M. J. Numa & Partners LLP
Trial Attorneys & Transaction Advisors

DATA PROTECTION AND THE BANKING SECTOR

www.mjnuma.com

ABSTRACT

Have you ever wondered how internet fraudsters get the bank information of bank customers? This work provides intends to provides an overview of the requirement for data protection in the banking sector, drawing guidelines and frameworks from organizations such as the Nigerian Data Protection Regulation (NDPR), The National Information Technology Development Agency (NITDA), The Cybercrimes (prohibition, prevention, etc.) Act. Data protection is a critical issue in the banking sector, where sensitive customer information is routinely and vastly collected, stored and processed. Banks must take comprehensive approach to safeguarding this data, including implementing technical measures, complying with data protection regulations, training employees, establishing incident response plans, and carefully vetting third-party providers. Failure to protect customer data can result in reputational damage, financial loss, and legal liabilities in the event of data breach or cyber-attack. This work intends to delve into the criticality of data breach in the banking sector of Nigeria and in other country jurisdiction.

INTRODUCTION:

Data protection has become a major concern in today's digital age, particularly in the banking sector where the handling of personal and financial information is paramount. As banks increasingly rely on technology to provide efficient and convenient services, ensuring robust data protection measures is essential to maintain trust, protect customer privacy, and defend against cyber threats. In an increasingly digital age, data has become a valuable asset, and protecting it has become paramount. Nowhere is this more critical than in the banking sector, where sensitive financial information is entrusted to financial institutions by customers.

In the financial sector in Nigeria, the Banking and other Financial Institutions Act 2020 ('BOFIA')[1] regulates banking and other financial institutions and matters connected to them. The Central Bank of Nigeria ('CBN') through the Central bank of Nigeria Act 2020 ('the CBN Act')[2] also regulates the banking sector. The BOFIA and CBN Act do not make specific provisions for data protection in the finance sector, however, certain guidelines issued by the CBN

[1] Cap B3 Laws of The Federation of Nigeria, 2004.
[2] Cap 19 Laws Of The Federation of Nigeria, 2004.

such as the Consumer Protection Framework ('the Framework'), and recently, the draft Consumer Protection Guidelines of Disclosure and Transparency, make some provision for data protection and privacy in the financial sector[3].

The Nigerian Data protection Act.[4]

A new Nigeria Data Protection Act was signed into law on the 12th of June 2023. The legislation is set to not only regulate the processing of personal data but to also introduce new copious innovative provisions that protects data in Nigeria. The Act highlights the need for a data protection impact assessment (DPIA) where the processing of personal data appears likely to result in a high risk to the rights and freedoms of data subjects by virtue of its nature. It goes further to mandate the data controller to consult the Commission prior to the processing if the DPIA indicates that the processing of the data would result in a high risk to the rights and freedoms of data subjects. The Act defines a DPIA and also empowers the Commission to issue guidelines and directives on DPIA, including the categories of processing subject to the requirement for a DPIA. This article will examine the need of data protection in the banking sector in cognizance to the Nigerian Data Protection Act. (NPDA) 2023 and its provision of data protection for the personal data of individuals. Section 1(c)[5] promotes data processing practices that safeguard the security of personal of personal data and privacy of data subjects.

Section 1(e)[6] protects data subject' rights, and provides means of recourse and remedies in the event of the breach of data subject.

The NDPR, although considered as subsidiary legislation, is the extant data protection guide in Nigeria and mainly makes provisions for personal data of individuals as opposed to that of corporate and legal entities, this article would delve into the importance of data protection in the banking sector, exploring the challenges it faces, and highlight the measures taken to ensure the security and privacy of customers' financial data with relative cognizance to the **Nigeria Data Protection Regulation. (NDPR) 2019[7]** and its provision of data protection for the personal data of individual.

---

[3] Davidson Oturu Alex, "Data Protection in the financial sector"<https://www.aelex.com/wp-content/uploads/2019/12/Nigeria-Data-Protection-in-the-Financial-Sector-_-DataGuidance.pdf>accessed 15th July 2023.
Beverly Agbakoba-Onyejianya and Esther Odunze"Unveiling The Nigeria Data Protection Act" <https://www.mondaq.com/nigeria/data-protection/1332160/unveiling-the-nigeria-data-protection-act-2023-an-expert-appraisal-of-key-provisions> accessed 15th July 2023.

[4] Nigerian Data Protection Act, 2023.

[5] Id.

[6] Id.

[7] Nigeria Protection Regulation, (NPDR), 2019.

The National Information Technology Development Agency (NITDA)[8], hereinafter referred to as The Agency) is statutorily mandated by the NITDA Act of 2007 to, inter alia; develop regulations for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour and other fields, where the use of electronic communication may improve the exchange of data and information; "The agency" hereby issues the **Nigeria Data Protection Regulation** and shall come into effect on the date issued by NITDA. The NDPR was issued under section 6 (a) and (c) of the National Information Technology Development Agency Act 2007 (the 'NITDA 'Act')[9] and is administered by the NITDA, which plays the role of the Data Protection Authority (DPA) in Nigeria.

As provided in **Part one, Section 1.2 of the Nigeria Data Protection Regulation**[10]**:Scope of the Regulation;**

This Regulation applies to all transactions intended for the processing of Personal Data, to the processing of Personal Data notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria.

Natural persons involve natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria; There have been issues where the data privacy of individuals or customers were violated.In the case of ***Godfrey Nya v MTN Nigeria communication ltd.***[11] the court gave an order of injunction restraining MTN from further giving unauthorised access of Mr Eneye's phone number to these unknown third parties, as well as an award of Five Million Naira (N5,000,000.00) against MTN as exemplary/aggravated damages. The court however dismissed Mr Eneye's claims of violation of his freedom of association and right to liberty.

Dissatisfied with this decision, MTN appealed to the Court of Appeal. The Court dismissed the main part of the appeal, holding that the disclosure of Mr Eneye's mobile phone number without his consent and the resultant unsolicited messages were in violation of his constitutional right to privacy. MTN seems to have further appealed to the Supreme Court, whose judgement will be awaited as another landmark decision on Nigeria's data privacy jurisprudence. This case is is also similar to the case of ***Ezugwu Emmanuel***

[8] National Information Technology Agency Act 2007, Laws Of The Federation.
[9] Id.
[10] Supra n.7
[11] CA/A/689/2013

***Anene v Airtel Nigeria Itd*[12], Mr Ezugwu Emmanuel Anene sued Airtel, his service provider, at the FCT High Court in 2015, alleging that countless unsolicited calls and text messages by Airtel and third parties it granted access to his number breached his constitutional right to privacy, among other claims.[5] As Airtel did not defend the suit, the trial court relied on the evidence produced by Mr Anene and delivered judgement in his favour, awarding Five Million Naira (5,000,000.00) damages to him for violation of his privacy right.**

In an attempt to highlight the significance of data protection in the banking sector, The definition of personal data would be provided pursuant to the provision of **Part one Section 1.3(xix) of the Nigeria Data Protection Regulation[13]:Definitions;**

Definition of Personal Data: "Personal Data" means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others;

The Significance of Data Protection in Banking:

Data protection is of utmost importance in the banking sector due to the nature of the information handled. Banks store and process vast amounts of personal and financial data, including account details, transaction records, credit history, and more. Such information, if compromised, could lead to severe consequences, including financial loss, identity theft, and reputation damage for both customers and banks.

Part one Section 1.1 of the Nigeria Data Protection Regulation[14]:Objectives of the regulation; establishes various objectives of the regulation which identifies the significance of Data protection in the Banking sector, which include the following;

a) to safeguard the rights of natural persons to data privacy;

---

[12] FCT/HC/CV/545/2015.

[13] Supra n.7.

[14] Supra n.7.

b) to foster safe conduct for transactions involving the exchange of Personal Data;
c) to prevent manipulation of Personal Data; and
d) to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

DUTIES OF THE BANK TO ENSURE DATA PROTECTION

1. Protecting Customer Privacy:

Banks hold vast amounts of personal and financial data, making them attractive targets for cyber criminals. Safeguarding customer privacy is a top priority, and banks employ strong security measures such as encryption, access controls, and secure data storage to prevent unauthorized access or data breaches. Regular audits and risk assessments are conducted to identify vulnerabilities and ensure compliance with privacy regulations.

2. Strengthening Cyber security in exchange of Personal Data:

With the rise of sophisticated cyber threats, banks invest heavily in cybersecurity to protect against data breaches, fraud, and identity theft. Multi-factor authentication, firewalls, intrusion detection systems, and continuous monitoring are essential tools used to detect and mitigate cyber threats. Regular security training for employees helps create a culture of awareness and vigilance.

3. Compliance with Regulatory Standards:

The banking sector operates under stringent regulations to protect customer data. Compliance with standards like the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) is crucial. These regulations outline guidelines for data collection, storage, and sharing, ensuring data protection, transparency, and accountability.

4. Data Encryption and Anonymization to ensure the competitiveness of Nigeria Business in International Trade:

Sensitive customer data, such as account details and transaction history, is often encrypted to prevent unauthorized access. Encryption transforms data into a coded format that can only be deciphered with the appropriate decryption key. Additionally, banks employ techniques like data anonymization to remove personally identifiable information when possible, further reducing the risk of data breaches.

Cyber Security and data breaches.

Banks face numerous challenges and threats when it comes to data protection. Cybercriminals continually evolve their methods, using sophisticated techniques to breach security systems and gain unauthorized access to sensitive data. Phishing attacks, malware, ransomware, and social engineering tactics pose significant risks to cyber security. Additionally, internal threats such as employee negligence or deliberate actions can also compromise data security and result to breach. Despite robust preventive measures, data breaches can still occur. Banks have well-defined incident response plans in place to swiftly address and mitigate the impact of any security incidents. The Cybercrimes (prohibition, prevention, etc.) Bill 2015[15], Nigeria's foremost law on cybercrimes criminalizes data privacy and punishes cybercrimes in Nigeria It prescribes that anyone, service, or institution shall take appropriate measures to safeguard such data.[16]

References shall be made to the Data Protection Laws in the United States America and United Kingdom. In the latter, the act which is responsible for data protection of individuals is the **Data Protection Act (DPA) 2018**[17]. The DPA controls how personal data and information is being used an kept by organizations, businesses, banks or the government.

Every organization responsible for using personal data has to follow the strict rules called the " data protection principles". Under the Data Protection Act 2018, individuals have certain rights and principles which are;

First principle: Fair and lawful processing: Personal data must be processed fairly and lawfully. This essentially means that the data must (a) have a legitimate ground for processing the personal data. (b) not using the data in ways that have an unjustified adverse effect on the individuals concerned (c) be transparent about how the data controller or organization intended to use the personal data, (d) make sure nothing which is against the law is unlawful.

Second principle: Personal data can only be obtained for one or more specified and lawful purposes, and must not be processed in a way that is incompatible with those purposes.

Third principle: Personal data must be kept accurate and kept up to date: A data controller must ensure that it holds sufficient personal data to fulfill its intended lawful purposes, but that personal data must be relevant and not excessive to those
purposes.

---

[15] Cybercrimes (Prohibition, Prevention, etc.) Bill,2015.

[16] <https;//www.mondaq.com/nigeria/privacy-protection/895320/data-privacy-and-protection-under-the-nigerian-law> accessed 19th July 2023.

[17] < https://www.legislation.gov.uk/ukpga/2018/12/contents> accessed 15th July 2023>.

Fourth principle: personal data must be accurate and kept up to date
Data controllers must ensure that personal data is accurate and, where necessary, kept up to date.
Fifth principle: Personal data processed for particular purposes should not be kept for longer than is necessary for those purposes. In practice, this means that the data controller must review the length of time it keeps personal data and consider the purpose or purposes it holds the information for in deciding whether and for how long to retain this information. This holds the say that personal data should data be deleted after use.
Sixth principle: Personal data should be processed in accordance with the rights of data subjects under the DPA. In particular, the data controller must: (a) provide information in response to a data subject's access request, (b) comply with a justified request to prevent processing which is causing or will be likely to cause unwarranted damage or distress to the person.

In The United States of America, The Privacy Act of 1974[18] is a federal law that regulates the collection, use, and personal disclosure of personal information by the federal government of the United State. This act establishes certain right for individuals with respect to their personal information. The act also gives limit on disclosure of personal information by federal agencies the act also requires federal agencies and organizations to obtain written consent before disclosing personal information to third parties, subject to certain exceptions. The privacy Act of the 1974 has been amended several times since enactment to reflect changes in technology and to address emerging privacy concerns. The exceptions to the privacy Act of 1974 include situations where the disclosure of personal information is required by law is necessary to protect the health or safety of an individual, or is necessary for the law enforcement purposes.
Federal Trade Commission: The FTC is the most influential government body that enforces privacy data and protection in the United States. It oversees essentially all business conduct in the country affecting interstate and international commerce and individuals. The Federal Trade Commission does not have a specific section that protects privacy data, but it has a broad mandate to protect consumers from unfair and deceptive practices, including those related to the collection, use, and sharing of personal information. The FTC enforces a number of laws and regulations related to privacy, including the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA). The FTC also has issued

[18] <https://www.justice.gov/opcl/privacy-act-1974> accessed on 15th June 2023.

guidelines and best practices for companies to follow when collecting, using, and sharing personal information.

In conclusion, Data Protection is a critical issue in the banking sector. Banks collect and store vast and large amount of personal and financial data from their customers and it is their responsibility to ensure that this data is safe and protected from unauthorized access, use and disclosure. Banks Must comply with the General Data Protection Regulation(GDPR), The Nigerian Data protection Act (NPDA). In my opinion, banks should collaborate with law enforcement agencies to combat cyber threats. By working together, banks can protect the financial data of their customers from cyber threats and data breaches.

M.J Numa & Partners LLP
Trial Attorneys & Transaction Advisors.

Triple A Villa, 495 Adegboyega Atanda Street,
Mabushi, Abuja.

+2347033740393
mj.numa@mjnuma.com
www.mjnuma.com