THOUGHT LEADERSHIP

A REVIEW OF THE CYBERCRIME AMENDMENT ACT AND THE CBN CYBERSECURITY CIRCULAR

Jackson, Etti & Edu

WWW.JEE.AFRICA

The Nigerian President recently assented to the amendment of the Cybercrime Act titled Cybercrimes (Prohibition, Prevention, ETC) (AMENDMENT) Act 2024. In addition to that, the Central Bank of Nigeria, on the 6th of May 2024, released a circular on Cybersecurity titled Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy, which was made in furtherance to the amended Cybercrimes Act. This has made it necessary to undertake a careful perusal of the amended sections of the Act.

According to the object of the Act, the amendment aims to alter the provisions of the Cybercrimes (Prohibition, Prevention, etc.) Act, No. 17, 2015 to insert some consequential words that were inadvertently omitted in the Act. To this end, our review will assess the amended sections and their impact on Nigerians' cyberspace activities.

Our review will also consider the CBN circular on Cybersecurity in line with the amendment of the Cybercrimes Act identifying the reasons relied on by CBN to issue the directive. We shall also identify the propriety of the act of CBN in furtherance of the provision of the Act.

The following are the amendments to the sections of the Act:

1. **Enhancing Clarity and Legal Validity of Electronic Signatures:** Section 17 of the Cybercrime Act 2015 of Nigeria has been amended as follows:

- In subsection (1 b), the word "geniuses" is corrected to "genuineness", ensuring accuracy in the term and providing meaning to the sentence. It was obvious that the entire sentence was contextually meaningless with the word geniuses.
- In subsection (2), the amendment introduces the inclusion of the phrase "Certified True Copies" after the word "signature". This inclusion clarifies that electronic signatures may be legally verified in Certified True Copies, providing a framework for authentication in electronic transactions.

We believe this will enhance the clarity and legal validity of electronic signatures, ensuring their enforceability in transactions while also providing the guidelines for their legal verification when necessary, thereby contributing to the efficiency and reliability of electronic transactions under the Cybercrime Act. This is in line with the recent amendment of Section 84 of the Evidence Act, which now recognizes electronic records, information, and digital signatures. The Cybercrime Act further strengthens the legal weight of digital signatures, ensuring their reliability in contracts. Together, these laws create a robust legal framework for electronic transactions, promoting secure information exchange and evidence handling. This aligns Nigeria's legal system with global advancements and international standards. We believe this harmonization will support economic growth by facilitating e-commerce, digital communication, and online transactions.

2. **Cyber Incident Response and Reporting:** Section 21 of the Cybercrime Act 2015 of Nigeria has been amended as follows:

(a) **Insertion of "Coordination Center" and "sectoral CERTs or sectoral Security Operations Centres (SOC)"**:

- In subsection (1), the amendment introduces the requirement for service providers to coordinate with their respective sectoral Computer Emergency Response Teams (CERTs) or sectoral Security Operations Centres (SOC) through a Coordination Center, enhancing collaboration in handling cyber incidents.

(b) **Change in time frame for Reporting**:

- Subsection (3) has been amended to alter the timeframe for reporting incidents. Instead of "7 days of its occurrence," it is now "72 hours of its detection." This change emphasizes the importance of prompt reporting and response to cyber incidents for effective mitigation and prevention of cyber threats.

These amendments aim to strengthen cybersecurity measures by facilitating better coordination among service providers and law enforcement agencies, as well as ensuring timely reporting and response to cyber incidents in Nigeria. This is also in line with the data breach reporting requirements of the Nigerian Data Protection Act, which compel reports of data breaches within 72 hours of becoming aware of the data breach.[1] Although the NDPA already covered the ambit of data breaches, cyber incidents are wider than data breaches and may or may not include data breaches. For example, a cyber incident may cause network outages or disruptions, and during that network disruption, data may not be breached or stolen. Hence, where there is a cyber incident, the report should be made in accordance with the Cybercrime Act and the NDPC should be informed where there is a data breach during the cyber incident.

3. **Expansion of the Scope of Identity Theft Offences**: Section 22 of the Cybercrime Act 2015 of Nigeria has been amended as follows:

    (a) Insertion of "public or private organisation":

    - Section 22 (1) of the principal Act is amended by adding "public or private organisation" after the term "any financial institution". This expands the scope of the offence of identity theft to include individuals engaged in the services of both financial institutions and public or private organizations.

This amendment broadens the legal framework to address identity theft comprehensively, encompassing not only financial institutions but also public or private organizations, thereby enhancing protection against fraudulent activities across various sectors.

4. **Broadening Prohibited Content and Intent in Online Communication**: Section 24 (1) of the Principal Act has been amended by substituting new paragraphs "(a)" and "(b)". The amendment expands the prohibited content of messages sent via computer systems or networks. Paragraph (a) now includes the prohibition of messages that are pornographic. Paragraph (b) has been revised to include the dissemination of false information with the intent of causing a breakdown of law and order, posing a threat to life, or facilitating the transmission of such messages.

    These changes broaden the scope of prohibited content and intent under section 24 of the Cybercrime Act. By explicitly banning the transmission of pornographic material and false information intended to disrupt societal order or endanger lives, the amendments aim to enhance the regulation of online communication. This

[1] Section 40(2) of the Nigerian Data Protection Act 2022.

reinforces efforts to combat cyber threats and promote a safer digital environment for users in Nigeria.

5. **Extension of Employee Collusion Offences to Public and Private Organizations):** Section 27(2) of The Cybercrime Act 2015 has been amended by substituting the phrase "a financial institution" with "any public or private organisation". This amendment expands the scope of the offence related to employee collusion in perpetrating fraud using computer systems or networks beyond financial institutions to encompass any public or private organization. This will ensure that any public or private organisation, regardless of its mission or purpose, is held accountable for employee collusion and fraud, protecting resources, data, and stakeholders from internal threats.

6. **Updated Offences related to Fraudulent Payment Technologies:** Section 30 of the Cybercrime Act 2015 of Nigeria has been amended as follows:
    a) In subsection (1), after the word "terminals", the phrase "or any other payment technology means" is added.
    b) In subsection (2), the phrase "or point of sale device" is replaced with "or any other payment technology means".

    These amendments to section 30 broaden the scope of the offences related to fraud involving ATMs or Point of Sales (POS) terminals under the Cybercrime Act. The inclusion of "any other payment technology means" in subsection (1) expands the definition of devices covered, reflecting the evolving nature of payment technologies. Similarly, replacing "point of sale device" with "any other payment technology means" in subsection (2) extends the applicability of the law beyond traditional POS devices. These changes align the legislation with contemporary payment methods, ensuring comprehensive legal coverage against fraudulent activities in electronic payment systems within Nigeria.

    This development is particularly significant for the Fintech industry, which has grown rapidly in Nigeria in recent years. The amendment provides a much-needed boost to the sector, enabling Fintech companies to operate with confidence and security, knowing that their innovative payment solutions are protected by law.
    This expansion will also cover AI-powered payment systems thereby enhancing the overall security of both existing and emerging digital payments. By incorporating other payment technology means into the law, Nigeria is demonstrating its commitment to creating a secure, trustworthy, and innovative digital payment ecosystem.

7. **Data Retention and Protection Requirements for Service Providers:** The amendment of Section 38 involves substituting subsection (1) with a new provision. The revised subsection (1) now mandates service providers to retain and safeguard specific traffic data and subscriber information in accordance with the Nigeria Data Protection Act and as prescribed by the relevant regulatory authority responsible for overseeing communication services in Nigeria, for a duration of two years.

   This amendment to section 38 introduces a more comprehensive and aligned approach to data retention and protection by incorporating the requirements of the Nigeria Data Protection Act[2]. It establishes a clear timeframe for compliance, enhancing accountability and consistency among service providers. Additionally, by mandating adherence to data protection regulations, the amendment strengthens and safeguards individuals' privacy rights and promotes transparency and security in the management of telecommunications data within Nigeria.

8. **Enhanced Statutory Authority for the Office of the National Security Adviser**

   The amendment to the Act ushered in an expansion of the scope and responsibilities of the office of the National Security Adviser as provided under Section 41 of the Principal Act. New paragraphs (d) – (j) were introduced to replace the hitherto paragraphs (d) – (h), in efforts towards coordinating cybersecurity in Nigeria.

   The following is a breakdown of the specific amendments and their effects on the principal act:

   - **Establishment of Sectoral CERTs and SOCs (Substituted Paragraphs (d) and (e))**: The amendment now mandates the establishment of sectoral Computer Emergency Response Teams (CERT) and sectoral Security Operation Centres (SOC) to feed into the national CERT. This ensures a more distributed and specialized approach to cyber incident response and protection of the national cyberspace.
   - **Establishment of a National Computer Forensic Laboratory (Substituted Paragraph (f))**: The amendment maintains the establishment and maintenance of a National Computer Forensic Laboratory, extending its coordination to all relevant law enforcement, security, and intelligence agencies. This reinforces the importance of digital forensics in investigating cybercrimes.

[2] Section 39 of the Nigeria Data Protection Act 2023

- **Capacity Building (Substituted Paragraph (g))**: The amendment broadens the mandate to build capacity not only for security and intelligence agencies but also for law enforcement and military services. This ensures a comprehensive approach to skill development necessary for combating cybercrimes effectively.
- **Establishment of PPP Platforms (Substituted Paragraph (h))**: The amendment continues the establishment of appropriate platforms for public-private partnerships (PPP), emphasizing the importance of collaboration between government and private entities in cybersecurity efforts.
- **International Cybersecurity Cooperation (New Paragraph (i))**: The amendment introduces a new provision to coordinate Nigeria's involvement in international cybersecurity cooperation. This underscores the significance of aligning Nigeria's cybersecurity efforts with global frameworks and standards.[3]
- **General Provision for Necessary Acts (New Paragraph (j))**: The amendment adds a catch-all provision allowing the National Security Adviser's office to undertake any other acts or things necessary to effectively perform the functions of relevant security and enforcement agencies under the Act. This provides flexibility for adapting to evolving cybersecurity challenges.

The amendments to Section 41(1) of the Principal Act strengthen Nigeria's cybersecurity framework by expanding the scope of responsibilities, enhancing coordination mechanisms, and emphasizing the importance of capacity building and international cooperation in combating cybercrimes.

9. **Removal of Passport Cancellation for Cybercrime Offenses:** Section 48 (4) of the Cybercrime Act which previously mandated the cancellation of an individual's international passport upon conviction of a cybercrime offence has been repealed. Specifically, the subsection provided that a person convicted under the Act would have their international passport cancelled. This amendment is significant as it removes a punitive measure that was deemed excessive and potentially infringing on individuals' rights to freedom of movement. The previous provision also applied to foreigners, who would have their passports withheld until they served their sentence or paid the imposed fines.

   The repeal of this subsection aligns with the principles of proportionality and fairness in sentencing, ensuring that individuals convicted of cybercrimes are not subjected to undue hardship and restrictions on their travel. This amendment promotes a more balanced approach to combating cybercrimes while respecting the rights of individuals.

[3] Note that Nigeria is yet to ratify the African Union Convention on Cyber Security and Personal Data Protection the Malabo Convention. Nigeria is not a member of any international framework for cybersecurity or data protection.

10. **Enhanced Administration and Enforcement of the National Cyber Security Fund**: The amendment to Section 44 of the Principal Act introduces several changes aimed at enhancing the administration and enforcement of the National Cyber Security Fund. Firstly, in subsection (2), the amendment substitutes paragraph (a) to impose a levy of 0.5% (0.005) on the value of all transactions by *businesses specified in the Second Schedule to the Act*. This adjustment increases the financial contribution from businesses towards the Fund. The businesses specified in the Second Schedule of the Act which section 44 (2)(a) refers to are:
    a. GSM Service providers and all telecommunication companies;
    b. Internet Service Providers;
    c. Banks and other Financial Institutions;
    d. Insurance Companies;
    e. Nigerian Stock Exchange.

    Secondly, the amendment introduces new subsections (6) to (8), outlining specific administrative and compliance measures. Subsection (6) designates the Office of the National Security Adviser as responsible for administering the Fund, keeping proper records, and monitoring compliance. Subsection (7) mandates that the Fund's accounts be audited in accordance with CIRCULARs provided by the Auditor General for the Federation. Lastly, subsection (8) establishes penalties for non-compliance, stating that businesses failing to remit the levy commit an offence and are liable to fines of not less than 2% of their annual turnover. Additionally, failure to comply may result in the closure or withdrawal of the business's operational license.

    These amendments aim to strengthen the financial resources and management of the National Cyber Security Fund, ensuring adequate funding for cybersecurity initiatives while imposing stricter measures to enforce compliance and deter non-compliance by businesses.

INTERPRETATION OF 'TRANSACTIONS BY *BUSINESSES*' AND THE EFFECT OF SECTION 44 VIS-A-VIS THE CBN CIRCULAR ON CYBERSECURITY LEVY

In furtherance to the amendment of section 44, the Central Bank of Nigeria on May 6, 2024[4] introduced a certain cybersecurity levy on different levels of transaction. The circular provides that the levy shall be at the point of electronic transfer origination, then deducted and remitted by the financial institution. The deducted amount shall be reflected in the customer's account with the narration: "Cybersecurity Levy". The circular listed out transactions that are exempted from the cybersecurity levy[5]. It also provided that deductions shall commence within 2 weeks from the date of the circular for all financial institutions.

The introduction of a cybersecurity levy on all kinds of electronic transactions by the Central Bank of Nigeria (CBN) has raised concerns and questions regarding the authority of the CBN to impose such a levy within the provisions of the Cybercrime Act. The interpretation of the term '...on the value of all transactions by *businesses*' is the main conundrum through which all arguments, objections, powers and concerns must pass through. How did the CBN interpret the provisions of the amended Act for the levy of customers engaged in electronic transfers?

Firstly, a careful perusal of the Act specifically mentions *businesses specified in the Second Schedule* as subject to the levy, whereas the CBN's decision extends it to all transactions, irrespective of the nature of the entities involved. The Act, in our interpretation, intends to levy businesses and not individuals Although, it can be argued that there is no way the businesses will remit the levies without delineating the charges on certain transactions in their day-to-day businesses with customers. However, such an argument or interpretation is overreaching over the clear provisions of the Act. It is the business that is being levied. Whilst the businesses mentioned may carve out a business model for replenishing the cost, we believe that it will be ultra vires the Act to charge out the levy on the customers as a cybersecurity levy/tax.

Secondly, the Cybercrime Act delineates the powers and procedures related thereto, to the National Cyber Security Fund, including the imposition of levies on specified businesses.

---

[4] Circular to all Commercial, merchant, non-interest, and payment service banks; other financial institutions, mobile money operators and payment service providers. RE: Cybercrimes (Prohibition, Prevention, ETC) (AMENDMENT) Act 2024 - Implementation Guidance on the Collection and Remittance of the National Cybersecurity Levy dated May 6, 2024

[5] Loan disbursements; salary payments; intra-account transfers within the same bank or between different banks for the same customer; Intra-bank transfers between customers of the same bank; Other financial institutions' instructions to their correspondent banks, Interbank placements; Bank transfers to CBN and vice versa; Inter-branch transfers within a bank; Cheques clearing an settlements; Letters of Credits (LCs); Banks' recapitalisation related funding - only bank 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 transactions e.g. Pension Payments; Non-profit and charitable transactions including donations to registered non-profit organisations or charities; Educational Institutions, including tuition payments and other transaction involving schools, universities, or other educational institutions; Transactions involving bank's internal accounts such as suspense accounts, clearing accounts, profit and loss accounts, inter-branch accounts, reserve accounts, nostro and vostro accounts and escrow accounts.

The Act does not explicitly grant the CBN governor the authority to unilaterally extend the levy to cover all transactions. Therefore, the propriety of the Governor's decision hinges on whether it aligns with the powers granted by the Act and the intent of the legislation. One can argue that the CBN as the regulator of one of the businesses mentioned in the second schedule of the Act can proceed to determine for the businesses under its control how the levies are to be charged. But when its interpretation and circular extended to customers at large, it went contrary to the provisions of the enabling law. The proper thing for the CBN to do would have been to create a business guide so financial institutions could recuperate such expenses without directly charging customers for such levies.

Another issue to be considered is that the actions of the CBN bring about multiple taxation of Nigerians. If all the business sectors listed in the second schedule decided to charge their customers for this levy, would that not be too much burden for the citizens? Will that not lead to a case of multiple taxation on the same subject matter plus other recurring taxes? The answer is obvious. In our opinion, the Act specifically mention businesses and we do not think this includes individuals trading with the businesses. The decision of each regulator to delineate the levy on the customers of the business will be too much of a burden to the citizens.

CONCLUSION:

One of the basic functions of law is to maintain order, peace and progress of the people. One of the merits of the sociological and utilitarian school of thought is that the law should not be far from the interests and needs of society. Currently, Nigerians are suffering from harsh economic realities and are suffocated with taxes – direct and indirect.

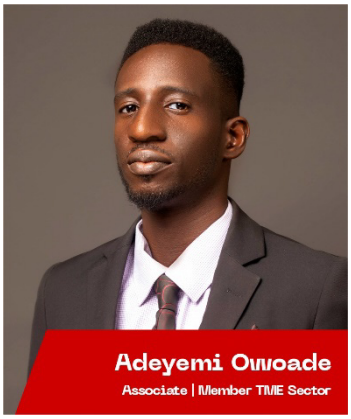
This action of CBN may limit digital inclusion in the country, as individuals will bear the burden of the levy through increased transaction costs, potentially leading to multiple taxation on the same subject matter. The extension of the levy to all transactions, including individual transactions, goes beyond the intent of the Cybercrime Act, which specifically mentions businesses as subject to the levy. This move may discourage electronic transactions, hindering the country's progress towards a digital economy and financial inclusion.

P.S:

While working on this review, the Nigerian President, Asiwaju Bola Ahmed Tinubu, announced that the Cybersecurity levy on electronic transactions has been suspended. Also, on Friday, 17th May 2024, the CBN issued another circular to financial institutions withdrawing the previous circular on the cybersecurity levy. We recommend that all stakeholders mentioned in the

second schedule of the Act should meet and agree on the proactive ways to charge this levy, appropriately interpreting section 44 of the Act and preventing multiple taxations thereby easing the burden on the populace.

Author:



Jackson, Etti & Edu

Key Contacts

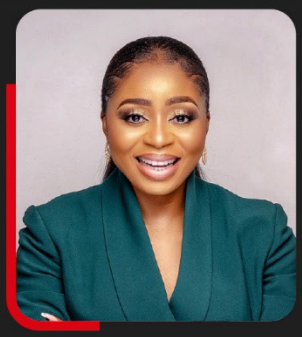
For further information, kindly reach the key contacts below:

NGOZI ADERIBIGBE

Partner, Sector Head - Technology,
Media & Entertainment.

+234 1 4626841/3

E: ngozi.aderibigbe@jee.africa



YEYE NWIDAA

Partner, Sector Head - Technology,
Media & Entertainment.

(234) 1 4626841/3

E: yeye.nwidaa@jee.africa

Victoria Island

RCO Court,
3-5 Sinari Daranijo Street,
Victoria Island,
Lagos, Nigeria

Tel

+234-02-4626841/3,
+234-02-2806989

Email

jee@jee.africa

Abuja

42, Moses Majekodunmi Crescent.
Utako, FCT, Abuja

Ikeja

1st floor, ereke house,
Plot 15, CIPM Avenue
CBD Alausa Ikeja
Lagos Nigeria

Accra

3 Emmause, 2nd Close
Akosombo House
Labone, Accra, Ghana
P.O. Box 14951
Accra, Ghana

Yaoundé

3rd Floor, Viccui Building
Apt. 15-16, Carr Street
New Town, Yaoundé
Cameroon

Harare

38 Clairwood Road,
Alexandra Park,
Harare,
Zimbabwe.