



TOPE ADEBAYO LP

OPEN BANKING IN NIGERIA:

LEGAL CONSIDERATIONS FOR DATA
SHARING IN FINANCIAL SERVICES



OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



“Economies that embrace data sharing for finance could see GDP gains of between 1 and 5 per cent by 2030, with benefits flowing to consumers and financial institutions.” -McKinsey

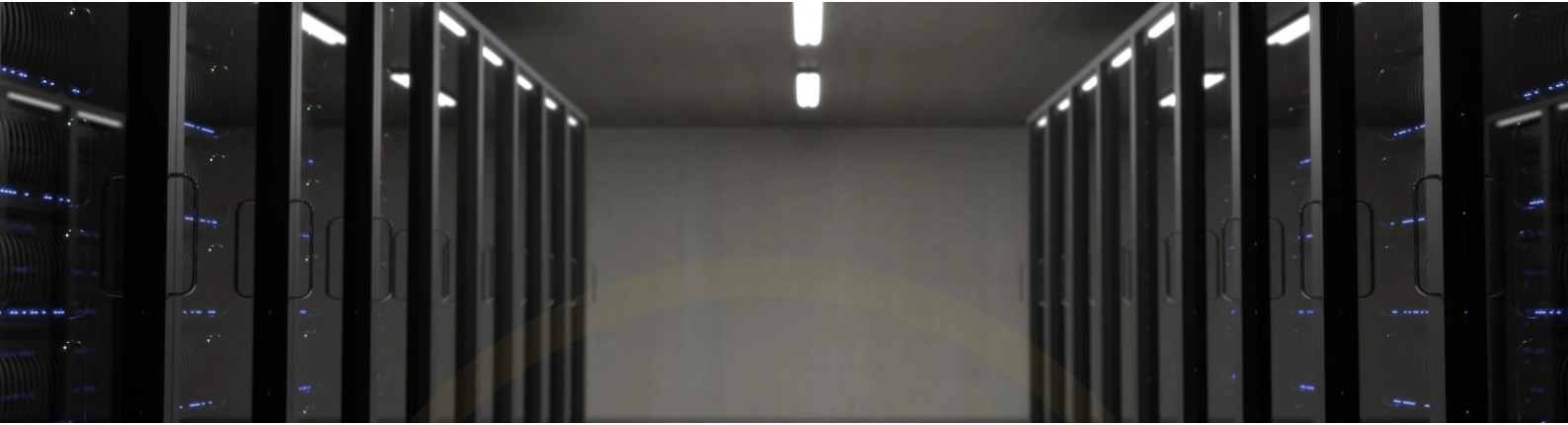
Introduction

Data is considered one of the most valuable assets in the world today. The amount of data being collected has grown exponentially with the rapid growth of digital technologies and the interconnectedness of various industries. According to the [Economist](#), 97% of businesses use data for revenue growth. The whole concept of open banking leverages the use of customers' financial data by third-party providers to personalize the customers' banking experience and create solutions and services. Data sharing must be governed by strict privacy and security measures to protect the confidentiality and integrity of customer information.

Traditionally, banks and financial institutions manage and retain customers' financial data, but with open banking, customers can manage their information by consenting to share the information with third-party companies. Nigeria joined the open banking space with the release of the Central Bank of Nigeria (CBN) [Operational Guidelines](#) for Open Banking, which outlines the framework for sharing financial data and establishes regulatory standards. This article explores key aspects of the CBN Guidelines in promoting and protecting financial data sharing in open banking and makes recommendations to enhance the effectiveness of open banking in Nigeria.



OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



Understanding Open Banking

Open banking is a system that allows third-party financial service providers to access customers' financial and non-financial data, including account information, transaction history, and other pertinent data, between various banks and approved third-party suppliers, with the customer's consent, through application programming interfaces (APIs). Open banking recognizes that customers have control and ownership over their data and can grant authorisations to service providers.

Open banking initiatives vary across different countries and regions, but they generally involve creating standardized APIs that holders of customers' data, like financial institutions, could make available to authorized third-party providers. These providers can then develop innovative applications and services that leverage the customer's financial data to deliver personalized and value-added financial solutions.

Stakeholders in Open Banking

In open banking, there are three primary stakeholders: API providers, API consumers, and customers. API providers are entities that offer their APIs to third parties, allowing them to access client data and develop financial applications and services. It is worth noting that an API provider does not necessarily have to be a bank or financial institution. However, for the pur-

OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



poses of this article, we will assume that an API provider is a financial institution, given its focus on the financial sector. An API Consumer is any third party, which can include regulated financial institutions, FMCG firms, merchants, or payroll service providers, who use consented consumer data to offer financial solutions. Customers are people or companies with bank or other financial accounts who permit third parties to access their financial information via the APIs of the API providers. This makes it possible to securely share financial data with authorized service providers, who can offer personalized financial advice and services.

Leveraging Financial Data for Open Banking

“Data is the new oil. It's valuable, but if unrefined it cannot really be used.” – Clive Humby

Financial data provides information on the financial well-being of an entity. Customers' financial data are data relating to their financial activities like income, expenses, credit history, cash inflow and outflows, and transactions. Historically, banks retain customers' data for their use and may share this data within the permissible ambit of the

law.

Within the open banking ecosystem, customers can determine how their data is utilized outside ordinary banking platforms. Both banks and non-banks can utilize customers' data to optimize financial services. Open banking not only gives customers control over their financial information, but it also allows customers to access their data across multiple platforms, not just localized banking platforms. Additionally, these third-party companies can access customers consented data to offer personalized investment advice and services, including:

- a. Enhanced financial management and decision making: Customers can access their financial information from multiple accounts or institutions from one location, and can then examine their whole financial picture, including account balances, transactions, and spending habits, through a single platform or app. Organizations and businesses can by analyzing these data, make informed decisions to improve their services and enhance operational efficiency.
- b. Personalized financial services: Open banking enables users to securely exchange

OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



their financial information with approved third parties. Based on the customer's unique financial state and needs, these suppliers can then offer personalized and specialized products and services. API Consumers can leverage financial data to personalize their offerings and tailor financial services to individual customer [preferences](#).

c. **Increased competition and innovation:** Open banking fosters competition by enabling third-party providers to offer financial products and services, which in turn promotes flexibility and responsiveness to market trends and developments. This increased competition has the potential to result in lower prices, enhanced customer

service, and the creation of innovative solutions to cater to customer needs.

d. **Facilitates payments and transfers:** Open banking facilitates faster payments and transfers. Customers can initiate transactions directly from their bank accounts through authorized third-party apps or platforms, eliminating the need for manual entry or switching between different banking interfaces. This can speed up the payment process and make it easier and more convenient.

e. **Control over data sharing:** Customer consent is usually required for sharing data under open banking. Customers can decide what data is shared and with whom, so to speak. They have more transparency and control over their personal financial information because they may revoke access at anytime.

Is the CBN's Operational Guidelines Adequate for Regulating Open Banking in Nigeria?

The 2023 CBN's Guidelines expand on the 2021 Regulatory Framework for Open Banking in Nigeria. The Framework provides for matters such as categories of data,

OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



tiers of third-party providers, responsibilities of the API Providers and API Consumers, and the required standard for an API.¹ The Guidelines provide for the establishment of an open banking registry (“OBR”), accreditation criteria, consent management, reporting standards, and risk management.

²

Additionally, the Guidelines provide that all API providers and API consumers who wish to participate in open banking must be incorporated as a company by the Corporate Affairs Commission (CAC) and have their company name and RC number registered in the OBR. The Guidelines require the API providers and API consumers to implement security measures to protect customer data and conduct regular vulnerability assessments and penetration testing. The Guidelines also make provisions for the roles and responsibilities of the CBN. Most importantly, the Guidelines emphasize customer consent, specify the types of data that can be shared and with whom, and establish standards for data protection and sharing.

The CBN's Guidelines draw inspiration from both the European Union [Revised Payment Service Directive](#) (“EU's PSD2”) and the UK's Open Banking Standard. Similarities include customer consent, strong authentication,

data protection, and API standards. Both PSD2 and the Open Banking Standard have encouraged innovation and competition in their respective markets, leading to new services and financial management tools.

Despite being a step in the right direction, the CBN Guidelines have potential lapses when compared to the UK or EU regulations. These include the absence of a specific accreditation process for third-party providers and no provision for compensating customers for losses resulting from fraud or data breaches. These gaps could impact data protection, security, and customer trust.

Global Trends on Open Banking

Nigeria is just recently delving into the open banking landscape while some countries have adopted open banking practices over the years. Open banking trends are constantly evolving however some of the significant observations are:

a. Regulatory initiatives: many countries have introduced or expanded their regulatory frameworks to facilitate open banking. The EU's PSD2 has been a driving force, requiring banks to provide access to customer data through APIs and promoting competition and innovation. Other coun-

²Paragraphs 6 to 11 of the Guidelines

OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



tries, such as the United Kingdom, Australia, Singapore, and Canada, have also implemented open banking regulations or initiatives to promote data sharing and consumer-centric financial services.

b. **Collaborations and partnerships:** Collaboration between traditional banks and fintech startups have become more prevalent in open banking. Banks recognize the need to embrace innovation and customer-centric approaches, leading to partnerships with fintech companies to leverage their technology expertise. These collaborations aim to combine the strengths of traditional banking infrastructure with the innovation of fintech to deliver enhanced services to customers.

c. **Data security and privacy:** As the sharing of sensitive financial data increases, ensuring robust data security and privacy measures becomes paramount. Open bank-

ing initiatives prioritize the protection of customer data through secure API standards, encryption, and consent management. Compliance with data protection regulations, such as the Global Data Protection Regulation, is a critical aspect of open banking implementations.

d. **Global adoption and standardization:** Open banking is gaining traction globally, with various countries and regions adopting similar principles and standards. Efforts are being made to establish interoperability and common standards for APIs, data formats, and security protocols. International organizations and industry consortia are working towards harmonizing open banking practices to facilitate cross-border data sharing and interoperability.

Legal Considerations for Data Sharing

“Data is the greatest asset in the world, but it's also the most vulnerable. Protect it, respect it, and share it wisely.” - Tim Berners-Lee

Open banking necessitates data exchange, which entails risks and legal considerations such as data protection and privacy, data

OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



ownership and governance, data ethics, and trust. These risks can be effectively managed using robust security measures and regulatory oversight.

1. Data Breach: Open banking is designed to share customers' data with third-party providers which poses potential risks of data breach on the face of it. Data sharing must comply with the relevant laws and regulations that govern how personal and sensitive data can be collected, used, and shared. However, while these potential risks of breaches associated with open banking exist, it is not necessarily a data breach in and of itself. The security and privacy risks associated with open banking can be mitigated using robust security measures and data protection mechanisms.

For example, similar to the UK's Open Banking Standard and the EU's PSD2 regulation, the CBN's Guidelines mandate financial institutions and third-party providers to implement strong customer authentication measures, encryption of data in transit and at rest, strong controls to restrict access to customer data, and other security measures designed to protect customer data from unauthorized access or use. Furthermore, the CBN, like the Capital Markets Authority

(CMA) in the United Kingdom and the European Banking Authority (EBA) in the European Union, is the regulatory agency in charge of overseeing the implementation of open banking and enforcing compliance with essential data protection rules. These regulatory bodies are responsible for ensuring that banks and third-party providers meet the necessary security and privacy requirements, and for investigating and addressing any breaches or non-compliance issues that may arise.

2. Data ethics and trust: Data sharing must adhere to ethical principles and values that guide how data is used and shared. [Data sharing](#) must also build trust among data providers, recipients, and subjects by demonstrating the benefits, risks, and safeguards of data sharing.

3. Consent and authorization: Prior consent from customers is crucial when sharing their financial data. Organizations should establish clear consent mechanisms, ensuring that individuals have a comprehensive understanding of what data is being shared, with whom, and for what purposes. Consent should be freely given, specific, informed, and revocable.

OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



4. Data minimization and purpose limitation: Organizations should adhere to the principles of data minimization and purpose limitation. Only collect and share data that is necessary for the intended financial service and ensure that the data is not used for purposes beyond what was initially consented to.

5. Security and confidentiality: Robust security measures should be implemented to protect shared data from unauthorized access, breaches, or misuse. Encryption, access controls, and regular security audits are some measures that can help safeguard sensitive financial data.

6. Regulatory compliance: Financial institutions and third-party providers need to comply with specific regulations govern-

ing their industry, such as anti-money laundering (AML) and know-your-customer (KYC) regulations. Ensure that data-sharing practices align with these regulatory requirements to prevent illegal activities and financial fraud.

7. Cross-Border Data Transfers: If data is being shared across borders, organizations should comply with applicable cross-border data transfer regulations, such as the Nigeria Data Protection Act 2023 requirements for adequate safeguards or specific transfer mechanisms like Standard Contractual Clauses (SCCs) or Binding Corporate Rule (BCR).

8. Vendor Management: When engaging third-party providers for data sharing, organizations should have contractual

OPEN BANKING IN NIGERIA: LEGAL CONSIDERATIONS FOR DATA SHARING IN FINANCIAL SERVICES



agreements in place that outline the responsibilities, obligations, and data protection measures expected from the vendor. Conduct due diligence to ensure that the third-party provider adheres to relevant data protection regulations.

Challenges with the CBN's Operational Guidelines

The following are some gaps that the CBN needs to improve.

1. Accreditation: While the Nigerian regulation requires third-party providers to be licensed by the CBN, it does not have a specific accreditation process like the UK's Open Banking Standard, which requires third-party providers to undergo rigorous testing and accreditation before being allowed to access customer data. This could potentially lead to a lower standard of security and reliability among third-party providers in Nigeria. We recommend that a robust and unbiased accreditation process for third-party providers be implemented to maintain a high standard of security and reliability.

2. Compensation: The Guidelines do not require financial institutions to compensate customers for any losses resulting from

open banking-related fraud or data breaches. This could discourage customers from participating in open banking and limit its potential benefits. It is worth noting, that the Nigerian regulation on open banking is a step in the right direction which is still evolving and may be updated over time to address these and other potential lapses. We recommend that financial institutions be required to compensate customers for any damage or losses resulting from open banking-related fraud or data breaches, to promote customer's trust and confidence in the open banking system.

Conclusion

Open banking has the potential to transform the Nigerian financial sector, but it must be accompanied by strong security measures and customer protection. The CBN Guidelines provide a foundation for open banking in Nigeria, but improvements are necessary to align with international standards. By addressing the recommended enhancements, Nigeria can harness the benefits of open banking while safeguarding customer data and promoting innovation and competition in the financial services industry.

PLEASE NOTE THAT THIS ARTICLE IS FOR INFORMATION PURPOSES ONLY AND DOES NOT CONSTITUTE LEGAL ADVICE

MEET THE AUTHORS



IFEOMA EZERIBE
MANAGING ASSOCIATE

EXCELLENT T. EPELLE
ASSOCIATE TRAINEE

Brought to you by TALP's Corporate and Commercial Department

For further enquiries, log onto www.topeadabayolp.com

Do you need to get in touch with us, to know more how we can help you and your business?
Please contact us using any of the details provided below:

TOPE ADEBAYO LP

25C Ladoke Akintola Street, G.R.A. Ikeja Lagos, Nigeria
p: +234 (1) 628 4627
e: info@topeadabayolp.com
w: www.topeadabayolp.com

