TLP ADVISORY

Open Banking in Nigeria

Client Briefing Note

April, 2023

Introduction

On 07 March 2023, the Central Bank of Nigeria (the "CBN") issued the Operational Guidelines for Open Banking in Nigeria (the "Guidelines"), making Nigeria the first African country to adopt open banking regulations. We are excited about this development as it is a potential game-changer for the Nigerian fintech sector and tech sector in general.

The CBN, in collaboration with industry stakeholders, developed the Guidelines in line with the provisions of the Regulatory Framework for Open Banking in Nigeria 2021. The Guidelines provide a framework for data sharing across the banking and payments ecosystem in Nigeria and outline the risk management requirements and standards for the open banking participants.

In this client briefing note, we will explain this framework and its potential impact on your business.

What is Open Banking?

Open Banking is the practice of using open technologies to share financial information electronically with third-party financial service providers. It provides guidance on how third-party financial service providers can access and utilise customer bank data in a standard format from a centralised location to provide more open, transparent and competitive financial services.

Under the Guidelines, the sharing of financial data is enabled by the use of open Application Programming Interfaces (APIs). APIs allow for the transmission of data by allowing financial service providers with different technology platforms to interact with one another.

Open Banking Registry

The CBN maintains an open banking registry (the "Registry") that serves as the primary means by which API Providers manage the registration of their API Consumers. The Registry is also responsible for providing regulatory oversight and enhancing the operations of open banking in Nigeria.

The Guidelines require that data shared within the open banking system follow standards such as the 9 ALCOA+ principles of data integrity, i.e. the data must be **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, **A**ccurate, **C**omplete, **C**onsistent, **E**nduring, and **A**vailable.

API Providers are only authorized to share information about a customer with an API Consumer upon receipt of valid proof of consent from the customer. The API Providers are required to authenticate this consent to ensure that it originates from the customer.

Participants of Open Banking in Nigeria

Open banking participants refer to any organisation in possession of customers' data, which may be exchanged with other entities to provide innovative financial services within Nigeria. The Guidelines categorise the participants into the following:

- **API Provider**: This refers to a participant that uses API to provide data or service to another participant. The API Provider can be a licensed financial institution/service provider, a health technology company, an insurance technology company, an education technology, an entertainment company, and any other company that can provide customers' data.

- **API Consumer**: This refers to a participant that uses API released by the API providers to access data or services. The API Customer can be a licensed financial institution/service provider, an FMCG or other retailer, Payroll Service Bureau, a health technology company, an insurance technology company, an education technology, an entertainment company, and any other company that can require access to customers' data.

- **Customer**: This refers to the data owner who is required to provide consent to the API Provider for the release of his data to enable him access financial services.

Data and Service Catergories in Open Banking Syetem

A combined analysis of the Guidelines and the Framework establishes the following data and service categories:

- **Product Information and Service Touchpoints (PIST) - low risk**: This includes information on products provided by participants to their customers and access points available for customers to access services e.g. ATM/POS/Agents locations, channels (website/app) addresses, institution identifiers, service codes, fees, charges and quotes, rates, tenors, etc.

- **Market Insight Transactions (MIT) – moderate risk**: This includes statistical data aggregated on basis of products, service, segments, etc. This data is not associated with any individual customer or account. This data could be exchanged at an organisational level or an industry level.

- **Personal Information and Financial Transaction (PIFT) – high risk**: This includes data at the individual customer level which can be either general information on the customer (e.g. KYC data, total number or types of account held, etc.) or data on the customer's transaction (e.g. balances, bills payments, loans, repayments, recurring transactions on customer's accounts, etc.)

- **Profile, Analytics and Scoring Transaction (PAST) – high and sensitive risks**: This includes information on a customer which analyses, scores or gives an opinion on a customer e.g. credit score, income ratings etc.

Data Access Levels and Risk Management Requirements

Participant Category	Risk Management Maturity Level	Access Level by Data and Service Category	Sponsors	Risk Management Requirements
Participants without regulatory licence	Tier 0	PIST and MIT	Tier 2 or Tier 3	The sponsors must ensure that Tier 0 participants complete a thorough risk assessment report, signed by the Chief Risk Officer of the sponsoring party, within three working days of registration on the Registry.
Participants through the Bank Regulatory Sandbox	Tier 1	PIST, MIT and PIFT	Tier 2 or Tier 3	Sponsors must ensure that Tier 1 participants have sufficient corporate governance and risk management policies and procedures in place to effectively manage potential risks that could impact the services provided
Licensed Payment Service Providers and other Financial Institutions	Tier 2	PIST, MIT, PIFT and PAST	None	At the minimum, Tier 2 participants are required to implement corporate governance and maintain the below-listed business operational documents and processes

Deposit Money Banks	Tier 3	PIST, MIT, PIFT and PAST	None	At the minimum, Tier 2 participants are required to implement corporate governance and maintain the below-listed business operational documents and processes

Contract Management

API Providers and API Consumers are required to execute a Service Level Agreement (SLA) to govern their relationship. At the minimum, the SLA is required to include accounting and settlement provisions, fee structure, roles and responsibilities of the parties and any third party, and comprehensive dispute resolution processes, including timelines for resolution.

When asking a customer for consent, it should be done in the manner stated in the SLA. The customer should be provided with a copy of the customer's consent and the API Provider and API Consumer are required to keep a copy of such consent. If the customer's data will be shared with a third party, such as an outsourced service provider, a contract must be signed and approved by the CBN.

Cyber Security, Data, and Information Management

API Providers and API Consumers are required to develop and maintain the following:

- Data governance policy that ensures that all aspects of the data are well-managed and fulfil legal and regulatory requirements
- Data privacy agreements, which must comply with the Nigerian Data Protection Regulation 2019 or any CBN-issued data protection regulation for financial institutions, to protect customer data
- Data ethics framework
- Information security policy
- Data breach policy and procedure
- Incident management procedure

To protect the confidentiality, integrity and availability of information and data in the open banking system, the participants are required to implement information security controls in line with the security standards with minimum security principles encapsulated in the United States of America National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC).

Business Operational Documents and Processes

API Providers and API Consumers are required to develop the following operational documents and policies:

- Regulatory risk framework
- Risk assessment report, and evaluation criteria
- Insurance policy to cover losses
- Know Your Customer/Continuous Due Diligence Policy (KYC/CDD)
- Know Your Partner Checklist (KYP)
- AML/CFT Due Diligence
- Dedicated compliance officer
- Compliance policy/manual
- Security policies
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Communication plan for all incident types
- Ticket management systems and processes
- Reporting templates and systems
- Fraud management processes
- Legal and business framework for treating liabilities.

Reporting and Monitoring

API Providers and API Consumers are required to send monthly reports to the CBN on their API performance, including but not limited to incidents, compliance with SLAs, fraud, disputes, and changes made. API Providers also have to let customers know when an API Consumer accesses their account and provide them with a report. Additionally, API Providers and API Consumers must monitor their API infrastructure and report to the CBN monthly using the Registry API interface, while also complying with extant AML/CFT regulations and cyber-security frameworks and guidelines for financial institutions in Nigeria.

Conclusion

Should you want to integrate your products or services within the Nigerian open banking system, we, at TLP Advisory, can help you navigate the legal and regulatory landscape. We are also able to advise on compliance with data protection and cybersecurity regulations, intellectual property protection, negotiating contracts with third-party providers, and related legal issues.

Please do not hesitate to reach out to us via email at **info@tlpadvisory.com** with any questions or concerns.

Esther Oyewole
Associate
TLP Advisory