The Cybercrimes (Prohibition, Prevention, etc.) Amendment Act 2024 - Insights into Key Amendments

SEPTEMBER 2025

Introduction

The digital revolution that began in the late 1900s has blossomed in this century aided by a rapid growth in technological advancement, a growth that has successfully disrupted the traditional brick-and-mortal approach of everyday activities. This growth has been precipitated by the surge in online activities, some of which have led to insurmountable feats and increased output and productivity in virtually every sector of the economy.[1] The digital revolution has also been used by bad faith actors to destabilize industries and sectors by using the new digital tools to perpetrate traditional and emerging crimes. Since the advent of the digital revolution, there have been numerous incidences of advanced fee fraud, hacking, data privacy violations, tampering of financial institutions, telecommunication satellites, digital impersonation etc.[2] These issues are not alien to Nigeria, to that end, the Nigerian government enacted the Cybercrimes (Prohibition, Prevention, etc) Act 2025 to address some of these issues and create a regulatory framework and procedural mechanism for cyber related crimes and activities.

Digitalization is a hydra-headed monster that keeps on growing as man continues to innovate and stretch the boundaries of possibilities, it became imperative that the Act be amended to cater for some of the risks rising from continued innovation such as data privacy issues, cyber issues, banking and financial issues etc. Owing to increased cyber threats, risks and issues prevalent in the current digital age, it became necessary to provide further protection to amend ambiguous provisions; address insufficiency of the Principal Act; address factors that have impeded the effective implementation of the Principal Act; bolster Nigeria's cybersecurity framework; safeguard Nigeria's CNII; combat terrorism and violent extremism; enhance national security; and protect Nigeria's economic interests.

[1] Amber Pariona, 'What Was The Digital Revolution?' (World Atlas, 25 April 2017) <https://www.worldatlas.com/articles/what-was-the-digital-revolution.html> accessed 15 September 2025.

[2] Robert Muggah, 'The Dark Side of Digitalization - and How to Fix It' (World Economic Forum, 23 September 2020) <https://www.weforum.org/stories/2020/09/dark-side-digitalization/> accessed 15 September 2025.

This led to a legislative review of the Act which culminated into the Cybercrimes (Prohibition, Prevention, etc.) Amendment Act, 2024 (the "Amendment Act"). A year into the enactment of the Amendment Act, this publication provides insight into key provisions and innovations introduced by the Amendment Act.

Key Provisions in the Amendment Act

The Amendment Act clarified ambiguities in language and intention of the draftsmen and also established several mechanisms to aid the fight against cyber threats. They are:

1. Reporting of Cyber Threats

Pursuant to **section 3** of the Amendment Act,[3] any individual or institution facing a cyberattack, intrusion, or disruption must notify the National CERT via their respective Sectoral CERTs or SOCs within 72 hours of detection. Failure to comply will result in denial of internet access and a mandatory fine of ₦2,000,000 (Two Million Naira) payable to the NCF. This swift escalation to the National CERT aims to mitigate cyber threats promptly, thus preventing disruptions of the cyberspace.

2. Implementation of the Cybersecurity Levy

Section 44(1)(2)(a) of the Principal Act[4] establishes a fund known as the National Cyber Security Fund and provides for a levy of 0.005% to be paid and credited into the fund by businesses specified in the second schedule to the Principal Act.[5] This provision was not implemented due to the ambiguity in its wordings particularly the figure which did not reflect the intentions of the draftsman. This ambiguity was cured by section 4 of the Amendment Act which provided that a levy of 0.5% (0.005%) equivalent to half a percent of all

[3] Cybercrime (Prevention, Prohibition, Etc) (Amendment) Act 2024 (the "Amendment Act'), section 3.
[4] Cybercrime (Prevention, Prohibition, Etc,) Act 2015 (the "Principal Act'), section 44(1)(2)(a).
[5] Businesses stated in the Second Schedule to the Act includes: GSM service providers, telecommunication companies, internet service providers, banks, financial institutions, insurance companies, and the Nigerian Stock Exchange.

electronic transactions value by the business specified in the second schedule to the (principal) Act. Additionally, **section 44(6)(a)** of the Principal Act was amended by the Amendment Act to the effect that it empowered the Office of the National Security Adviser (ONSA) to administer, keep proper records of the accounts and ensure compliance monitoring mechanism.

In executing the implementation of the levy, the CBN issued a circular on the Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy (the "Circular").[6] The Circular provided a framework for remitting the required levy by mandating the collection and remittance of the cybersecurity levy to the National Cybersecurity Fund administered by ONSA. The Circular instructed Banks and Financial institutions to apply the levy at the point of electronic transfer origination and remit it to the fund, except for transactions listed in Appendix 1 of the Circular.[7] This meant that levy only applied to the sender unlike other subsidiary electronic charges that accrued to both sender and recipient. According to government sources, the essence of the creation of the fund is to fund the counterterrorism efforts of the federal government.

The cybersecurity levy was heavily criticized due to the negative impact it will have on customers of banks and financial institutions in Nigeria and undermine the CBN cashless policy drive.[8] Following the House of Representatives statement to the CBN to withdraw its circular on the cybersecurity levy, President Bola Ahmed Tinubu directed ONSA to suspend the implementation

---

[6] CBN, 'Circular to all Commercial, Merchant, Non-interest and Payment Service Banks; Other Financial Institutions, Mobile Money Operators and Payment Service Providers' (CBN, 6 May 2024) <https://www.cbn.gov.ng/Out/2024/CCD/CIRCULAR%20REF%20PSMDIRPUBLAB017004%2006052024.pdf> accessed 15 September 2025.

[7] Transactions excluded include loan disbursement and repayments, salary payments, intra-account transfers within the same bank or different banks for the same customer, intra-bank transfers between customers of the same bank, other financial institutions (OFIs) instructions to their correspondent banks, interbank placements, banks' transfers to CBN and vice-versa, Inter-branch transfers within a bank, cheques clearing and settlements, Letters of credits, Bank's recapitalization related funding – only bulk funds movement from collection accounts, savings and deposits including transactions involving long-term investments such as treasury bills, bonds and commercial papers, government social welfare programs.

[8] Emmanuel Ochayi, 'Why Cybersecurity levy Will Worsen Nigeria's Hardship-NLC, TUC' (Prime Business Africa, 8 May 2024) <https://www.primebusiness.africa/why-cybersecurity-levy-will-worsen-nigerias-hardship-nlc-tuc/> accessed 15 September 2025.

of the levy.[9] Finally, the CBN withdrew its circular on the cybersecurity levy.[10]

3. Manipulation of ATM/POS Terminals

Section 30 of the Principal Act limited payment systems to Automated Teller Machines (ATMs) and Point of Sale (POS) terminals, while ignoring several other payment technologies used in Nigeria. **Section 7** of the Amendment Act closes this gap by holding individuals accountable for manipulating not only ATMs and POS terminals, but also other payment technologies. This extension supports Nigeria's varied range of payment systems, offering full coverage while lowering the fraud risks associated with unorthodox payment methods.

4. Inclusion of the requirement of National Identification Number (NIN)

Section 8 of the Amendment Act adds the words "National Identification Number (NIN) issued by the National Identity Management Commission and other valid" to **section 37(1)(a)** of the Principal Act, which therefore requires clients performing electronic financial transactions at financial institutions to present their National Identification Number (NIN) issued by the National Identity Management Commission (NIMC) for identity verification.This requirement intends to speed up the tracing of defaulters or criminals by utilizing NIN, which contains individual data such as physical addresses. However, there are concerns that deployment will be difficult because defaulters may use authentic NINs to build deceptive locations.

5. Protection of Specific Traffic Data and Subscriber Information

Section 9 of the Amendment Act amends **Section 38(1)** of the Principal Act by creating a new subsection 1 with the effect of reconciling it with the Nigeria Data Protection Act (NDPA). Service providers are now obligated to not only

[9] Deji Elumoye, 'Tinubu Suspended Cybersecurity Levy Implementation To Ease Economic Hardship, Says Presidency' (Arise News, 13 May 2024) <https://www.arise.tv/tinubu-suspended-cybersecurity-levy-implementation-to-ease-economic-hardship-says-presidency/> accessed 15 May 2025.

[10] Aghogho Udi, 'CBN withdraws circular on cybersecurity levy' (Nairametrics, 19 May 2024) <https://nairametrics.com/2024/05/19/cbn-withdraws-circular-on-cybersecurity-levy/> accessed 15 September 2025.

store specific traffic data and user information, but also to protect it. This amendment underlines the government's commitment to protecting data and subscriber information, and it reinforces the data security and privacy agenda.

6. Establishment of Sectoral Computer Emergency Response Teams (CERT) and Sectoral Security Operation Centres (SOC)

Section 10 of the Amendment Act establishes Sectoral Computer Emergency Response Teams (CERTs) and Security Operation Centres (SOCs) that will work alongside the National CERT described in the Principal Act. These Sectoral CERTs and SOCs are responsible for gathering information from individuals or institutions operating public or private computer systems or networks in the event of a cyberattack or outage. Their major role is to respond immediately to such occurrences.In addition, they will manage the integration and routing of internet and data traffic from all public and commercial enterprises to ensure national cyberspace security.

Conclusion

The Amendment Act reflects Nigeria’s evolving response to the complexities of digitalization by strengthening existing safeguards, introducing innovative mechanisms for enforcement, and aligning domestic regulation with global standards. While its provisions on data protection, response to cyber threats and jurisdictional reach mark a significant leap forward in addressing contemporary threats, the effectiveness of the Act will ultimately hinge on robust implementation, inter-agency collaboration, and continuous adaptation to technological change.

OUR SERVICES

Anti-Counterfeiting | Copyright | Commercial IP | Trademarks | Patents | IP Liigation & Disputes | Designs | Domain Names | IP Advisory

CONTACT US:

Continental Re Centre, 17 Olosa Str. Victoria Island, Lagos, Nigeria

+2348107251119

info@necs-legal.com

NECS-Legal