ALUKO & OYEBODE

CBN ISSUES REGULATORY FRAMEWORK FOR OPEN BANKING IN NIGERIA

May 2021

Introduction

Open banking was first implemented in the United Kingdom through the revised Payment Services Directive (PSD2) and Open Banking Standard in 2018 and since then several jurisdictions around the world have begun to adopt their own approaches to open banking.[1]

In line with its mandate to promote the stability and deepening of the financial system, on 17 February 2021, the Central Bank of Nigeria (the "**CBN**") issued the regulatory framework for open banking in Nigeria (the "**Framework**"). The Framework stipulates, among other things for the access requirements for data and Application Programming Interface (API), principles for API, data, technical and information security specifications.

What is Open Banking?

Open banking is the arrangement that allows you as a customer (end-user) to authorise your bank or financial service provider to share your financial information with other participants within the financial services system (e.g., other banks, third party financial service providers) so as to develop more customer-centric services and financial products. Open banking is powered by a technology called Application Programming Interface (API). With open API, participating banks and other financial institutions will be able to access information on other participants' financial products and services as well as personal information, transaction history, credit score, income ratings etc. of other participants' individual customers.

For example, open banking will allow an investment app to have access to a person's financial information (including number of accounts, balances, loans, repayments etc.) from all that person's banks or financial service providers (provided the person has granted consent to same) in one central location.

Who are the Participants?

The participants in an open banking arrangement under the Framework are categorised into the following tiers: Tier 0 (participants without regulatory licence), Tier 1 (participants within the CBN regulatory sandbox), Tier 2 (licensed payments service providers and other financial institutions), and Tier 3 (deposit money banks). Participants may assume any of the following roles based on the level of their risk maturity: (a) API provider; (b) API user; (c) financial technology companies (FinTechs)[2]; and (d) developer community.

The API is developed or designed by the developer community based on requirements under this Framework. The API provider on the other hand defines the data and services accessible through the APIs. The API user (usually FinTechs) executes a data access agreement and service level agreement with the provider to access data or services through the APIs. The end-users are the customers whose data are released through the API.

[1] Deloitte, Open Banking: Disruption is afoot for regulators as well as banks (Deloitte Perspectives) available at <Open Banking: Disruption is afoot for regulators as well as banks | Deloitte UK> 16 April 2021.

[2] FinTechs are usually consumers of APIS, however there could be occasions where FinTechs are also providers of API. In either case, FinTechs will assume the responsibilities of a provider or consumer depending on the role they play at any point in time.

Scope

The Framework is specifically focused on the following types of banking and other related financial services: (a) payments and remittance services; (b) collection and disbursement services; (c) deposit-taking; (d) credit; (e) personal finance advisory and management; (f) treasury management; (g) credit ratings/scoring; (h) mortgage; (i) leasing/hire purchase; and (j) other services as may be determined by the CBN.

Data and Service Categories

Under the Framework, not all customer data and services are eligible to be exchanged through APIs. Only the following categories of data may be exchanged, and corresponding API services may be implemented by and used by participants:

S/N	Category	Data/Information Covered	Risk Rating
1.	Product information and service touchpoints (PIST)	Information on products provided by participants to their customers and access points available for customers to access those services will be covered e.g., automated teller machine (ATM)/point of sale (POS)/agents' locations, channel (website/app) addresses, institution identifiers, service code, fees, charges and quotes, rates, tenors etc.	Low
2.	Market insight transactions (MIT)	Statistical data aggregated on basis of products, service, segments, etc. and which are not specific to any individual customer or account will be covered and could be exchanged either at an organisational or industrial level.	Moderate
3.	Personal information and financial transaction (PIFT)	General information on an individual customer (e.g., know your client (KYC) data, total number or types of account held etc.) or data relating to the customer's transactions (e.g., balances, bills payments, loans, repayments, recurring transactions on customer's accounts, etc).	High
4.	Profile, analytics and scoring transaction (PAST)	Information on a customer which analyses, scores, or gives an opinion on a customer e.g., credit score, income ratings etc.	High & Sensitive

Data and Service Access Governance

Under the Framework, access to the different categories of data set out above will be determined by the risk management maturity level of the participant. The risk management maturity level of participants will range from Tier 0 to Tier 3. Data and API access requirements among participants of various maturity level would be as follows:

(a) **participants without regulatory licence (Tier 0)**: Tier 0 participants will only have access to PIST and MIT data (as defined above). Tier 0 participant must be sponsored by a Tier 2 or Tier 3 participants who will be responsible for making the application

for registration on the open banking registry on its behalf. The Application for registration will be accompanied by a comprehensive risk assessment report on the Tier 0 participant, duly signed by the Chief Risk Officer of the sponsoring Tier 2 or 3 participant;

(b) **participants through the CBN regulatory sandbox (Tier 1):** Tier 1 participants must have been admitted into the CBN regulator sandbox and will only have access to PIST, MIT and PIFT data (as defined above). Please note however that the CBN may, as it deems fit and, on a case-by-case basis, stipulate further requirements for eligibility as Tier 1;

(c) **licensed payments service providers (PSSPs) and other financial institutions (Tier 2):** Tier 2 participants will have access to all categories of data i.e., PIST, MIT, PIFT and PAST data (as defined above). Tier 2 participants must hold a valid licence from the CBN and must present a satisfactory risk assessment report by at least two (2) partner participants including both Tier 2 and Tier 3 participants before it can be listed on the open banking registry; and

(d) **deposit money banks (DMBs) (Tier 3)**: Tier 3 participants also have access to all categories of data i.e., PIST, MIT, PIFT and PAST data (as defined above). The tier 3 participant must hold a valid licence from the CBN and must present a satisfactory risk assessment report by at least two (2) partner participants which must be a tier 2 and 3 participants before it can be listed on the open banking registry.

Guiding Principles for API Specifications

The CBN will be responsible for facilitating the development of a common banking industry API standard. The development of common API standard by the industry and/or by participants will be guided by the following principles: (a) openness[3]; (b) reusability[4]; (c) interoperability[5]; (d) modularity[6]; (e) robustness[7]; (f) user-centric;[8] and (g) security.[9]

Specifications for Data, Information, Data standards, Information Security Standards
The Framework provides the following list of standards that should be adopted for API design, data, and information security:

(a) **API Design Model Standard:** Representational State Transfer (REST) and Simple Object Access Protocol (SOAP);

(b) **Data Standards:** Open Financial Exchange (OFX), eXtensible Business Reporting Language (XBRL) and ISO 9735- Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT), Financial product Markup Language (FpML),

[3] Accessible to all interested and permissioned parties.
[4] Premised on existing standards and taxonomy of technology.
[5] Supports exchange of object across technologies, platforms, and organisations.
[6] Loose coupling with provision for flexible integration.
[7] Scalable, improvable, evolvable, and transparent.
[8] Enhances user experience for consumers.
[9] Ensures data privacy and safe exchanges and transactions.

Financial Information Exchange (FIX), Market Data Definition Language (MDDL), Security Assertion Markup Language (SAML) 2.0, ISO 20022 and Statistical Data and MetaData eXchange (SDMX)

(c) **Information Security Standards**: These are further categorised into the following:

I. Authentication: OAuth 2.0, OpenID Connect, FAPI and Security Assertion Markup Language (SAML) 2.0;

II. Authorisation: OAuth 2.0, ISO 10181-3 – Access Control Framework and FAPI;

III. Encryption: Transport Layer Security (TLS) v. 1.2, RSA Public/private key, AES and Secure File Transfer Protocol (SFTP);

IV. Data integrity: JSON Web Token (JWT), WS Security and Keyed Hash Message Authentication Code (HMAC); and

V. Secure hosting: ISO 2700, ISO 22301, and PCI DSS.

Guidance on Operational Rules

According to the Framework, operational rules must ensure consistent application based on RM maturity levels defined. Data Access Agreements (DAA) and Service Level Agreements (SLA) among participants must be mandatory under any operational rules. All operation rules must discourage dominant party and anti-competition practices and ensure dispute resolution protocols for basic operational issues are codified.

Participants' Roles and their Responsibilities

S/N	Provider	API Users	FinTechs	Developer Community	CBN
1.	Publish the APIs and define requirements and technical guidelines; leverage the common Banking Industry API Standard.	Execute a DAA and SLA with the API provider ("**Provider**").	Ensure that it leverages API to innovate products and solutions that are interoperable.	Comply with the provisions of this Framework.	Oversee the implementation and operations of open banking in Nigeria.
2.	Define the data and services accessible through the APIs and establish DAA and SLA with other participants.	Obtain consent of the end-user on each action that may be performed on of the end-user's and specify the	Avoid alteration of APIs published by the Provider without consent of the providers.	Execute service agreements with the partner participant outlining the participant's business	Enforce this Framework.

		implications of the consent to be given.		requirement and technical guidelines.	
3.	Carry out Know Your Partner (KYP) due diligence on partner participants which before executing any DAA or SLA.	Cooperate with the Provider for the regular monitoring of its control environment and ensure annual re-validation of DAA and SLA.	Comply with data privacy laws and regulations.	Employ secure coding and development standards and practices.	Arbitrate disputes among participants before any litigation or commencement of judicial process.
4.	Ensure partner participant obtains consent of the end-user and certify that the partner participant define to the end-user the implication of granting such consent.	Implement any remedial actions to management vulnerabilities in its environment.	Maintain customer service/complaint desk on 24 hours/7 days a week basis for financial institutions to resolve complaints of end-users.	Maintain strict avoidance of interaction with the production server of the partner participant.	Apply the Consumer Protection Framework to open banking disputes with end-users.
5.	Evaluate the vulnerability of its systems and environment and manage all fraud and related risks.	Collaborate effectively with the Provider to investigate any breach or fraud.			Facilitate the development of common banking industry API Standards within 12 months of the issuance of this Framework.
6.	Maintain logs on adoption, specify risk metrics and thresholds and notify the partner participant of intention to terminate relationship within 48hours of breaching the risk thresholds.	Comply with data privacy laws and all consumer protection regulations.			Maintain of the open banking registry.
7.	Notify the CBN of any terminated relationships with partner participants within three (3) business days to update information in the open banking	Take all reasonable steps to ensure that the end user/customer understands the implication and risk of			

	registry where necessary.	his/her data to be shared.			
8.	Maintain customer service/complaint desk on 24 hours/7 days a week basis and comply with all data privacy laws and regulations.				

Risk Management and Compliance

Under the Framework, all participants will be responsible for risk management and are required to:

(a) have information technology, information security policies and a risk management framework that address APIs;

(b) designate a chief risk officer who will be responsible for implementing effective internal control and risk management practices;

(c) maintain updated API Risk catalogues, API process control mapping and risk control matrix;

(d) agree with partners on risk management processes and metrics and deploy appropriate technology to monitor and report on the metrics to partners;

(e) avail the CBN with risk assessment report on partner participants and provide the CBN with reports on the assessments of its control environment;

(f) collaborate with partner participants on cyber risks and frauds and promptly implement remedial measures to prevent, detect and manage cyberattacks and frauds; and

(g) collaborate with partner participants to ensure compliance with data privacy laws and regulation.

Customer Rights, Responsibility and Redress Mechanism

Participants under the Framework are required to adhere to the provisions of the CBN Consumer Protection Framework in their dealings with customers. The following consumer protection provision will apply specifically to open banking:

(a) the agreements presented to the customer by the participant are to be simple, explicit and in the customer's preferred language and form including written, electronic, video or audio;

(b) customer's consent is to be obtained in the same form the agreement was presented and a copy of the consent will be made available to the customer and preserved by the participant;

(c) the specific rights which the customer will be granting to the participant and the implication of granting those rights to the participant would be listed for the customer to consent to separately for each right to be given to the participant;

(d) the consent of the customer is to be re-validated annually and where the customer had not used the service of the partner for one-hundred and eighty (180) days;

(e) the participant would avail the customer with security updates regularly in his/her preferred form and language to help him or her conduct transactions safely;

(f) the customer would be required to adhere to procedures for authenticating transactions and ensure that login and authentication details are not compromised through negligence; and

(g) participant and its partner would be jointly responsible and bear liability for any loss to the customer, except where the participant can prove wilful negligence or fraudulent act against the customer.

Data Privacy Issues

Data privacy in Nigeria is governed primarily by the Nigeria Data Protection Regulations, 2019 (the "**NDPR**") and the NDPR Implementation Framework. The NDPR has tightened up the controls that customers have in respect of access to and use of their personal data by third parties and includes financial implications on companies and organisations that do not adhere to the data privacy regulations. In line with the NDPR, the Framework provides that before any participant in the open banking system (i.e., banks and other financial service providers, which are data controllers and processors) can share the personal data of a customer, the consent of the customer must have been sought and obtained and the implication of granting such consent must have been communicated to the customer by the bank. Where the customer suffers any loss, the participant and its partner will be jointly liable except where the participant can prove wilful negligence or fraudulent act by the customer. Due to the fact that the NDPR puts the onus of data protection on both data controllers and data processors (i.e., the participants), it is in their interest to ensure that their data protection practices, and technology are of the highest quality.

Conclusion

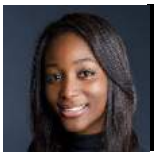
The opportunities presented by open banking are enormous and so are the risks. While open banking is likely to enhance financial inclusion, enable innovative and customer-centric financial products and services and promote competition in banking and other financial services, it is also fraught with data privacy and fraud risks. The CBN must therefore not only ensure that the data, technical and information security standards stipulated in the

Framework are complied with but also closely monitor how the permissioned data is used to avoid abuse. Given that participants and their partners will be jointly liable for any loss to the customer except where negligence or fraud can be proved against the customer, the relevant participant must ensure that the consent of the end user is obtained and secure the exchange of customer data and information through APIs.

Contact Details

Oludare Senbore
Partner

M + 234 803 403 5127
E Oludare.Senbore@aluko-oyebode.com



Ina Arome
Senior Associate

M + 234 810 216 4162
E Ina.Arome@aluko-oyebode.com

Oluwaseun Ayansola
Associate

M + 234 906 281 8466
E Oluwaseun.Ayansola@aluko-oyebode.com