Journal of Law and Intellectual Property Rights
ISSN: 3049-0979, Volume 3 Number 1 (June' 2026) pp. 1–8
DOI: https://doi.org/10.66566/jlipr/2026.v3n1.01
Journal website: https://www.jlipr.in

Received: 24 Nov' 2025 | Revised: 03 Feb' 2026 | Accepted: 12 Feb' 2026 | Published: 01 Jun' 2026

OPEN ACCESS

Review Article

Economic Implications of Cyber Crime as a Predominant Financial Crime in Nigeria

Ogwu James Onoja

Senior Lecturer, Bingham University, Abuja, Nigeria.

Email: ojonoja@gmail.com

ABSTRACT: ***Cybercrime is a pervasive financial crime in Nigeria that had significant implications for the country's economy. This study examined the nature, causes, and consequences of cybercrime in Nigeria, focusing on the regulatory framework and measures to combat it. The research adopted a doctrinal approach, analyzing secondary data from reputable sources. The findings revealed that cybercrimes such as online fraud, cyber-enabled financial crimes, and data breaches were often perpetrated through phishing, hacking, and other forms of cyber-attacks, resulting in substantial financial losses. The study recommended strengthening cybersecurity measures, enhancing law enforcement capabilities, and increasing public awareness to combat cybercrime. Collaboration between regulatory bodies, financial institutions, and international organizations was also suggested to effectively tackle the menace. In conclusion, cybercrime was a serious financial crime in Nigeria that required concerted efforts from all stakeholders to combat.***

KEYWORDS: ***Cyber Crime, Financial Fraud, Legal System, Law Enforcement, Nigeria.***

INTRODUCTION

Cybercrime is a significant financial crime that involves using technology to commit financial fraud, theft, or deception, resulting in financial losses or gains for the perpetrator, often through methods like hacking, phishing, and malware. Cybercrime and financial fraud have become pressing concerns in Nigeria, posing significant threats to economic stability and national security. The rapid advancement of digital technologies has provided new opportunities for cybercriminals to exploit financial systems. Cybercriminals exploit weaknesses in financial institutions, government agencies, and individual users to commit fraud, identity theft, hacking, and other offenses. The financial losses resulting from these activities are substantial, affecting both individuals and organizations.[1]

In Nigeria, cybercrime is not only a financial issue but also a reputational one, as the country has gained notoriety for fraudulent online schemes, such as advance-fee fraud (419 scams). Despite government efforts to curb cybercrime through legislation and enforcement, cybercriminals continue to evolve, leveraging sophisticated methods to evade detection.[2]

[1] Esa O. Onoja '*Economic Crimes in Nigeria: Issues and Punishment*' (Lawlords Publications 2018) 151.
[2] Ibid.

IMPACT OF CYBERCRIME AND FINANCIAL CRIME IN NIGERIA

Economic Impact

Cybercrime results in significant financial losses to businesses, individuals, and the government. The Cyber-Security Association of Nigeria reported that cybercrime from Nigeria hit USD 9.3 Billion yearly.[3] According to Central Bank of Nigeria, electronic payment fraud alone is responsible for the loss of N4 Billion since 2012.[4] Cybercrime accounted for about 43% of total monetary loss due to fraud in 2016. These losses have negative impacts on individuals, businesses and the government in terms of welfare losses, business disruption, profit reduction/rising operating cost and revenue losses.[5] Cybercrime and fraudulent financial practices also distort markets, creating unfair advantages and eroding investor confidence. These issues can deter investments and reduce economic growth.[6]

Impact on Governance and Institutions

Cybercrimes and Financial Fraud in Nigeria have undermined public trust in government institutions such as; banks, and other corporations. Citizens have become skeptical of governance, leading to diminished political engagement.[7] Banks and financial institutions suffer reputational damage and financial losses due to cyber fraud. Fraudulent transactions lead to increased operational costs as banks invest in advanced cybersecurity measures. According to KPMG (2021)[8], Nigerian banks lose millions annually to cyber fraud, despite improved security protocols.

Impact on Businesses

Businesses that are implicated in cybercrimes and financial fraud have suffered reputational harm, leading to loss of consumer trust and decreased market value[9]. The collapse of Enron in 2001 demonstrated the devastating impact of fraudulent accounting on a company's reputation and survival. Now Companies must invest heavily in compliance systems and risk management to prevent and detect financial crimes, thereby increasing operational costs[10].

Global Impact

Nigeria's global reputation as a cybercrime hub discourages foreign investors. Many international firms are hesitant to engage in digital transactions or partnerships with Nigerian businesses due to the risks associated with cyber fraud. International perception of the level of victimization by fraudsters generally, and alleged Nigerian cybercriminals is so acute that some embassies warn their citizens that they can shake the hands of Nigerians but that they should count their fingers afterwards.[11] A study by KPMG (2021) found that 63% of foreign investors

---

[3] Rotimi Afon, President, Cyber-security Association of Nigeria (CSEAN) *The Nation Newspaper,* 30th October, 2015.

[4] Central Bank of Nigeria, "Electronic payment fraud hits N4bn" *Daily Trust Newspaper,* 28th October, 2015 p. 9.

[5] Umar Ibrahim "*The Impact of Cybercrime on the Nigerian Economy and Banking System*' (2019) <https://nigeriareposit.nln.gov.ng/server/api/core/bitstreams/ea0f0242-ce94-47ad-9257-7d1304e39a1f/content> accessed on 6th May, 2025.

[6] Ibid.

[7] Saddiq, S.A. and Abu Bakar, *A.S., "Impact of economic and financial crimes on economic growth in emerging and developing countries: A systematicreview", Journal of Financial Crime, [2019] (26)(3), pp. 910-920. <https://doi.org/10.1108/JFC-10-2018-0112> accessed on 2nd February, 2025.*

[8] KPMG '*Cyber Security and Financial Fraud in Nigerian Banking Sector' (*2021) <https://kpmg.com/ng> accessed 6th February, 2025.

[9] Ibid.

[10] Ibid.

[11] Ibid.

perceive Nigeria as a high-risk environment for digital transactions, leading to a decline in foreign direct investment (FDI) in key sectors, such as fintech and banking.[12]

Impact on National Security

Cybercriminals have hacked government institutions, leading to data breaches and loss of sensitive information. In 2020, the Nigerian Immigration Service (NIS) database was hacked, exposing the personal details of thousands of Nigerians. Government websites, including those of the CBN, EFCC, and INEC, have been targeted by hackers seeking financial or political gains[13]. Cybercrime and financial fraud have been linked to money laundering and illicit financial flows. The Nigerian Financial Intelligence Unit (NFIU, 2021) reported that Nigerian cybercriminals launder millions of dollars annually through cryptocurrency, offshore accounts, and shell companies[14]. Terrorist groups such as Boko Haram and bandit groups use cyber fraud to fund criminal activities.

CAUSES OF CYBERCRIMES AND FINANCIAL FRAUD

The following are some of the identified causes of cyber-crime and financial fraud in Nigeria.

Unemployment

Unemployment is one of the major causes of Cybercrimes and Financial Fraud in Nigeria. It is a known factthatover20milliongraduatesin the country does not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.

Greed and Impatience

Quest for Wealth is another cause of cybercrime and Financial Fraud in Nigeria. Youths of nowadays are very greedy, they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.

Lack of strong Cyber Crime Laws

Lack of strong Cyber Crime Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.

Incompetent Security on Personal Computers

Some personal computers do not have proper or competent security controls[15]; it is prone to criminal activities hence the information on it can be stolen[16].

[12] Ibid.

[13] INTERPOL '*Cybercrime and Organized Fraud Networks in West Africa'* (2021) <https://www.interpol.int/> accessed on 6th February, 2025.

[14] Nigerian Financial Intelligence Unit (NFIU). "*Illicit Financial Flows and Money Laundering in Nigeria'* (2021) <https://www.nfiu.gov.ng> accessed 6th February, 2025.

[15] Hassan, A. B. Lass F. D. and Makinde J. 'Cybercrime in Nigeria: Causes, Effects and the Way Out', ARPN Journal of Science and Technology, (2012) 2(7), 626-631.

[16] Ibid.

LEGAL AND REGULATORY FRAMEWORKS FOR COMBATING CYBERCRIME AND FINANCIAL FRAUD IN NIGERIA

Cybercrime and financial fraud have become major challenges in Nigeria, prompting the government to establish legal and regulatory frameworks to combat them.[17] These frameworks consist of laws, institutions, and international collaborations aimed at preventing, detecting, and prosecuting cybercriminals. This section examines the major laws and institutions responsible for combating cybercrime and financial fraud in Nigeria.[18]

Cybercrime (Prohibition, Prevention, etc.) Act, 2015

The Cybercrime Act (2015) is the cornerstone of Nigeria's legal response to cybercrime. It provides a comprehensive legal framework for prohibiting, preventing, investigating, and prosecuting cyber offenses such as; hacking, cyber stalking, identity theft, and financial fraud, etc. prescribing penalties ranging from fines to imprisonment.[19] The Act empowers law enforcement agencies including EFCC, to investigate and prosecute cybercrimes and also mandates cooperation with international agencies to combat global cybercrime.

The Economic and Financial Crimes Commission (Establishment) Act, 2004

The Economic and Financial Crimes Commission (EFCC) Act established the EFCC as Nigeria's primary agency to enforce the Act and adopt measure to combat economic and financial crimes by investigating and prosecuting all financial crimes including; advance fee fraud, money laundering, counterfeiting, illegal charges transfers, and all types of fraud.[20]

Money Laundering (Prevention and Prohibition) Act, 2022

This Act criminalizes money laundering, which is closely linked to cybercrime and financial fraud and provides mechanisms for combating same through investigation, prosecution and punishment of same. The Act imposes an obligation on financial institutions to report suspicious transactions and imposes penalties for non-compliance with reporting obligations.[21]

The Nigerian Data Protection Act, 2023

This Act regulates the collection, processing, and storage of personal data to prevent identity theft and online fraud. The Act requires organizations to protect user data from breaches, and also criminalizes unauthorized access, disclosure, or misuse of personal data. It also mandates financial institutions and telecom operators to enhance cyber security measures[22]. The Nigeria Data Protection Commission (NDPC) oversees enforcement, but low compliance remains a challenge.

Central Bank of Nigeria Act 2007

This Act established the Central Bank of Nigeria with the principal function of currency regulation in order address financial fraud among other vices. The Act regulates financial

[17] Ibid.
[18] Ibid.
[19] Section 1 Cybercrimes (Prohibition, Prevention, etc.) Act 2015.
[20] EFCC, '*About Us*' <https://www.efcc.gov.ng/efcc/about-us-new/the-establishment-act> accessed on 6th February, 2025.
[21] A. D. Boyer and S. Light *"Dirty Money and Bad Luck: Money Laundering in the Brokerage Context" Virginia Law & Business Rev.* (3)(1) [2008] at pp. 84-85.
[22] Section 1 National Data Protection Act 2023.

institutions in Nigeria through guidelines and regulations some of which requires Banks and other financial institutions to strengthen digital security measures and report cyber incidents.[23]

Nigerian Communication Commission (NCC) Regulations

The Nigerian Communication Commission regulates the telecommunications industry, which is vital in combating cybercrime. Its regulations require service providers to implement security measures that can help deter cyber offenses in Nigeria[24].

Advance Fee Fraud and Other Fraud Related Offenses Act, 2006

This law addresses financial, particularly 419 Scams, commonly associated with advance fee fraud schemes. It prescribes penalties for obtaining property or money through false pretense and criminalizes fraudulent business schemes.

Independent Corrupt Practices and Other Related Offenses Commission (ICPC) Act

This Act established the Independent Corrupt Practices and Other Related Offenses Commission (ICPC) which is primarily responsible for preventing, investigating, and prosecuting corruption-related offenses. The Act empowers the ICPC to probe individuals suspected of illicit wealth accumulation.

REGULATORY FRAMEWORK IN NIGERIA

Economic and Financial Crimes Commission (EFCC)

The EFCC is the primary agency for investigating and prosecuting financial crimes in Nigeria which include fraud and cybercrimes. The Commission as part of their responsibilities enforce financial regulations, conduct investigations into financial crimes and collaborate with other law enforcement and regulatory bodies to address all forms of financial crimes which include cybercrimes and financial fraud.[25]

Nigerian Police Force (NPF)

The Nigerian Police Force has a specialized unit known as 'Cybercrime Unit' for investigating cyber-related offenses, carry out arrests and prosecutions of cybercriminals[26]. The unit also collaborates with international law enforcement agencies to achieve their aim and objective.

Nigerian Communications Commission (NCC)

The Nigerian Communications Commission (NCC) regulates the telecommunications industry and ensures compliance with security protocols among service providers.[27] The Commission enforces regulations to protect data and mitigate cyber threats. It also promotes public awareness initiatives about cyber security.

[23] Central Bank of Nigeria *'Statement of Core CBN Mandate'*<https://www.cbn.gov.ng/AboutCBN/> accessed 7th February, 2025.

[24] Nigerian Communication Commission (NCC) *'Regulations'*<https://ncc.gov.ng/licensing-regulation/legal/regulations> accessed on 7th February, 2025.

[25] Ibid.

[26] Nigerian Police Force National Cybercrime Center *'About Us'*<https://nccc.npf.gov.ng/page/about-us> accessed on 7th February, 2025.

[27] Joe NMLC 'Nigerian Communication Commission' *Wikipedia* <https://en.m.wikipedia.org/wiki/Nigerian_Communications_Commission> accessed on 7th February, 2025.

National Information Technology Development Agency (NITDA)

The National Information Technology Development Agency formulates policies to develop Information Technology (IT) in Nigeria and oversees data protection regulations. As part of the functions of the commission, they promote cyber security awareness, implement the cyber security policies, and encourages the adoption of cyber security measures across sectors.[28] The Agency has a department known as 'Cyber Security' which carries out those functions.

Central Bank on Nigeria (CBN)

The Central Bank of Nigeria oversees the banking sector and financial institutions. It issues guidelines for safe electronic payment systems, and regulates financial institutions to prevent fraud and ensure compliance with anti-money laundering standards.[29]

Independent Corrupt Practices and Other Related Offenses Commission (ICPC)

The Independent Corrupt Practices and Other Related Offenses Commission (ICPC) is one of Nigeria's foremost anti-corruption agencies, established by the Independent Corrupt Practices and Other Related Offenses Commission (ICPC) Act, 2000. The Commission is primary responsible for preventing, investigating, and prosecuting corruption-related offenses which are forms of financial fraud in Nigeria, and involve cybercrime in some cases.

GLOBAL EFFORTSTOWARDS COMBATING CYBER CRIME

International Cooperation and Agreements

International cooperation is essential in combating cybercrime, as it enables countries to share information, coordinate investigations, and harmonize laws. Several international agreements and organizations play a crucial role in facilitating this cooperation.

a. Budapest Convention: The Council of Europe's Convention on Cybercrime (2001) is a landmark treaty that aims to harmonize cybercrime laws and facilitate international cooperation.[30]The Convention has been ratified by 66 countries, including the United States, Canada, and many European countries.[31]

b. United Nations: The UN has been actively involved in addressing cybercrime through various initiatives, including the UN Congress on Crime Prevention and Criminal Justice.[32] The UN has also established the UNODC (United Nations Office on Drugs and Crime) Cybercrime Programme to provide technical assistance to countries.[33]

c. G20 and G7: These forums have recognized the importance of international cooperation in combating cybercrime and have made commitments to enhance collaboration.[34] The G20 has established a working group on cybercrime, which focuses on improving international cooperation and developing best practices.[35]

[28] Brovic, *'National Information Technology Development Agency' Wikipedia* <https://en.m.wikipedia.org/wiki/National_Information_Technology_Development_Agency> accessed on 7th February, 2025.
[29] Ibid.
[30] Council of Europe. (2001). *Convention on Cybercrime.*
[31] Council of Europe. (2022). *Chart of signatures and ratifications of Treaty 185.*
[32] United Nations. (2020). *Combating Cybercrime.*
[33] UNODC. (2020). *Cybercrime Programme.*
[34] G20. (2017). *G20 Leaders' Declaration: Shaping an interconnected world.*
[35] G20. (2020). *G20 Cybercrime Working Group.*

Capacity Building and Training

Capacity building and training are essential for law enforcement agencies and other stakeholders to effectively combat cybercrime. Several organizations provide training programs and capacity-building initiatives.

a. Cybercrime Training Programs: Organizations like the International Association of Chiefs of Police (IACP) and the National Cyber-Forensics & Training Alliance (NCFTA) offer training programs for law enforcement agencies.[36] These programs cover topics such as digital forensics, cybercrime investigation, and cybersecurity.

b. Capacity Building Initiatives: The Global Forum on Cyber Expertise (GFCE) and the International Telecommunication Union (ITU) provide capacity-building initiatives for countries to enhance their cybercrime prevention and investigation capabilities.[37] These initiatives include training programs, technical assistance, and policy development.

Public-Private Partnerships

Public-private partnerships are critical in combating cybercrime, as they enable governments, private companies, and civil society to share information and coordinate efforts.

a. Information Sharing: Public-private partnerships facilitate information sharing between governments, private companies, and civil society to enhance cybercrime prevention and investigation.[38] For example, the Cybersecurity Information Sharing Act (CISA) in the United States enables private companies to share cybersecurity threat information with the government.[39]

b. Industry-Led Initiatives: Companies like Microsoft and Google have launched initiatives to combat cybercrime, such as the Microsoft Digital Crimes Unit and Google's Threat Analysis Group. These initiatives include threat intelligence, incident response, and cybersecurity research.

Law Enforcement Collaboration

Law enforcement collaboration is essential in combating cybercrime, as it enables agencies to share information, coordinate investigations, and apprehend cybercriminals.

a. Europol and Eurojust: These EU agencies have established dedicated cybercrime units to facilitate cooperation among European law enforcement agencies. Europol's European Cybercrime Centre (EC3) provides threat intelligence, incident response, and training to EU member states.

b. Interpol: Interpol has a dedicated cybercrime unit that provides training, technical assistance, and operational support to its member countries. Interpol's Cybercrime Directorate focuses on combating cybercrime, including online child exploitation, cyber terrorism, and cyber-enabled financial crime.

Challenges and Future Directions

Despite the progress made in combating cybercrime, several challenges remain.

[36] IACP. (2020). *Cybercrime Training Programs.*
[37] GFCE. (2020). *Capacity Building Initiatives.*
[38] Microsoft. (2020). *Cybersecurity Policy Framework.*
[39] US Congress. (2015). *Cybersecurity Information Sharing Act* (CISA).

a. Jurisdictional Issues: Cybercrime investigations often involve multiple countries, highlighting the need for clear jurisdictional frameworks. The lack of harmonization in cybercrime laws and procedures can create challenges for international cooperation.

b. Resource Constraints: Many countries lack the resources and expertise to effectively combat cybercrime. The need for capacity building and training is critical to enhance cybercrime prevention and investigation capabilities.

c. Emerging Technologies: The rapid evolution of technologies like artificial intelligence, blockchain, and the Internet of Things (IoT) presents new challenges for cybercrime prevention and investigation. These technologies can be used for malicious purposes, such as spreading malware or conducting DDoS attacks.

Several examples demonstrate the effectiveness of international cooperation in combating cybercrime.

a. Operation Aurora: A global operation led by Europol and involving law enforcement agencies from several countries resulted in the takedown of a major malware network. The operation involved coordination between law enforcement agencies and private companies.

b. Takedown of Darkode: A joint operation by US and international law enforcement agencies resulted in the shutdown of Darkode, a notorious cybercrime forum. The operation involved coordination between law enforcement agencies and demonstrated the effectiveness of international cooperation in combating cybercrime.[40]

CONCLUSION

Cybercrime was a significant financial crime in Nigeria, with substantial financial losses to individuals, businesses, and the government. The research revealed that cybercrimes such as online fraud, cyber-enabled financial crimes, and data breaches were often perpetrated through phishing, hacking, and other forms of cyber-attacks. To combat cybercrime, the study recommended strengthening cybersecurity measures, enhancing law enforcement capabilities, and increasing public awareness. Regulatory bodies and financial institutions should collaborate with international organizations to share best practices and effectively tackle these crimes. In conclusion, cybercrime was a serious financial crime in Nigeria that required concerted efforts from all stakeholders to combat. Strengthening cybersecurity measures, enhancing law enforcement, and promoting public awareness were essential to mitigate the impact of cybercrime on Nigeria's economy.

[40] US Department of Justice. (2015). *Operation Darkode.*