The Cybercrimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024 – A Primer on Key Amendments

www.doa-law.com

Introduction

Nigeria stands at the forefront of a digital revolution, characterized by its swift adoption of digital technologies across diverse sectors. However, amidst this technological advancement, the digital age has ushered in new avenues and tools for perpetrating both traditional and emerging forms of crime. In Nigeria, there has been a notable increase in internet-based advance fee fraud hacking and infringements on the privacy rights of individuals and institutions. These challenges demand urgent solutions. According to the Central Bank of Nigeria (CBN), a staggering 70% of attempted or successful fraud/forgery cases in the Nigerian banking system stem from electronic channels. Perpetrators increasingly exploit the proliferation of online transactions, e-commerce platforms, and electronic messaging systems to engage in illicit activities[1].

In a bid to address these complexities associated with cybercrimes, Nigeria enacted the Cybercrime (Prohibition, Prevention, Etc.) Act 2015 (the "**Principal Act**"). The primary objectives of the Act are to establish a comprehensive legal, regulatory, and institutional framework for combating cybercrimes effectively as well as safeguarding Critical National Information Infrastructure (CNII), enhance cybersecurity measures, and protect various aspects of digital assets such as computer systems, networks, electronic communications, data, intellectual property, and privacy rights.

Despite the enactment of the Principal Act and the sustained efforts to eliminate cybercrimes, cybercrimes continue to be on the increase taking innovative forms. Responding to this urgent need, legislators have undertaken a review of the Principal Act 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.

The legislative review led to the enactment of the Cybercrimes (Prohibition, Prevention, etc.) Amendment Act, 2024 (the "**Amendment Act**")[2]**.** This newsletter examines the key provisions and innovations introduced by the Amendment Act, exploring its impact on both Nigerians and the broader cyberspace landscape upon implementation.

Key Provisions in the Amendment Act

1. Implementation of the Cybersecurity Levy

Section 44(2)(a) of the Principal Act established a levy of 0.005 on electronic transactions for businesses listed in the second schedule of the Principal Act[3]. However, compliance with this provision has been lacking due to ambiguity in its wording, particularly regarding the figure 0.005, which does not accurately reflect the intention of the draftsmen of the Act. The Amendment Act addresses this issue by revising the subsection to specify that the levy shall

[1]ThisDay, 'Beyond amending the Cybercrime Act' Available at: https://www.thisdaylive.com/index.php/2024/03/05/beyond-amending-the-cybercrime-act (accessed on May 7, 2024).

[2] Lucky Obewo-Isawode, 'NSA orders enforcement of cybercrimes law', Available at: https://www.channelstv.com/2024/05/03/nsa-orders-enforcement-of-cybercrimes-law (accessed on May 8, 2024.

[3] 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.

be 0.5% (0.005), equivalent to half a percent of all electronic transactions[4], and this provides the much-needed clarity to the provision.

In furtherance of the above, the CBN issued the circular on the Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy (the "**Circular**"). The Circular mandates the collection and remittance of the cybersecurity levy to the National Cybersecurity Fund (NCF), administered by the Office of the National Security Adviser (ONSA). Banks and financial institutions are instructed to apply the levy at the point of electronic transfer origination and remit it to the NCF, save for transactions listed in Appendix 1 of the Circular[5]. The Circular further provides that system reconfigurations towards ensuring complete and timely submission of remittance files to the Nigeria Interbank Settlement System (NIBSS) Plc shall be completed within 4 (four) weeks of this Circular for commercial, merchant, non-interest, and payment service banks, and mobile money operators and 8 (eight) weeks of this Circular for microfinance banks, primary mortgage banks, and development finance institutions.

The cybersecurity levy is anticipated to have a negative impact on customers of Banks and other financial institutions in Nigeria which may occasion a decline in electronic payment transactions and financial inclusion rate; and hinder the CBN's drive for a cashless economy as more people may opt for cash transactions to avoid the extra charges.

Additionally, Section 44(6)(a) of the Principal Act (as amended by the Amendment Act) empowers the ONSA to establish a compliance monitoring system[6] to monitor the deduction and remittance of the cybersecurity levy.

The cybersecurity levy is also applicable in the telecommunication sector, insurance sector, and Nigeria Stock Exchange. However, at the time of writing this newsletter, the regulators in these sectors are yet to enact the necessary framework for the implementation of the cybersecurity levy.

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

The Amendment Act establishes Sectoral CERTs and SOCs, which will collaborate with the National Computer Emergency Response Teams **(**CERT) as outlined in the Principal Act[7]. These Sectoral CERTs and SOCs are tasked with receiving information from individuals or institutions operating computer systems or networks, both public and private, in the event of cyberattacks or disruptions[8]. Their primary responsibility is to promptly respond to such incidents. Additionally, they will oversee the integration and routing of internet and data traffic from all public and private organizations to ensure the protection of the national cyberspace[9].

---

[4] Section 11 of the Cybercrime (Prevention, Prohibition, Etc,) (Amendment) Act 2024 (the "**Amendment Act**')
[5] 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.
[6] *Supra* note 4.
[7] Section 10 of the Amendment Act
[8] Section 3(a) of the Amendment Act
[9] *Supra note 8*

3. Reporting of Cyber Threats

Under the Amendment Act, 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[10]. 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[11]. This swift escalation to the National CERT aims to mitigate cyber threats promptly, thus preventing disruptions of the cyberspace.

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

The Amendment Act mandates that customers conducting electronic financial transactions at financial institutions must present their National Identification Number (NIN) issued by the National Identity Management Commission (NIMC) for identity verification[12]. This requirement aims to expedite the tracking of defaulters or perpetrators using NIN, which contains individual data including physical addresses. However, there are concerns that implementation may face challenges, as defaulters could potentially create deceptive locations using authentic NINs.

5. Protection of Specific Traffic Data and Subscriber Information

The Amendment Act revises Section 38(1) of the Principal Act, aligning it with the Nigeria Data Protection Act (NDPA). Now, service providers are not only required to retain specified traffic data and subscriber information but are also mandated to ensure their protection.[13] This amendment reflects the government's commitment to safeguarding data and subscriber information, reinforcing the agenda of data security and privacy.

6. Manipulation of ATM/POS Terminals

The Principal Act restricted payment systems to Automated Teller Machines (ATMs) and Point of Sales (POS) terminals, overlooking various other payment technologies prevalent in Nigeria[14]. The Amendment Act addresses this gap by holding individuals accountable for manipulating not only ATMs and POS terminals but also other payment technology means[15]. This expansion accommodates the diverse range of payment systems in Nigeria, ensuring comprehensive coverage and mitigating fraud risks associated with unconventional payment methods.

Conclusion

The Amendment Act represents a significant step forward in Nigeria's efforts to combat cybercrimes and safeguard its digital landscape. Through key provisions such as the implementation of the cybersecurity levy, establishment of Sectoral CERTs and SOCs, and inclusion of measures for compliance monitoring and reporting of cyber threats, the Amendment Act addresses critical gaps and strengthens the country's cybersecurity

[10] Section 3(b) of the Amendment Act
[11] Section 21(3) of the Cybercrime (Prohibition, Prevention, Etc.) Act 2015 (the "**Principal Act**")
[12] Section 8 of the Amendment Act
[13] Section 9 of the Amendment Act
[14] Section 30 of the Principal Act
[15] Section 7 of the Amendment Act

framework. However, challenges remain, particularly concerning the practical implementation of certain provisions and potential impacts on financial inclusion. Moving forward, effective collaboration between government agencies, private sector stakeholders, and Nigerians will be essential in ensuring the successful implementation of the Amendment Act and safeguarding Nigeria's digital future.

LAGOS
Plot 1B, Block 129
Jide Sawyerr Drive
Lekki Phase I
Lagos State, Nigeria

ABUJA
4th Floor, Abia House
Plot 979, 1st Avenue
Off Ahmadu Bello Way
Central Business District
Abuja FCT, Nigeria

Tel.: 0700 DOALAW (0700 362529)
Email: info@doa-law.com
www.doa-law.com

DUALE, OVIA & ALEX-ADEDIPE