ADVOCAAT
LAW PRACTICE

DATA PRIVACY CONSIDERATIONS ON OPEN BANKING IN NIGERIA

LAGOS | ABUJA | CALABAR

www.advocaat-law.com | Advocaat Law Practice | advocaatlawpractice

INTRODUCTION

In February 2021, the CBN issued a Regulatory Framework for Open Banking in Nigeria (the Framework), and its Operational Guidelines were issued in 2023.[1] . However, its implementation experienced notable delays due to limited public awareness, inadequate technological infrastructure, and prevailing security concerns.[2] To address these and other concerns, the implementation of the Framework was shifted to August 2025. With the launch in August, Open Banking is expected to redefine financial services in Nigeria by enabling secure, transparent data sharing between financial institutions and licensed third-party providers, paving the way for greater innovation, competition, and financial inclusion[3].

Open banking refers to a system where banks and financial institutions allow Third-Party Providers (TPPs) access to consumer financial data, such as transaction history and account balances, through Application Programming Interfaces (APIs), with the customer's explicit consent.[4] The Framework empowers customers to manage their financial information across various platforms, promoting competition and encouraging innovation. Examples include initiating payments via third-party apps or aggregating account details across multiple banks for better financial management. Open banking also offers financial institutions access to a shared data ecosystem, enabling them to seamlessly import a prospective customer's existing financial data from another bank, thereby simplifying the onboarding process for customers switching providers.[5] However, the success of open banking relies heavily on the responsible handling of customer data. As such, regulatory oversight and privacy safeguards become indispensable.

Open banking offers substantial benefits,[6] including enhanced financial services through personalised tools like budgeting apps and investment trackers. It provides wider access to financial services across multiple institutions, enables faster real-time payments via third parties, and allows users to consolidate various accounts into a single, integrated financial overview for better planning. Additionally, open banking fosters increased innovation and competition, empowering FinTechs to challenge traditional institutions and improve service delivery.

While open banking fosters innovation and improves customer access to tailored financial services, it also raises significant concerns regarding data privacy and security, especially within Nigeria's evolving regulatory environment. Thus, as the financial sector advances, the need to balance financial innovation with robust data protection has never been more important.

---

[1] **Circular on the Regulatory Framework for Open Banking in Nigeria, https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf**

[2] Open Banking in Nigeria, https://openbanking.ng/open-banking-in-nigeria/

[3] **Open Banking in Nigeria: A game-changer for 2025 and beyond, https://www.vanguardngr.com/2025/01/open-banking-in-nigeria-a-game-changer-for-2025-and-beyond/**

[4] **Circular on the Regulatory Framework for Open Banking in Nigeria, https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf**

[5] Why open banking and what is in it for banks in Nigeria, http://openbanking.ng/why-open-banking-and-whats-in-it-for-banks-in-nigeria/

[6] What is open finance and what does it mean for Nigeria? https://openbanking.ng/whats-open-finance-and-what-does-it-mean-for-nigeria/

REGULATORY FRAMEWORK

In March 2023, the CBN released the Operational Guidelines for Open Banking in Nigeria (Guidelines). Notably, this is not the first regulatory intervention where open banking is concerned, as a previous guideline, in the form of a Regulatory Framework for Open Banking in Nigeria (Framework), was released in 2021. While the Framework introduced a preliminary outline for legislative consciousness within Nigeria's financial services sector, the Guidelines offer an operational methodology for the adoption of open banking services. Together, these documents establish a comprehensive framework for data sharing within the banking and payments system to foster innovation and competition.

The Guidelines define the roles and responsibilities of API Providers (APs) and API Consumers (ACs), emphasising customer consent, data privacy, and robust information security. Key areas covered include risk management, incident handling, performance monitoring, and dispute resolution within the evolving open banking ecosystem. Equally relevant is the CBN consideration of the existence of the Nigerian Data Protection Regulation (NDPR), 2019 and the Nigeria Data Protection Act (NDPA) 2023 as chief legislations that deal with the regulation of data protection and data privacy in Nigeria.

Under Guideline 9.2 of the Guidelines, the CBN mandates that API Provider (API) and API Consumer (ACs) must adhere to NDPR or any data protection regulations issued by the CBN for financial institutions, ensuring the protection of customer data. It suffices to say that although the Guidelines prefaced the introduction of the NDPA, the logical inference is that the aforementioned Guideline 9.2 will apply in pari passu with the NDPA and the GAID. [7]

By implication, open banking participants must comply with the standards set by the NDPA and General Application and Implementation Directive (GAID) 2025 in the operation of this regime, including informing individuals about how their personal (especially financial) data will be used, stored, and protected.[8] They must also mandate strong data security measures and procedures for breach notifications.[9] Customers, as data subjects, have clear rights, including the ability to object to data processing and withdraw consent at any time. Consent must be explicit and provable,[10] Open banking participants must comply with these standards to avoid significant penalties.

OPEN BANKING AND ITS DATA PRIVACY CONSIDERATIONS

Open banking thrives on data sharing, and this opens up significant privacy challenges that stakeholders must confront. As personal and financial information flows more freely between banks and third-party providers, the risks

[7] When the NDPA was introduced, it did not expressly repeal the NDPR and both legislations were operational. However, the recent introduction of the GAID has replaced the NDPR. Thus, making only the NDPA and the NDPR applicable to data protection and data privacy in Nigeria.

[8] Section 34 Nigeria Data Protection Act
[9] Section 39 Nigeria Data Protection Act
[10] Section 40 Nigeria Data Protection Act

associated with misuse, unauthorised access, and weak security protocols increase. Some of the key data privacy considerations that must be prioritised to safeguard users' rights and maintain trust in the system include:

1. Cybersecurity Risks

One of the foremost concerns in open banking is the increased surface for cyberattacks. In traditional banking models, data is mainly secured within a single institution's infrastructure. As of 2024, banks in Nigeria recorded about 18,872 cyberattacks monthly.[11] With open banking, however, data is transmitted through APIs to multiple entities, some of which may not have the same level of cybersecurity maturity as banks.

Nigeria has experienced several high-profile cyberattacks in recent years, including ransomware attacks and account breaches.[12] With open banking, unauthorised actors could exploit API vulnerabilities to access transaction data, account balances, and personal identifiers. This increases the risk of data breaches involving mass exposure of financial records, identity theft, where criminals use accessed data to impersonate customers and systemic threats and where coordinated attacks could affect multiple institutions.

The Operational Guidelines for Open Banking in Nigeria mandate vulnerability assessments, penetration testing, and encryption protocols[13]. The Central Bank of Nigeria (CBN) in 2023 issued a Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks (DMBs) and Payment Service Banks (PSBs), to enhance cybersecurity practices within the financial sector and protect customer data.[14] However, enforcement and transparency in reporting breaches remain areas for development.

2. Unauthorised Data Use

Another key privacy issue is the misuse or repurposing of customer data beyond the scope of their consent.[15] While the regulatory frameworks mandate explicit and informed consent, enforcement remains weak, and loopholes can be exploited.

Some third-party providers may use collected data for targeted advertising without proper consent, profile customers using behavioural data to influence credit or loan decisions and resell consumer information to advertisers or data brokers.[16]

This is particularly concerning in Nigeria, where data privacy awareness is still growing, and regulatory authorities may lack resources for full-scale monitoring. For example, a FinTech startup offering financial advice may gradually aggregate user data and analyse it for commercial gain without adequately informing users or seeking renewed consent for secondary use.

The NDPA and GAID[17] addresses this by providing data subjects the right to object to processing, withdraw consent, and seek redress. The NDPA also upholds the principle of data minimisation[18], requiring

[11] Cyberthreats mount as Nigerian Banks record 18,872 attacks monthly, https://businessday.ng/technology/article/cyberthreats-mount-as-nigeria-records-18872-attacks-monthly/
[12] Nigeria's Security Outlook 2025, https://www.deloitte.com/ng/en/services/consulting risk/perspectives/Nigerias-cybersecurity-landscape-in-2025.html
[13] Article 5.3.4 of Operational Guidelines for Open Banking in Nigeria
[14] CBN Risk-based Cybersecurity Framework and Guidelines, https://www.cbn.gov.ng/Out/2024/BSD/CBN%20Risk-Based%20Cybersecurity%20Framework%20for%20DMBs%20and%20PSBs_2024.pdf
[15] Data Protection and Privacy Challenges in Nigeria, https://www.researchgate.net/publication/373343733_data_protection_and_privacy_challenges_in_nigeria_lessons_from_other_jurisdictions
[16]ibid
[17] Article 19 of General Application and Implementation Directive (Gaid)
[18] Article 24 of the Nigeria Data Protection Act, 2023

organisations to collect and process only the personal data strictly necessary for a clearly defined and lawful purpose. It further mandates periodic Data Protection Impact Assessments (DPIAs) to identify potential breach risks and implement appropriate safeguards to mitigate them[19]. Nonetheless, banks and TPPs must proactively embed privacy-by-design in their systems to prevent data misuse.

3. Phishing and Social Engineering

As open banking increases access channels, consumers become more exposed to social engineering threats. Phishing attacks, where fraudsters mimic legitimate financial service providers to gain login credentials or consent tokens, are on the rise globally, and Nigeria is no exception[20].

Imagine a customer receiving an email or SMS that appears to be from their bank or a legitimate FinTech provider, requesting access to their financial data under the guise of offering a new service. Once they click and approve access, fraudsters could drain their accounts or misuse their data.

In open banking, third-party applications often request broad data access through user authorisation flows. If these flows are poorly designed or not accompanied by robust user verification, they become a goldmine for cybercriminals. The Cybercrime (Prohibition, Prevention, etc.) Act 2015 makes it an offence to falsely assume the identity of another person or organisation for fraudulent purposes[21].

While the Guidelines[22] and NDPA encourage strong authentication mechanisms and user awareness, there is a pressing need for user education campaigns about phishing and fake authorisation requests, security UX design that warns users when permissions requested are overly broad, and blacklist systems to block known fraudulent apps from accessing bank APIs.

4. Consent and Security of Data

Consent and data security form the backbone of ethical data processing in open banking. Under the NDPA, no personal data shall be collected or processed unless the subject has given informed, specific, and freely given consent[23]. In practice, however, issues such as consent forms often being hidden in lengthy terms and conditions, technicality or ambiguity of the language or users being unaware they can withdraw consent at any time, arise.

Additionally, the security of consented data is critical. It is not enough to obtain valid consent; data controllers must ensure that once data is shared, it is encrypted, stored securely, and only accessible to authorised personnel or systems. As more entities hold user data, the probability of breaches at any point in the data chain increases.

The NDPA places the burden of data security on the data controllers, including the obligation to foresee and prevent foreseeable threats, whether internal (employee misconduct) or external (cyberattacks). Institutions failing to meet these standards may be subject to regulatory sanctions and penalties.[24].

[19] **Article 39 of the Nigeria Data Protection Act, 2023**
[20] **Identifying Phishing as a form of Cybercrime in Nigeria, https://www.ajol.info/index.php/naujilj/article/view/215400/203155**
[21] Section 16 of the Cybercrime (Prohibition, Prevention etc.) Act, 2015
[22] **Article 9.3.1 of the Operational Guidelines for Open Banking**
[23] **Article 19 of the General Application and Implementation Directive (Gaid)**
[24] **Section 39-40 Nigeria Data Protection Act**

RECOMMENDATIONS

Based on the understanding of open banking and the associated regulatory framework, including the Guidelines, the Framework, NDPA and GAID, the following recommendations may be considered:

1. The CBN should implement more rigorous vetting processes for third-party providers, ensuring that only qualified and secure entities are granted access to customer data. This must go beyond mere registration to include deep dives into their cybersecurity posture, data governance policies, technical infrastructure, and incident response capabilities. Only demonstrably qualified and secure entities should be granted access to customer data, safeguarding sensitive financial information and reinforcing trust in the Open Banking ecosystem.

2. Regulators and financial institutions must collaborate to conduct comprehensive consumer education campaigns. These initiatives should focus on informing customers about their data protection rights, potential risks, and practical steps to identify and prevent fraud.

3. Financial institutions should be aware that they would be held liable for any damages resulting from unauthorised disclosures or security breaches caused by their third-party partners. Establishing clear liability frameworks will incentivise all parties to uphold stringent data protection standards. Financial institutions and third-party providers should prioritise the use of advanced techniques like differential privacy and k-anonymity when sharing data for analytical or development purposes. This minimises the risk of re-identification while still allowing for valuable insights to be derived from the data, aligning with international recommendations for privacy-preserving data sharing.

4. Beyond initial consent, customers should have easily accessible and understandable options to manage and revoke their data-sharing permissions at any time. This includes allowing users to specify exactly which data elements can be shared and for what specific purposes, consistent with principles of user control and transparency found in global data protection regulations. Regular prompts for users to review their consent preferences should also be implemented.

5. The Central Bank of Nigeria (CBN) and the Nigeria Data Protection Commission (NDPC) should collaborate to establish a joint Open Banking Privacy Sandbox. This controlled environment would allow financial institutions and third-party providers to test emerging privacy-enhancing technologies and data protection measures before full-scale deployment.

6. Nigeria can adopt international best practices by drawing lessons from the UK's Open Banking Implementation Entity (OBIE), which enforces stringent onboarding standards for third-party providers, mandates regular independent audits, and maintains a centralised API directory to enhance

transparency and trust within the open banking ecosystem.[25]

CONCLUSION

Open banking presents an exciting opportunity to revolutionise Nigeria's financial sector. However, the success of this model hinges on safeguarding data privacy. Stakeholders, including regulators, financial institutions, FinTechs, and consumers, must work collaboratively to ensure that personal data is handled with the highest standards of transparency, integrity, and security. Ultimately, trust is the currency of open banking, and protecting customer data is the surest way to earn and maintain it.

CONTACTS

ROTIMI AKAPO
rotimi.akapo@advocaat-law.com

ADEYEMI OWOADE
adeyemi.owoade@advocaat-law.com

MIRACLE IKANI
miracle.ikani@advocaat-law.com

[25] UK Open Banking Implementation Entity (OBIE), Standards and Guidelines, 2024.

LAGOS OFFICE
13 Norman Williams Street
Off Keffi Street, Ikoyi
Lagos Nigeria

ABUJA OFFICE
Nigerian National Merit Award House Enspire
1st Floor Room 3
Plot 22 Aguiyi Ironsi Way Maitama Abuja
Nigeria

CALABAR
Akom Building
15 Murtala Mohammed Highway Calabar
Cross River
Nigeria

TELEPHONE (LOS)+234 02014547932 (ABJ)+234 8105340496

EMAIL: info@advocaat-law.com **WEBSITE:** www.advocaat-law.com