ÆLEX

ARTICLE SERIES

REVIEW OF THE DRAFT OPERATIONAL GUIDELINES FOR OPEN BANKING IN NIGERIA

JUNE 2022

www.aelex.com

WHAT IS OPEN BANKING?

We had earlier delved into the concept of Open Banking and its regulatory framework in our articles accessible here[1] and here[2]. In summary, Open Banking is a system that grants third-party providers (TPPs) open access to consumer banking, transactions, and other financial data from banks and non-bank financial institutions(NBFIs) through the use of Application Programming Interface (API).

With Open Banking, customers can share their financial data with different financial institutions. In order for this to be effected, the institution require the express consent of the customers. It represents a shift from a closed model, where financial institutions operated in silos, to one in which data is shared between different members of the banking ecosystem with authorisation from the customer.

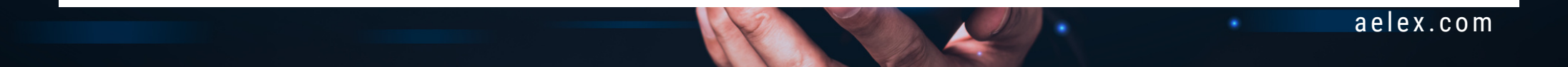
Thus, with Open Banking, service providers are able to communicate seamlessly through the networking of accounts and data across institutions for use by consumers, financial institutions, and TPPs.

Open Banking will lead to a situation where regardless of how many accounts and financial products a customer has with multiple institutions, he can manage them from a centralised location without having to check out from one system to another.

For example, a consumer could have a bank account with GTBank and operate an account with a fintech like Piggyvest. When the customer wants to check his inflows and outflows from his different accounts, he will have to log into the separate platforms.

However, with Open Banking, the customer can seamlessly operate his investments and track his transactions on different platforms from a centralised location through the use of APIs. The APIs can also look at the transaction data of the customer and identify the best financial products he can invest in that would yield better interest rates.

[1] Regulatory framework for Open Banking in Nigeria
[2] The Effect Of Nigeria's Data Protection Regime On Open Banking



Developments in Nigeria

In February 2021, the Central Bank of Nigeria (the "CBN") released the Regulatory Framework for Open Banking in Nigeria (the "Open Banking Framework") to provide an enabling regulatory environment for provision of innovative and customer-centric financial services through the safe utilisation of shared data.

In May 2022, and building on the Open Banking Framework, the CBN released the Exposure Draft of the Operational Guidelines for Open Banking in Nigeria (the "Operational Guidelines"). The Operational Guidelines set out detailed provisions on the responsibilities and expectations for the participants in the Open Banking ecosystem, the framework for sharing information and customer experience standards, among others.

This article therefore examines the salient provisions of the Operational Guidelines in line with relevant provisions of the Open Banking Framework, and their implications for Open Banking in Nigeria.

KEY PROVISIONS

Scope

The Operational Guidelines are applicable to banking and other related financial services as identified in the Open Banking Framework.[3] These services are:

1. payment and remittance;
2. collection and disbursement;
3. deposit-taking;
4. credit rating/scoring;
5. personal finance advisory and management;
6. treasury management;
7. credit;
8. leasing/hire purchase;
9. mortgage; and
10. other services as may be determined by the CBN[4]

Participants

The Operational Guidelines provides that any organisation with customer data which may be shared with other entities to achieve the provision of innovative financial services within Nigeria is eligible to participate in the Open Banking ecosystem.

[3] Paragraph 4.0 of the Operational Guidelines
[4] Paragraph 5.0 of the Open Banking Framework

The import of this is that even organisations that non-financial service providers are eligible to participate, subject to compliance with the relevant laws and regulations.[5]

The categorisation of participants is based on the specific roles they may perform, while acknowledging that participants may assume more than one role depending on their offerings. These participants are:

1. API Provider – this refers to a participant that uses APIs to provide data or service to another participant. Notably, the CBN has adopted a broad eligibility approach; as such, an API Provider can be a licensed financial institution/service provider, a Fast-Moving Consumer Goods (FMCG), retailer, Payroll Service Bureau etc.

2. API Consumer – this refers to the participant on the receiving end that uses API released by API Providers to access data or service. Like an API Provider, an API Consumer can be a licenced financial institution/service provider, an FMCG, company, retailer, Payroll Service Bureau etc.

3. Customer – this refers to the data owner and end-user whose consent is required for the release of their data for the purpose of accessing financial services.

Categories of Data and Risk Rating

One of the notable provisions of the Open Banking Framework is its classification of data that can be exchanged by participants into four categories. The categories of data are further assigned risk ratings based on their sensitivity and are as follows:[6]

[5] Paragraph 4.1 of the Operational Guidelines
[6] Paragraph 4.1 of the Open Banking Framework

SN	CATEGORY	DESCRIPTION	RISK RATING
1	Product Information and Service Touchpoints (PIST)	Includes information on products provided by the participants to their customers and access points available for customers to access services e.g ATM/POS/Agent locations, channels (website/app) addresses, institution identifiers, service codes, fees, charges and quotes, rates, tenors, etc.	Low
2	Market Insight Transactions (MIT)	Includes statistical data aggregated based on products, service, segments, etc. It is noteworthy that this category of data is not associated to any individual customer or account.	Moderate
3	Personal Information and Financial Transaction (PIFT)	Includes data at the level of the individual customer which can be general information on the customer e.g. KYC data, number of accounts held, etc., or data on the customer's transactions e.g. balances, bills payments, loans, repayments, recurring transactions on customer's accounts etc.	High
4	Profile, Analytics and Scoring Transactions (PIST)	Includes information on a customer which analyses, scores or gives an opinion on a customer e.g. credit score or income ratings.	Sensitive

Tiers of Participants

The participants in Open Banking have also been grouped into tiers based on how trusted they are, with attendant restrictions to the categories of data accessible to each tier of participants. The tiers of participants are as follows: [7]

SN	TIER	PARTICIPANT
1	0	A participant without a regulatory licence. This participant must be sponsored by a Tier 2 or Tier 3 participant and can only access PIST and MIT data.
2	1	This refers to participants through the CBN Regulatory Sandbox. Participants under this tier are given access by virtue of their admission into the CBN Regulatory Sandbox and can access PIST, MIT and PIFT data.
3	2	This refers to Licenced Payment Service Providers and other financial institutions. These participants have access to all categories of data.
4	3	This category is for Deposit Money Banks. Participants in this tier also have access to all categories of data.

[7] Paragraph 5.1 of the Open Banking Framework

RESPONSIBILITIES OF PARTICIPANTS

API Providers

The Operational Guidelines places enormous responsibilities on API Providers to ensure adequate planning, monitoring, security and efficiency of their operations. Some of the notable responsibilities of API Providers include:

a) API Providers are required to execute Service Level Agreements ("SLA") with API Consumers to govern their relationships. The SLA must provide for accounting and settlement, fee structure, reconciliation of bills, registration and sponsorship responsibilities, etc.[8]

b) API Providers are required to device an incident management plan which provides for classification of incidents and incident management procedures. The incident management procedure must include provisions on determining the scope and impact of an incident, notification of API Consumers, investigation of root cause and resolution of the incident.[9]

c) API Providers are required to provide or prescribe secure real-time communication platforms for first level incident responders within their organisation and respective API Consumers for incident notification, investigation and resolution. Specifically, the communication platform shall accommodate text, voice and video conferencing modes of communication to support various scenarios; and emails have been designated as an insufficient method of incident management communication.[10]

d) API Providers also have reporting obligations to API Consumers on performance levels, statistics of incidents/problems, SLA compliance, number and category of fraud and disputes, etc.11] Similar reporting obligations are also owed to customers, notably when an API Consumer accesses the customer's account(s)/wallet(s).[12]

e) API Providers are barred from engaging in unethical and unprofessional anti-competition practices such as de-marketing.[13]

[8] Paragraph 8.1.2 of the Operational Guidelines
[9] Paragraph 8.2.2 of the Operational Guidelines
[10] Paragraph 8.7.1 of the Operational Guidelines
[11] Paragraph 8.8 of the Operational Guidelines
[12] Paragraph 8.8.2 of the Operational Guidelines
[13] Paragraph 8.9 of the Operational Guidelines

API Consumer

In the same vein, the Operational Guidelines places responsibilities on the API Consumer, particularly as it relates to data ethics, protection against data breach and information security. Some of the responsibilities on API Consumers include:

a) Every API Consumer is required to maintain a Data Governance Policy approved by a committee of its Board of Directors or at least, an executive management committee of the API Consumer.[14]

b) Similarly, API Consumers are expected to develop and maintain effective Information Security Policy, while conducting regular threat assessments.[15]

c) API Consumers must comply with the Nigeria Data Protection Regulation or any other CBN issued data protection regulation for financial institutions, while ensuring that they are constantly protected against data breaches.[16]

d) API Consumers are also required to render returns to the CBN monthly, detailing volume of transactions, value of transactions, number of users, success rates, security and fraud incidents, etc.[17]

OTHER RELEVANT PROVISIONS

Intellectual Property Preservation and Ownership of Open Data

The Operational Guidelines provides that participants' intellectual property in proprietary and protectable software source and object codes, aggregate data and aggregate services among other protectable information shall be protected under the applicable laws in Nigeria.[18]

Furthermore, all ownership rights in any open data or other information shall at all times remain with the party or the participant from which such data or other information originated, whether the open data or other information is in human or machine-readable form.[19]

Open Banking Registry

According to the Operational Guidelines, the CBN shall provide and maintain an Open Banking Registry (the "OBR") to provide regulatory oversight on participants; enhance transparency in the operations of Open Banking; and ensure that only registered institutions operate within the Open Banking ecosystem.[20]

[14] Paragraph 9.1 of the Operational Guidelines
[15] Paragraph 9.3.1 of the Operational Guidelines
[16] Paragraph 9.2 of the Operational Guidelines
[17] Paragraph 9.4 of the Operational Guidelines
[18] Paragraph 11.12 of the Operational Guidelines
[19] Paragraph 11.12.3 of the Operational Guidelines
[20] Paragraph 6.0 of the Operational Guidelines

The OBR shall serve as a public repository for details of registered participants, who shall be identified by their respective business registration numbers issued by the Corporate Affairs Commission (the "CAC").

Shared Information Framework

The Operational Guidelines make provision for a shared information framework, making Customer consent the sole basis for sharing customer information. Accordingly, an API Provider is only permitted to share information of a Customer with an API Consumer upon presentation of valid proof that the Customer has consented to the sharing, and such consent shall be authenticated to confirm it emanates from its Customer.[21] The verification of validity of consent exercise by the API Provider shall ascertain that:

1. The consent emanated from its Customer;
2. Request for customer's data contains the purpose of the request;
3. Request contains credentials of the requesting end-user;
4. Request contains a valid date and was made through appropriate channels.

[21] Paragraph 11.2 of the Operational Guidelines
[22] Appendix IV to the Operational Guidelines

Customer Experience Standards

A constant theme with the Operational Guidelines is the prioritisation of the Customer's safety and convenience. Accordingly, it mandates that participants shall prioritise customer experience in the operation and implementation of Open Banking.

Further to this, it stipulates the following customer experience principles which participants must implement: [22]

1. Control – Participants must provide Customers with the right tools and clarity of information at the right time. Furthermore, Customers must be made aware that they can view and cancel any consent given whenever they deem fit.

2. Speed – Participants are to ensure that each interaction has appropriate speed, clarity and efficiency without compromising security and control.

3. Transparency – Progressive levels of information must be provided to Customers in plain language. For example, where information is required from Customers, there must be clarity of any such information required, the reason and purpose of the requirement, and consequences of supplying the information.

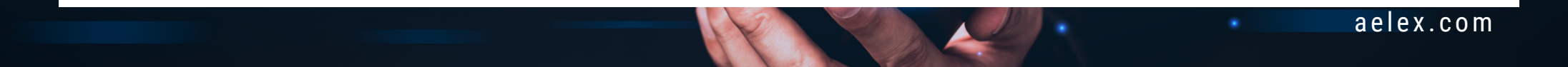
4. Security – Finally, participants must give assurances in relation to Customer data definition, use, security and protection.

CONCLUSION

The benefits of Open Banking, such as enablement of innovative products and services, competition and better customer experience are undeniable. However, a major risk with its adoption and implementation still remains data/security breach and abuse.

Indeed, this observation prompted the release of our publication titled "*The Effect of Nigeria's Data Protection Regime on Open Banking*" in May 2021, shortly after the CBN indicated its intention to facilitate the implementation of Open Banking in Nigeria.

Evidently, with the release of the Operational Guidelines, the CBN is aware of the risks associated with Open Banking and has consequently made comprehensive provisions to extirpate these risks. Accordingly, if properly implemented, the Operational Guidelines has the potential of ensuring the safe operation of Open Banking in Nigeria.



ÆLEX

AUTHOR

Davidson Oturu

Mubaraq Popoola

For further information, please contact:

Davidson Oturu
(doturu@aelex.com)

Frances Obiago
(fobiago@aelex.com)

Florence Bola-Balogun
(fbola-balogun@aelex.com)

Peretimi Pere
(Ppere@aelex.com)

Ifeoluwa Ebiseni
(iebiseni@aelex.com)

Ilamosi Ekenimoh
Iekenimoh@aelex.com)

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed here. You can also visit our website at www.aelex.com to learn more about our firm and its services.'

CONTACT DETAILS

LAGOS, NIGERIA

4th Floor, Marble House
1, Kingsway Road, Falomo
Ikoyi, Lagos

Telephone: (+ 234 1) 2793367; 2793368
4736296, 4617321-3;
Facsimile: (+ 234 1) 2692072; 4617092
E-mail: lagos@aelex.com

PORT HARCOURT, NIGERIA

2nd Floor,
Right Wing UPDC Building
26, Aba Road
P.O. Box 12636, Port Harcourt
Rivers State, Nigeria

Telephone: (+234 84) 464514, 464515
574628, 574636
Facsimile: (+234 84) 464516, 574628
E-mail: portharcourt@aelex.com

ABUJA, NIGERIA
4th Floor,
Adamawa Plaza
1st Avenue, Off Shehu Shagari Way
Central Business Area
FCT Abuja, Nigeria

Telephone: (+234 9) 8704187, 6723568,
07098808416
Facsimile: (+234 9) 5230276
E-mail: abuja@aelex.com

ACCRA, GHANA

Suite CCasa Maria
28 Angola Road
Kuku Hill, Osu
Accra

Telephone: (+233-302) 224828, 224845-6
Facsimile: (+233-302) 224824
E-mail: accra@aelex.com