Key contacts

Emmanuel Gbahabo
Partner and Head
Investigations, White Collar, & Compliance and Dispute Resolution
emmanuel.gbahabo@templars-law.com

Lawal Kazeem, ACIArb
Senior Associate
Investigations, White Collar, & Compliance and Dispute Resolution
lawal.kazeem@templars-law.com

Christiana Ufomba
Associate
Investigations, White Collar, & Compliance and Dispute Resolution
christiana.ufomba@templars-law.com

TEMPLARS ThoughtLab

The Cyber Crimes (Prohibition, Prevention, Etc.) (Amendment) Act 2024: A Paradigm Shift for Individuals and Businesses?

Introduction

In an era where digital technologies permeate every aspect of our lives, ensuring the security of cyberspace is paramount. Nigeria, like many nations, has recognized the critical importance of safeguarding its digital infrastructure against cyber threats. A significant step in this direction was the enactment of Cyber Crimes (Prohibition, Prevention, etc.) Act, 2015 (the "**2015 Act**"). Since its enactment, the government has been committed to implementing reforms across various sectors, including the nation's cyberspace. In this regard, the Federal Government of Nigeria also formulated a Cybersecurity Policy in 2021.

The National Cybersecurity Policy and Strategy of 2021

The National Cybersecurity Policy and Strategy of 2021 (the "**Policy**") outlines several key areas that amendments to the Cybercrimes Act[1] should address. These include penalties for breaches or disruptions to Critical National Information Infrastructure (CNII), timelines for cyber incident reporting, regulation of cybersecurity service providers, and the allocation of powers to the National Cybersecurity Coordination Centre (NCCC) to coordinate national cybersecurity and investigate cyber breaches. Additionally, the policy calls for enhanced enforcement of cybersecurity legislation, lawful interception, and child and gender online protection, as well as a review of penalties.

The 2015 Act which was enacted before the Policy addresses most of these concerns by providing penalties for breaches or disruptions to CNII and establishing timelines for cyber incident reporting. It also includes provisions for identity theft. The Cyber Crime (Prohibition, Prevention, etc.) (Amendment) Act, 2024 (the "**Amended Act**"), in addition, reviewed the penalties for certain offences. However, the Amended Act does not allocate powers to the NCCC for coordinating national cybersecurity and investigating cyber breaches.

[1] Given that the Policy was formulated in 2021, it is understood that the amendment contemplated here is any amendment to the 2015 Act.

Instead, the Act designates the National Computer Emergency Response Team (CERT) Coordination Centre to handle attacks, intrusions, and disruptions to computer systems or networks. The Amended Act and the 2015 Act also lack specific provisions for child and gender online protection, although the 2015 Act criminalizes child pornography and related offences, which aids in child protection.

In light of the ongoing reforms of the Federal Government, in the second quarter of 2024, the President of Nigeria signed theAmended Act into law. The Amended Act complements and addresses some of the issues that were inadvertently omitted or not treated in the 2015 Act. Overall, while the 2015 Act and the Amended Act are largely aligned with the National Cybercrime Policy, further adjustments are needed to achieve full alignment.

In this publication, we explore the key provisions of the Amended Act and their implications for individuals and businesses.

Highlight of Key Amendments

1. Extended Scope on the use of Electronic Signature

The 2015 Act excluded some contractual transactions and documents from the categories of documents that can be validated by electronic signature. This includes death certificate, birth certificate, wills etc. The Amended Act retains this provision generally but allows for the use of electronic signatures in respect of such transactions and documents when they are legally verified in certified true copies.[2] This means that these transactions and documents can be validly completed with electronic signatures if the documents or documentation used for the transaction are in fact legally verified in certified true copies by the issuing entity. There is thus an added layer of responsibility on concerned parties to ensure that the documents are first verified before such parties can resort to the use of electronic signatures. However, the practical implementation of this provision is unclear. We say so because, it is unclear how a party who intends to execute a document electronically should first certify the document that is yet to emanate from him. For example, the chairman of the National Population Commission cannot certify a birth certificate that has not yet been issued. It seems the intention of the Amended Act may be to allow for certification after the document has been executed. We recommend that the provision be reworded to either permit the use of electronic signatures without additional requirements or specify that the certification of electronic signatures can occur after the document's execution in certain circumstances.

2. Additional Provision on reporting of cyber threats:

The reporting of cyber security threats under the 2015 Act was required to be made directly to the National Computer Emergency Response Team (CERT) Coordination Center. The Amended Act, however, changed the reporting channel as it now requires the reporting of cyber threats to be done through sectoral CERT or sectoral Security Operations Centres (SOC).[3] The rechannelling of the reporting route is a welcome development as it will improve coordination and streamline the response process,

[2] Section 2 of the Amended Act.
[3] Section 3 of the Amended Act.

allowing for quicker and more efficient handling of cyber threats at both the sectoral and national levels.

To minimize the risk of escalation and the wider impact of cyber incidents the Amended Act also shortened the timeline for reporting from 7 (seven) days to 72 hours[4]. Therefore, concerned persons or institutions must report cyber threats to the sectoral SOC within 72 hours of their occurrence. Compliance with this requirement will, in our view, assist CERT in proactively dealing with cyber threats.

3. Expanded scope for identity theft and impersonation:

Under the 2015 Act, any employee of a financial institution who uses his/her special knowledge to commit identity theft against his/her employer, staff, service providers, or consultants with the intent to defraud is guilty of an offense. Identity theft and impersonation contemplates unlawfully obtaining and using another person's personal or financial information with the intent to deceive or defraud or assume another person's identity, typically to access resources, obtain credit, or conduct unauthorized transactions in the victim's name.

Under the 2015 Act, staff members of companies other, than financial institutions, could not be tried for identity theft and impersonation. This created an obvious loophole that could be exploited by unscrupulous employees of companies other than financial institutions, to defraud or generally harm unsuspecting members of the public. To correct this anomaly, the Amended Act extended the scope of service providers whose staff member could be tried for identity theft and impersonation to cover persons engaged in the services of public or private organizations.

4. Re-scoping the parameters for the offence of cyberstalking:

Section 24 of the 2015 Act makes it an offence for any person to transmit a message via computer systems or networks that is grossly offensive, pornographic, indecent, obscene, or menacing, or knowingly send false information for the purpose of causing annoyance, inconvenience, danger, obstruction, insult criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent.

This Section 24 of the 2015 Act has been a lightning rod for controversy since its inception. It has been criticized for its alleged role in curtailing and potentially undermining constitutionally guaranteed rights to freedom of the press and expression. This provision has been cited and used to justify alleged unlawful arrest of journalists and others based on their online activities.

The reason for this is the fact that the section was termed vague and overbroad. Terms like "insult," "hatred," "inconvenience," "ill will," and "needless anxiety" were not clearly defined. What constitutes an insult, hatred, annoyance, or inconvenience under the section? Is there a limit to what may be classified under these terms? These ambiguities left the section open to interpretation, allowing law enforcement agencies to target individuals arbitrarily. When a statute is vague, it gives undue power to prosecutors, leading to arbitrary enforcement, as highlighted by the US Supreme Court in ***Thornhill v.***

[4] Section 3 of the Amended Act.

Alabama.[5] The section was also criticized for its irreconcilability with sections 36(12) and 39(1) of the 1999 Constitution of the Federal Republic of Nigeria, 1999 (as amended).

In a notable legal challenge, the Court of Appeal in Lagos recently dismissed claims questioning the constitutionality of Section 24(1) of the 2015 Act, asserting that the allegations lacked merit.[6] The court upheld the Federal High Court's decision, dismissing a challenge to the constitutionality of section 24 of the 2015 Act on the ground that the offence created by the section was overbroad and vague and threatened the constitutional right to freedom of expression. The Court reasoned that the provision was not vague, that "cybercrime is incapable of direct definition" and that the restriction on freedom of speech was necessary in a democratic society in the interests of defense, public safety, public order, public morality or public health pursuant to section 45 of the 1999 Constitution of the Federal Republic of Nigeria (as amended).

In March 2024, reports emerged that the Economic Community of West African States (ECOWAS) Court of Justice ruled that Section 24 of the 2015 Act does not comply with Articles 9 of the African Charter on Human and People's Rights and the International Covenant on Civil and Political Rights. As a result, the ECOWAS Court of Justice ordered the Nigerian Government to amend section 24 of the 2015 Act.[7]

In reaction to the various criticisms, the Amended Act refined the language of Section 24 of the 2015 Act by limiting its parameters to *pornographic or false information* aimed at causing a breakdown of law and order or posing a threat to life.[8] In effect, if a message is shown to be true and not pornographic, then no offence would have been committed under Section 24 of the 2015 Act as amended. This amendment is commendable; it represents a significant stride by the Nigerian Government in safeguarding the constitutionally guaranteed freedom of expression.

Despite the changes introduced by the Amended Act and the ECOWAS Court of Justice's decision in March 2024, it has been reported that journalists are still being arrested, with law enforcement officers citing Section 24 of the 2015 Act as their authority.[9] This is likely because the Amended Act fails to clearly define what constitutes a breakdown of law and order. This ambiguity allows law enforcement officers to use the law as a pretext to target journalists, claiming their actions amount to a breakdown of law and order.

5. Liberalisation of the scope of the offence of conspiracy, aiding and abetting:

Under the 2015 Act, only employees of a financial institution were liable for conspiring, aiding and abetting the perpetration of fraud using computer systems[10]. However, the Amended Act broadens this scope to cover employees of both private and public organisations.[11] This move appears to have arisen from the recognition that cybercrime is not limited to the financial sector and that employees across various sectors can exploit

[5] 310 US 88 (1940).
[6] Solomon Okedara v Attorney General of the Federation (CA/L/174/18)
[7] https://www.premiumtimesng.com/news/top-news/520361-rights-violations-ecowas-court-orders-nigerian-government-to-amend-cybercrime-law.html?tztc=1
[8] Section 5 of the Amended Act.
[9] https://dailytrust.com/cybercrimes-act-despite-amendment-clampdown-on-journalists-persists/#:~:text=A%20review%20of%20the%20Cybercrimes,or%20network%20that%20is%20grossly
[10] Section 27 of the 2015 Act.
[11] Section 6 of the Amended Act.

computer systems and networks for fraudulent activities. The broader scope will indeed address the evolving landscape of cybercrime, ensuring comprehensive legal coverage and deterrence across all sectors.

6. Expanded the offence of manipulation of ATM/POS Terminals to include other payment technology

Manipulation with the intention to defraud which contemplates intentionally altering or interfering with payment systems to commit fraud was defined as an offence under the 2015 Act. While it was restricted to just Automated Teller Machines ("**ATM**") or Point of Sales ("**POS**") terminals under the 2015 Act, the Amended Act broadens its scope beyond just ATMs and POS terminals to include all forms of payment technology. The limited coverage of the 2015 Act meant that fraudsters could exploit other payment technologies, such as mobile money payment applications, online banking platforms, contactless payment systems, and e-commerce gateways without facing legal consequences. This limitation necessitated an amendment to broaden the scope so as to ensure that all forms of payment technology are covered to provide comprehensive protection against fraudulent manipulation.[12]

Individuals and financial institutions manipulating any payment technology can now face severe penalties, including imprisonment and fines. Financial institution employees colluding in such fraud can face even stricter consequences. This change emphasizes the need for vigilance by individuals and financial institutions in all payment technology transactions to avoid legal repercussions.

7. Additional means for verifying customers of Financial Institutions:

The Amended Act mandates that financial institutions must verify the identity of their customers conducting electronic financial transactions[13] and such customers must present their National Identification Number ("**NIN**") issued by the National Identity Management Commission, along with other valid documents bearing their names, before being issued ATM cards, credit cards, debit cards, or similar electronic devices. Previously, verification was limited to documents with the customer's name, address, and other relevant information.

The NIN provides a high level of credibility and verification as it helps institutions to access verified and reliable information about their customers. The NIN aids in cutting down the time needed for verifying customers and helps financial institutions to better prevent identity fraud and ensure that only authorized individuals get access to financial services.

8. Recognition of the new data protection regime

The pervasive use of information and communication technology has made the use of personal data and their protection a big issue globally. While the 2015 Act merely required data retention and protection as prescribed by the relevant authority, the Amended Act explicitly requires that such retention and protection be done in compliance with the Nigerian Data Protection Act (the "**NDPA**")[14], reinforcing its alignment with the new data protection regime heralded by the enactment of the NDPA. Specifically, the Amended Act requires service providers to keep and protect specific traffic data and subscriber

[12] Section 7 of the Amended Act.
[13] Section 8 of the Amended Act.
[14] Section 9 of the Amended Act.

information in accordance with the provision of the NDPA and as may be prescribed by the Nigerian Communications Commission (NCC), for a period of 2(two) years.

9. Introduction of 2% of annual turn over penalty for failure to pay cyber security levy

The controversial cyber security levy (the "**Levy**"), of 0.5% of all electronic transactions value, was recently widely criticised for imposing additional financial burden of certain businesses in view of Nigerian ailing economic conditions. Unfortunately, the Amended Act has made the implementation of this levy even more stricter by introducing a penalty of not less than 2% of the annual turnover for defaulting business and closure or withdrawal of the business's operational license[15].

It is worth noting that the amendment sparked significant controversy across the country. The crux of the outburst was even so more around the fact that the Central Bank of Nigeria (the "**CBN**") on 6 May 2024 issued a circular regarding the implementation guidance on the collection and remittance of the National Cyber Security Levy (the "**Circular**")[16]. The Circular provided a clear routine for implementing the Levy with a specification that the Levy must be applied at the point of electronic transfer origination, with deduction and remittance carried out by the financial institution. The deduction of the Levy was expected to take effect within 2 (two) weeks from the date of the Circular (i.e 20 May 2024). In a bid to avoid multiple applications of the Levy on the same transaction, the Circular provided for a list of transactions exempted from the Levy.

Barely 24 hours after the publication of the Circular, the Socio-economic Rights and Accountability Project ("**SERAP**") demanded its withdrawal within 48 hours.[17] SERAP also threatened legal action if the Levy was not rescinded and ultimately followed through with its threat.[18] The House of Representatives also directed the CBN to withdraw the Circular.[19] In light of this and numerous outcries, the CBN through a circular dated 17 May 2024[20] withdrew the circular on the implementation of the Levy.

The numerous outcries on the implementation of this levy when placed side-by-side with the now introduced stiff penalty for non-compliance, raises a pertinent question: "Will the levy ever be implemented?" It is perplexing that the provision was included in the Amended Act with stiffer penalty with no respite provided on enforcement. Unless Nigeria's economic condition takes a new turn, interesting days lies ahead concerning the enforcement of the Levy and its strict penalty.

In relation to the Cyber Security Fund, the Amended Act requires the office of the National Security Adviser ("**NSA**") to administer, keep proper records of the accounts and ensure compliance monitoring mechanism. The accounts are also to be audited in accordance with guidelines provided by the Auditor General of the Federation. We believe that the said guidelines will be an internal point between the NSA and the office of the Auditor General.

[15] Section 11 of the Amended Act.
[16] Ref:PSMD/DIR/PUB/LAB/017/004
[17] https://serap-nigeria.org/2024/05/07/serap-gives-tinubu-48-hours-to-withdraw-unlawful-cbn-directive-imposing-cybersecurity-levy-on-nigerians/
[18] https://www.channelstv.com/2024/05/12/serap-budgit-136-nigerians-sue-cbn-over-cybersecurity-levy/
[19] https://punchng.com/breaking-reps-direct-cbn-to-suspend-cybersecurity levy/#:~:text=The%20House%20of%20Representatives%20Thursday,the%20country%2C%20The%20Nation%20reports.
[20] Ref: PSM/DIR/PUB/LAB/017/005

10. Elimination of seizure of passports:

The Amended Act in Section 12 makes provision for deletion of Section 48 (4) of the 2015 Act which requires (i) the cancellation of the international passport of a Nigerian convicted under the Act and (ii) the withholding of passports belonging to foreigners, which will be returned only after completion of their sentence or payment of fines. This deletion is a welcome development. In our view, there is no reasonable justification and correlation between the commission of an offence under the 2015 Act, for which the offender will serve a jail term or pay fine, with the additional punishment of cancellation or withholding of passport.

Cybercrimes Act and the Budapest Convention on Cybercrime, 2001

The 2015 Act and the Amended Act (the "**Act"**) demonstrates Nigeria's compliance with its obligations as a signatory to the Budapest Convention on Cybercrime, 2001 (the "**Convention**"). Enacted after the Convention, the Act to a great extent incorporates modern-day realities and addresses various cybercrime issues. The Act aligns with the Convention by addressing illegal access to computer systems, illegal interception, data and system interference, misuse of devices, computer-related forgery, offences related to child pornography, attempts and aiding or abetting, corporate liability for cybercrimes, sanctions and measures, and the expedited preservation of stored computer data, among other procedural considerations.

While the Act does not cover copyright and related rights, this obligation is fulfilled by the Copyright Act of 2022. The Convention requires state parties to establish criminal offences for copyright infringement under their domestic laws, and Nigeria's compliance is ensured through the Copyright Act of 2022.

Implications for individuals and business

With the Amended Act introducing additional measures to safeguard our cyberspace, individuals and businesses now face heightened responsibilities. They must exercise extra caution to avoid falling foul of its provisions. Businesses, in particular, must implement stringent measures to prevent their employees from engaging in cyber crimes, which includes revising their data protection and ABC policies.

The Amended Act's imposition of severe penalties for non-compliance underscores its gravity and the critical importance of adhering to cybersecurity standards in Nigeria. It is imperative that individuals and businesses alike take proactive steps to steer clear of risky transactions that could lead to legal repercussions.

Finally, individuals and businesses must, in view of the amendments highlighted above, take steps to update their data protection and cybersecurity policies to comply with the provisions of the Amended Act. The strategies that business may implement include, among others, (i) conducting regular cybersecurity audits and trainings, (ii) implementing strict access control measures to ensure that employees only have access to the data and systems necessary for their job functions, and (iii) conducting regular audits of all network systems and monitoring of network traffic to detect any unusual or suspicious activities, (iv) performing thorough background checks on all employees, especially those who will have access to sensitive information or critical systems, (v) deploying advanced security software, such as firewalls, intrusion detection systems (IDS), and anti-malware tools, to protect against cyber threats.

The enactment of the Amended Act represents a significant advancement in fortifying Nigeria's cybersecurity and digital economy. It however carries important implications for both individuals and businesses which need to be navigated carefully.