have focused on the economic cost (Moore et al., 2009; Ibrahim, 2019), motivations, social organization (Tade & Aliyu, 2011), and internet fraud's local and global architecture. Research efforts have also been directed at unravelling its spiritual dimension (Tade, 2013; Alhassan, 2023), introducing a new paradigm into internet fraud discourses. However, not much assessment has been attempted to observe the disposition of law enforcement authorities towards the policing of internet frauds, and how the perceived conviviality is contributing to a laxity of enforcement efforts.

Understanding Internet Fraud

Internet fraud encompasses the various fraudulent activities perpetrated using information technology tools. It involves using deception and/or persuasion to obtain money or valuables from other users in cyberspace. Alnajim (2009) defines it as when the internet is used as the arena to commit fraud. These definitions explain internet fraud as a criminal activity and identify the perpetrators' mode of operation, tools, and terrain. The varieties of applications available on the internet, including electronic mailing, internet messaging, and chat systems, serve as veritable grounds for carrying out fraudulent activities (Ojedokun & Eraye, 2012).

Internet fraud in itself is not a crime but a category of crime (Kävrestad, 2014), which includes but is not limited to phishing, business email compromise, escrow services fraud, counterfeit cheque scams, investment fraud, parcel courier email schemes, dating scams, identity theft, advance fee scams, credit card fraud, contract scams, etc.

Like every other form of cybercrime, law enforcement authorities still do not fully understand internet fraud. Cybercrimes and internet use for illegal activities present a novel challenge that most law enforcement authorities in Nigeria and Africa are not adequately prepared for. In Nigeria, law enforcement's approach to crime fighting is still largely reactive rather than proactive, and this approach to policing has failed at preventing crimes, especially volatile crimes like internet fraud (Ismaila et al., 2019).

The widespread acceptance of internet fraud among Nigerian youths is not recent. In 2012, Ojedokun & Eraye wrote that:

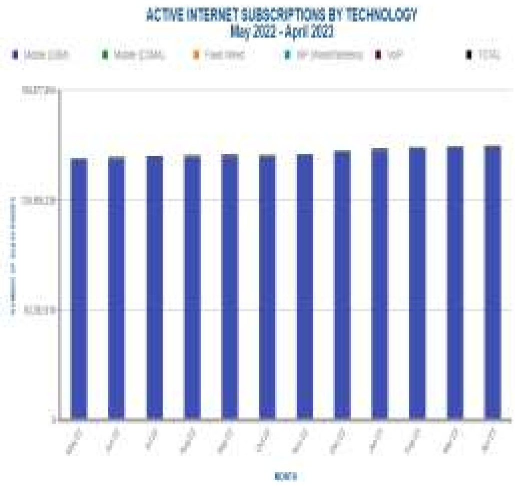
> *"Indeed, the recognition of this growing acceptance of cybercrime, otherwise known as yahoo-yahoo in Nigeria, as a way of life among the youths has compelled the federal government to formulate measures to contain the trend at different points in time. The problem has, however, remained pervasive, despite past efforts put in place to curtail it."* (p 1001)

Internet fraud and other forms of cybercrime continue to thrive yearly. This may not be unconnected to the growth of global connectivity (Chawki et al., 2015). Figure 1 shows a steady increase in active internet subscriptions per telecommunication technology class from May 2022 to April 2023. While internet subscription statistics have ebb and flow since 2019, the figures have undoubtedly been rising steadily in recent years. In 2020, there was an upsurge in internet subscriptions owing to the global pandemic and its resultant lockdowns. The COVID-19 pandemic aided the exponential growth of internet service subscriptions and, by extension, involvement in computer crimes. With the surge in internet subscriptions and increased information technology adoption, internet fraud continues to increase. It has attained a pathological state in crime evolution concerning its incidence and seriousness (Ikuomola, 2011).

Technological innovations like cryptocurrencies have also aided the perpetration of internet fraud as they are volatile (Kerr et al., 2023) and offer criminals more anonymity. Internet fraudsters also prefer cryptocurrency for its decentralized nature, which helps remove the controls banks and regulatory bodies have on the financial system.

Figure 1[1]

NCC's industry statistics on Internet subscription



[1] Note. This Graph from Industry Statistics by the NCC shows the number of active internet subscribers for data (internet) services on each licensed service provider utilizing the different technologies (CDMA, GSM, ISP, etc.). Nigerian Communications Commission (NCC) is the national regulator for the telecommunications industry in Nigeria.

Internet Fraud as a Transnational Phenomenon under International Law

Internet crimes often have a significant transnational component (Arnell & Faturoti, 2023). This is because perpetrators defraud their victims in their own country while laundering the proceeds across international borders. This extraterritorial component presents jurisdictional conflicts between national and international laws, which are often resolved in favor of national laws based on territorial integrity and sovereign equality principles. As a result, the international legal framework on internet financial crimes is largely facilitative rather than mandatory (Nguyen, 2020). For instance, international regulations and conventions like the Budapest Convention on Cybercrime, the United Nations Convention against Transnational Organized Crimes (Palermo Convention), and the United Nations Guidelines for the Regulation of Computerized Personal Data Files all regulate internet fraud and other related crimes only to the extent that national laws admit.

For instance, the Budapest Convention makes extensive provisions on matters including computer-related fraud, illegal access, illegal interception, etc., but only recommends that parties to the convention should adopt legislative and other measures under their domestic laws to ensure compliance. Nevertheless, the treaty introduces the principles of international cooperation (Article 23) and mutual assistance (Article 25) by which parties to the Convention pledge to cooperate and provide mutual assistance to one another in cybercrime investigations.

The Anti-Internet Fraud Law Enforcement Framework in Nigeria

The Police Act places the general crime detection and prevention responsibility on the Nigeria Police Force (s. 4(a)). It further saddles the force with the duty of maintaining law and order in the country. The Act places the police at the forefront of crime fighting in the country. However, the Act further provides:

> *"The Police Force shall— (d) enforce all laws and regulations without any prejudice to the enabling Acts of other security agencies."* (s.4(d))

The above provision, while empowering the force with the duty of enforcing the laws and regulations applicable to it, limits such power. In enforcing the applicable laws and regulations, the police must respect the enabling Acts of other security agencies, significantly where such laws, by their provisions, limit the enforcement oversight of the police.

Notably, the clause "without any prejudice to the enabling Acts of other security agencies" was absent in the repealed Police Act 2004. It was introduced into the 2020 Act to limit the jurisdiction of the police with regard to certain specialized crimes like economic and financial crimes. With the new provision in the 2020 Act, the police are empowered to enforce all laws and regulations in the country only in line with the provisions of the enabling Act of other security agencies. In the context of economic and financial crimes—under which internet fraud falls—the Economic and Financial Crimes Commission (Establishment) Act declares the commission as the coordinator of the fight against economic and financial crimes:

> *"The Commission shall be responsible for—*
> *(c) the coordination and enforcement of all economic and financial crimes laws and enforcement functions conferred on any other person or authority."* (s. 6(c))

Therefore, concerning fraud-related crimes enumerated in section 42 of the EFCC Act, the commission is designated as the chief anti-fraud law enforcement agency. The enforcement oversight of the EFCC includes the power to investigate all financial crimes, including advance fee fraud, online scams, counterfeiting of currencies, money laundering, fraudulent encashment of negotiable instruments, computer credit card fraud, and all other forms of cybercrime insofar as they amount to financial or economic crimes as defined under the Act. The Act in section 46 defines economic and financial crimes as follows:

> *"Economic and Financial Crimes means the non-violent criminal and illicit activity committed with the objectives of earning wealth illegally either individually or in a group or organized manner thereby violating existing legislation governing the economic activities of government and its administration and includes any form of fraud, narcotic drug trafficking, money laundering, embezzlement, bribery, looting and any form of corrupt malpractices, illegal arms deal, smuggling, human trafficking and child labour, illegal oil bunkering and illegal mining, tax evasion, foreign exchange malpractices including counterfeiting of currency, theft of intellectual property and piracy, open market abuse, dumping of toxic wastes and prohibited goods, etc."*

For the effectual prosecution of all financial crimes, the Act goes on to entrust the commission with the responsibility of enforcing the provisions of other laws, including the Advanced Fee Fraud and Other Fraud-Related Offences Act, 2006, Money Laundering (Prohibition) Act 2004, Terrorism Act, Banks and Other Financial Institutions Act 1991, the Miscellaneous Offences Act 1985, the Criminal Code Act, etc. With the enactment of the Cybercrime (Prohibition, Prevention, Etc.) Act in 2015, the EFCC is also saddled with the duty to enforce its fraud-related provisions.

Methods

This study combines both doctrinal and empirical analyses as it examines the statutes and legal frameworks on internet policing in Nigeria whilst investigating responses and insights obtained from research respondents to assess the research question. This study was conducted in Lagos, Abeokuta, and Ibadan—hotspots of internet fraud in Nigeria. The study was conducted between April and June 2023, three months.

Using the Snowball sampling technique to recruit respondents, primary data were sourced from 40 participants, including 25 internet fraudsters, 10 officers of the Nigeria Police Force, and 5 bank employees. No identifying information was collected, and the anonymity of respondents was guaranteed to enhance the volunteering of information. In-depth interviews (IDI) were adopted to elucidate information from the respondents.

Efforts were made to engage officers of the EFCC on the research questions. A letter addressed to the zonal commander of the Ibadan Zonal Command was submitted at the Zonal Office in Iyaganku GRA, Ibadan, Nigeria. In the letter, the purpose and focus of the research were explained and contact information was provided, but all attempts to engage officers of the EFCC were unsuccessful.

Research Findings and Discussions

Study findings show that there exists a rising degree of conviviality between law enforcement personnel and internet fraudsters. As a result, law enforcement agencies have relaxed their efforts and have taken a softer stance towards internet fraud. This helps to create a conducive atmosphere for internet fraudsters and also serves as motivation for new entrants, invariably leading to a proliferation of internet fraud and other forms of cybercrime.

It is also evident that law enforcement actions are not catching up with the growth rate of internet frauds. Internet fraud will continue to thrive if security agencies are miles behind cybercriminals (Makeri, 2017).

Factors Responsible for the Laxity of Law Enforcement Agencies towards Internet Fraud

1. Poor coordination

The EFCC Act places the EFCC at the heart of all anti-fraud law enforcement campaigns with the exclusive power to coordinate the efforts of all other law enforcement agencies concerning economic and financial crimes. This dichotomy has deeply influenced the attitude of the police toward cyber criminals. All the referenced police respondents acknowledged the centrality of the EFCC within the anti-fraud enforcement framework, as evident in the following excerpts:

> *"I am not actually the right person to ask these questions. I don't have any business with them. I don't even arrest them. Have you gone to EFCC?"* (IDI/ /Police officer/Ibadan)

The above response signals an indifference of the police officer towards internet fraud. While the commission maintains pole position with regard to the special crimes under the Act, the police still retain the general responsibility of detecting and investigating crimes under the Police Act and are therefore not relieved of the duty to pursue crimes, internet fraud inclusive.

Another respondent, a police officer in Lagos, said:

> *"The thing is, when they assign us to our different road stations, we don't go there because of Yahoo boys. We go there for different reasons. For instance, we may be tracking a stolen property, searching for a suspect, general inspection or even just to restore calm. So, we don't hunt Yahoo boys, that is the work of EFCC…"* (IDI/Police Officer /Lagos)

The responses from the police officers show an understanding of their limited jurisdiction over internet fraud. However, it also indicates a sense of relinquishment. This sense of relinquishment by the police towards internet fraud is inextricably linked to the societal acceptance and glorification of internet fraud and its perpetrators. In April 2023, Commandant Ayo Olowonihi of the EFCC expressed the dire situation when he said:

> *"The problem we are dealing with is so huge that we now have parents who take their kids out of formal school and enroll them into internet fraud training centers popularly known as Yahoo-Yahoo school* (EFCC, 2023).

This indicates a shift from the study findings of Olabode (2020) which showed that the majority of people do not accept Yahoo boys nor celebrate them in society.

2. Systemic corruption

The Nigeria Police have been linked to several cases of arbitrary arrests, extortion, torture, and bribery. Corruption within the policing sector not only compromises the integrity and legitimacy of the police to tackle crimes; it also discourages security personnel from tackling internet fraud. As a result, the objective changes from fighting crime to making illicit gains from internet criminals, leading to lax enforcement behavior.

From the excerpt below, we can see that the police may not be as tough on internet fraud as they ought or used to be:

> *"When they (police) arrest you, they won't even take you to the station, not to talk of taking you to EFCC. They just want you to settle them. I remember one time when we were returning from an outing last during Covid, they stopped us at Ring Road and asked that we transfer 200k. We were able to beat it down to 45k. That was when they allowed us to leave. Once you settle them you don't have any problem."* (IDI/Internet fraudster/22/Ibadan)

Similarly, the EFCC is not immune from the systemic corruption that is prevalent in the police. The corruption within the EFCC takes a different form, as explained by a respondent:

> *"I don't wish it on even my worst enemy. They (EFCC) don't negotiate with you like the police. They told me to pay a very high amount of money. They know I had the money because they have all these computer investigation tools. Before I knew it, they had seized my car. So, I had no choice."* (IDI/ Internet fraudster/29/Abeokuta)

Similarly, a report on human rights practices in Nigeria stated that the EFCC and the Independent Corrupt Practice and other related offences Commission only target low and middle-level officials suspected of corruption, leaving out high-profile officials (U.S. Department of State, 2022).

3. Damaged police integrity

Cases of police brutality and gross abuse of power by officers of the Nigeria Police and the Nigerian Army have marred the reputation of the force. For a long time, the menace of police brutality was left unaddressed, leading to the #ENDSARS protest in October 2020. However, the protests led by the youth against police brutality led to the convention of judicial panels of inquiry across the country. However, the reports of most of the panels were rejected by the state authorities, further destroying any hope of democratic policing. According to Nwagbara (2023), the rejection by the Lagos state government of the finding of the Panel forecloses any prosecution of members of the Nigerian Army responsible for the massacre and further reinforces the impunity of the Nigerian Army.

In spite of the states' reluctance to admit the atrocities of the security agencies, the protests however led to the disbandment of the Special Anti-Robbery Squad (SARS) which was responsible for most of the reported cases of police brutality. It is observed that the disbandment of SARS left a vacuum in the anti-fraud law enforcement ring. Although the mandate of SARs was strictly to combat violent crimes such as robbery and armed robbery, it had nonetheless acted outside the scope of its mandates to hunt Yahoo-Yahoo boys; using arbitrary arrests, extortion, torture, and in some cases, extrajudicial killings to carry out its unlawful acts.

> *"Back then, I don't go out. There's nowhere you'll go that you won't find SARS and they will bill you at gunpoint. I would just stay indoors and whenever I need to get anything, I call my girlfriend to help me buy them. That time, if SARS catch you, no be small money dem go bill you. But now, I give these normal policemen like 10k and they are my friends now."* (IDI/Internet Fraudster/25/Lagos)

4. New migratory trends among internet fraudsters

As law enforcement agencies continue to clamp down cyber criminals within cities, there has been an increasing outmigration of internet fraudsters from the cities into the more remote parts of town, away from the close view of the commission.

> *"I started Yahoo in 200L when I was in school. Then you had to be extra careful because there was always news of EFCC arrest either in school or somewhere in town. So, when I finished, I didn't think twice before moving down here (Obada, Abeokuta)."* (IDI/Internet fraudster/27/Abeokuta)

Another respondent in Lagos said:

> *"I used to stay at Isolo (Lagos) but the attention was too much. So, I moved to Ikorodu. Even though they come to burst guys once in a while but you can't compare to other places like Lekki, V.I. or even Ikotun. But here, once the police knows your face, they won't disturb you."* (IDI/Internet fraudster/28/Ikorodu, Ogun State)

While the 14 EFCC commands across the federation are situated in city precincts, there are more than 5,000 police commands spread across the country. This means that the police are closer to the retreating internet fraudsters than their counterparts in the EFCC. Despite the statutory hegemony accorded the EFCC to preside and coordinate all anti-internet fraud law enforcement efforts, the police still remain the initial faces of law enforcement (Singh, 2022).

5. Conditions of service differentials

One institutional factor contributing to the lax behaviour of law enforcement personnel towards internet fraud is poor conditions of service and inadequate compensation. This is particularly true of the Nigeria Police Force, whose personnel have lamented their low salaries for many years. EFCC personnel are better remunerated than their police counterparts, and this further explains why the two agencies exhibit varying degrees of laxity towards internet fraud. The relatively lower salaries of the Nigeria Police Force personnel make them more susceptible to corruption than their counterparts in the EFCC. A respondent said:

> *"See, there are too many of them (Yahoo boys) these days. Even young boys of 14 who are still in secondary school are doing it. How many do you want to arrest? How many do you want to take to EFCC? If you want to arrest 20 yahoo boys per day you will find. So sometimes you're like, what's the point of arresting them and sending all of them to EFCC ..."* (IDI/Police Officer/Abeokuta)

Another respondent described the situation from his perspective as a mobile police officer posted as security detail to an EFCC command:

> *"If you stand here (in front of the EFCC complex) long enough, you will see how*

> *some of them (policemen) would drive the Yahoo boys here and inside the car or bus you will see them bargaining with the Yahoo boys. The truth is that no Yahoo boy wants to be brought here, so they would rather settle the officers to buy their freedom."* (IDI/Mobile Police Officer/Ibadan)

6. Developments in Cybercrime: Cryptocurrency and Artificial Intelligence

Cryptocurrency is a heaven for con artists (Chergarova, et al., 2022). It offers online fraudsters the anonymity advantage and helps them to evade the prying eyes of banks and government regulators. Prior to the era of cryptocurrency, the common means of collection of fraud money in Nigeria was the banks (Tade & Aliyu, 2012). This is why the EFCC was structured to have representatives of commercial banks as well as the country's central bank in its membership—to catch cybercriminals at the point of collection. To avoid the attention of security agencies, Yahoo boys would establish rapport with some bank officials who help them to facilitate payment without alerting security agencies. Today, however, cybercriminals can bypass financial institutions and all their layers of security altogether by instructing or persuading their victims to send the monies to their cryptocurrency wallets instead of traditional bank accounts. This makes it harder for law enforcement authorities to track the transmission of large amounts of digital currency (Bray, 2016). An IDI respondent had this to say about the development:

> *"Before when I was still a picker, I used to go to the bank. Before leaving, I would call my friend there. So, once I get in, he would have helped me to package it. But now, I don't even have to step into any bank. I would just tell my client to fund my (cryptocurrency) wallet or even request for gift cards."* (IDI/Internet Fraudster/32/Lagos)

Cryptocurrencies no doubt offer Yahoo boys more anonymity than they enjoyed in the era of Western Union and MoneyGram when they had to establish a link with an insider in the banks. They are now able to carry out their operations and receive their loot without involving any traditional financial institution that could expose them to security agencies. In the Nigerian internet fraud world, gift cards are another popular tender. Cryptocurrencies and gift cards offer internet fraudsters a way to launder illicit money before layering them back into the traditional financial system.

> *"I am more of a vendor these days. I buy different types of gift cards and sell them at a higher rate. In a day I can buy up to $5k worth of gift cards. The thing is, I buy it from them at very cheap rates, depending on the card, and then sell it higher. So even when I am not bombing, I still make my money soft."* (IDI/Internet fraudster/24/Ibadan)

Another respondent offers some insight into the situation and its effect on certain banking transactions:

> *"The most investigated point in online crime is the payment point. That's where the spotlight is. The EFCC, the CBN, and all these regulators have their eyes on us. So, when the fraudster makes contact with a bank to complete a suspicious transaction, they are alerted by way of compliance. Yahoo boys know this, that's why cryptocurrencies are a game-changer for them but bad news for the security agencies. That's why MoneyGram and Western Union transactions have dipped."* (IDI/Bank official/Ibadan)

Fraud, whether virtual or actual, is perpetrated through deception. With artificial intelligence, the possibilities are endless for internet fraudsters who now have deep fake, AI-driven phishing, password guessing, social engineering and other manipulation tools at their disposal. Even before the advent of AI, cybercrimes were sophisticated and evasive. With the introduction of artificial intelligence, these attacks become virtually unstoppable (Guembe et al., 2021), imposing even more strenuous burden on security frameworks.

7. Dwindling level of cooperation by financial institutions

Despite the paradigmatic shift introduced by cryptocurrencies into online scams, banks and other financial institutions still represent an important gateway in financial crimes. This is evident in the rise of Authorized Push Payment scams. In 2022 alone, more than £485 million was lost to APP scams. In Nigeria, the Central Bank of Nigeria (CBN) continues to lament the increasing rate of fraud within the financial services sector, indicting financial institutions for their non-collaboration. In the same vein, banks often choose to save their reputation by hiding fraudulent transactions from law enforcement agencies and the public to avoid the loss of customers. For this same reason, banks hide their own fraud losses (Moore, et al., 2009; UN, 1997). Law enforcement agencies are therefore at a loss for actionable leads to commence their investigation.

Conclusion and Recommendations

Internet fraud has continued to grow in scale globally, and law enforcement authorities are struggling to catch up with the proliferation of the menace. In Nigeria, some degree of conviviality exists between law enforcement personnel and internet fraudsters. This new trend is due to several factors, including the poor service condition of security personnel, which has made them susceptible to corruption. Other factors include poor coordination amongst the various law enforcement authorities and technological innovations aiding the proliferation of fraud, making it difficult for law enforcement agencies to keep up with the growth rate of internet fraud. The EFCC and all other agencies should adopt more intelligence-led operations, cultivate critical local and transnational partnerships toward fighting crime, and wage war against internal corruption while also improving their crime prevention strategies.

The government should try to address the unemployment crisis and other underlying socioeconomic difficulties that incentivize internet fraud. This will help to discourage prospective criminals and will go a long way to reduce the incidence of computer-related fraud in the long term.

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declarations of interest: The authors declare none.

CONFLICT OF INTEREST

The author (s) declares that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancy, have been completely observed by the authors.

OPEN ACCESS

PUBLISHER'S NOTE

CIFILE Publisher remains neutral concerning jurisdictional claims in published maps and institutional afflictions.

REFERENCES

1. Alhassan, A. R. K., Ridwan, A. (2023). Identity Expression—the Case of 'Sakawa' Boys in Ghana. *Hu Arenas* 6, 242–263. https://doi.org/10.1007/s42087-021-00227-w
2. Alnajim, A. M. (2009). *Fighting internet fraud: Anti-phishing effectiveness for phishing websites detection.* [Doctoral thesis, Durham University] Durham e-Theses. http://etheses.dur.ac.uk/2149/
3. Arnell, P., Faturoti, B. (2023). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers & Technology, 37*(1), 29-51. doi:10.1080/13600869.2022.2061888
4. Bray, J. D. (2016). *Anonymity, cybercrime, and the connection to cryptocurrency.* [Online theses and dissertations, Eastern Kentucky University], 344. https://encompass.eku.edu/etd/344/
5. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, digital forensics and jurisdiction*. Cham, Switzerland: Springer.
6. Chergarova, V., Arcanjo, V., Tomeo, M., Bexerra, J., Vera, L. M., & Uloa, A. (2022). Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency. *Issues in Information Systems, 23*(2), 242-252.
7. Chukwuka, O. U. (2022). Internet fraud: The menace of 'yahoo boys' and the deceitfulness of riches. *Sapientia Global Journal of Arts, Humanities and Development Studies, 5*(2), 87-97.
8. Economic and Financial Crimes Commission. (2023, April 6). *EFCC adopts new strategies to curb cybercrime.* https://www.efcc.gov.ng/efcc/news-and-information/news-release/9054-efcc-adopts-new-strategy-to-curb-cybercrime
9. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandex-Sanz, L., and Pospelova, V. (2022). The emerging threat of AI-driven cyber-attacks: A review. *Applied Artificial Intelligence, 36*(1).
10. Ibrahim, U. (2019). The impact of cybercrime on the Nigerian economy and banking system. *NDIC Quarterly, 24*(12), 1-20.
11. Ikuomola, A. D. (2011). Intelligence information and policing in Nigeria: Issues and way forward. *The Journal of*

International Social Research, 4(17), 474-484.

12. Ismaila, I., Legbo, V. Y., Ikuesan, A. R., Imavah, S. A., Mohammad, A. B., Abduldayan, F. J. & Baba, M. (2019). Towards a digital policing in developing nations: The Nigerian context. *International Journal of Innovative Technology and Exploring Engineering, 8*(7), 205-213.
13. Kävrestad, J. (2014). *Defining, categorizing and defending against online fraud.* [Master's thesis, University of Skövde] DiVA Portal. https://www.diva-portal.org/smash/get/diva2:738375/FULLTEXT01.pdf
14. Kerr, D. S., Loveland, A. L., Smith, K. T., & Smith, L. M. (2023). Cryptocurrency risks, fraud cases, and financial performance. *Multidisciplinary Digital Publishing Institute, 11*(3), 1-15. https://doi.org/10.3390/risks11030051
15. Makeri, Y. A. (2017). Cyber security issues in Nigeria and challenges. *International Journal of Advanced Research in Computer Science and Software Engineering, 7*(4), 315-321.
16. Moore, T., Clayton, O., & Anderson, R. (2009). The economics of online crime. *Journal of Economics Perspectives, 23*(3), 3-20. doi:10.1257/jep.23.3.3
17. Nguyen, C. (2020). National criminal jurisdiction over transnational financial crimes. *Journal of Financial Crime, 27*(4), 1361–1377. doi:10.1108/jfc-09-2019-0117
18. Nigerian Communications Commission. (2023). *Active internet subscriptions by technology in Nigeria, from May 2022–April 2023* [Graph]. Retrieved June 12, 2023.
19. Nwagbara, I. T. (2023). Impunity: An impetus for repeated atrocities Nigerian Army as a case study. *CIFILE Journal of International Law 4*(7), 62-79.
20. 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.
21. Olabode, T. K. (2020). Yahoo-Yahoo practice: A sociological commentary on the acceptability and celebrity of the actors in Nigeria. *A Covenant Journal of Business and Social Sciences, 11*(2). https://doi.org/10.20370/cjbss.v11i2.2422
22. Singh, D. (2022). The causes of police corruption and working towards

prevention in conflict-stricken states. *Multidisciplinary Digital Publishing Institute, 11*(5), 1-19. https://doi.org/10.3390/laws11050069

23. Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860-875.
24. Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, *23*(4), 689-705. https://doi.org/10.2478/s13374-013-0158-9
25. Tan, H. S. K. (2002). E-fraud: Current trends and international developments. *Journal of Financial Crime, 9*(4), 347-354.
26. United Nations. (1997). *International review of criminal policy – United Nations manual on the prevention and control of computer related crime.* Para. 29.
27. U. S. Department of States. (2022). *2022 country reports on human rights practices: Nigeria.* *https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/nigeria/*