REGULATORY FRAMEWORK

FOR

OPEN BANKING IN NIGERIA

CENTRAL BANK OF NIGERIA

FEBRUARY 2021

Contents

1.0 Introduction

The Central Bank of Nigeria, in furtherance of its mandate for the stability of the financial system and pursuant to its role in deepening the financial system, developed the regulatory framework on open banking in Nigeria. Having observed the growing integration of banks and other financial institutions with innovators in the financial services space and the increasing adoption of Application Programming Interface (API) based integrations in the industry, it has become expedient for the Bank to provide appropriate framework to regulate the practice.

The opportunities presented by Open Banking for enhancing financial inclusion, improving competition in the financial services space and promoting efficient services are compelling cases for the implementation of Open Banking in Nigeria. The Bank is committed to adopting beneficial international standard practice in the Nigerian Banking Industry with due cognisance given to risk management and applicability in the Nigerian environment.

Therefore, the Bank hereby issues the Regulatory Framework for Open Banking in Nigeria to foster the sharing and leveraging of customer-permissioned data by banks with third party firms to build solutions and services that provide efficiency, greater financial transparency and options for account holders and to enhance access to financial services in Nigeria.

2.0 Objectives

The objectives of this framework are as follows:

i. To provide an enabling regulatory environment for provision of innovative and customer-centric financial services through the safe utilisation and exchange data and services;

ii. To define risk based data access levels and service categorisations towards effective management of risk in the operation of open API;

iii. To outline baseline requirements and standards for the exchange of data and services among participants in the financial services sector;

iv. To provide risk management guidance for operators in the financial services space for leveraging data and APIs in the provision of financial services;

v. To promote competition in banking and other financial services and enhance access to financial services.

3.0 Scope

The framework is specifically for banking and other related financial services as follows:

i. Payments and remittance services
ii. Collection and Disbursement services
iii. Deposit-taking
iv. Credit
v. Personal finance advisory and management
vi. Treasury Management
vii. Credit ratings/scoring
viii. Mortgage
ix. Leasing/Hire purchase
x. Other services as may be determined by the Bank

4.0 Data and Service Categories

The framework provides for data that may be exchanged and corresponding API services that may be implemented by and used by participants.

4.1 Categories

Open exchange of data and services through APIs shall be according to the following data and services categories:

i. **Product Information and Service Touchpoints (PIST)**: This shall include 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.

ii. **Market Insight Transactions (MIT)**: This shall include statistical data aggregated on basis of products, service, segments, etc. It shall not be associated to any individual customer or account. These data could be exchanged at an organisational level or at an industry level.

iii. **Personal Information and Financial Transaction (PIFT)**: This shall include data at individual customer level either on 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)

iv. **Profile, Analytics and Scoring Transaction (PAST)**: This shall include information on a customer which analyses, scores or give an opinion on a customer e.g. credit score, income ratings etc.

4.2 Data and Service Risk Rating

S/N	Category	Risk Rating
1.	Product Information and Service Touchpoints (PIST)	Low
2.	Market Insight Transactions (MIT)	Moderate
3.	Personal Information and Financial Transaction (PIFT)	High
4.	Profile, Analytics and Scoring Transaction (PAST)	High & Sensitive

5.0 Data and Service Access Governance

5.1 Risk Management (RM) Maturity Level and Data & Services Access Level

Data and API access requirements among participants shall be guided by the following risk management maturity levels of participants:

S/N	Participants Category	RM Maturity Level (Tier 0 – 3)	Access Level by Data and Service Category
1.	Participants without regulatory licence	Tier 0	PIST and MIT
2.	Participants through CBN Regulatory Sandbox	Tier 1	PIST, MIT and PIFT
3.	Licenced Payments Service Providers and OFIs	Tier 2	PIST, MIT, PIFT and PAST
4.	Deposit Money Banks	Tier 3	PIST, MIT, PIFT and PAST

5.2 Data and API Access Requirements

5.2.1 Tier 0 Requirements

i. The on-boarding requirements for Tier 0 Participants shall be determined by respective sponsoring Tier 2 or Tier 3 participants;

ii. Upon on-boarding the Tier 0 Participant, the sponsoring Tier 2 or Tier 3 participants, within 3 working days of on-boarding the Tier 0 participant shall register the Tier 0 participant on the Open Banking Registry to be maintained by the Central Bank of Nigeria;

iii. The sponsoring Tier 2 or Tier 3 participants shall seek the registration of the Tier 0 participants on the Open Banking Registry with a comprehensive risk assessment report, duly signed by the Chief Risk Officer of the sponsoring participant, carried out on the Tier 0 participant.

5.2.2 Tier 1 Requirements

i. The admission into the CBN regulatory sandbox cohort shall be the primary requirement for Tier 1 Participants;

ii. The Central Bank of Nigeria may, as deemed fit and on a case by case basis, stipulate further requirements;

iii. Tier 1 participant shall be listed on the Open Banking Registry.

5.2.3 Tier 2 Requirements

i. The Tier 2 Participant shall hold a valid Licence from the Central Bank of Nigeria;

ii. Satisfactory Risk Assessment Report by at least two (2) partner participants. The report should address, the Know Your Partner (KYP) assessment in respect of business & governance, financial strength analysis, control environment assessment and risk management practices. The two partner participants issuing the Risk Assessment Report shall include both Tier 2 and Tier 3 participants;

iii. Tier 2 participant shall be listed on the Open Banking Registry

5.2.4 Tier 3 Requirements

i. The Tier 3 Participant shall hold a valid Licence from the Central Bank of Nigeria;

ii. Satisfactory Risk Assessment Report by at least two (2) partner participants. The report should address, the Know Your Partner (KYP) assessment in respect of business & governance, financial strength analysis, control environment assessment and risk management practices. The two partner participants issuing the Risk Assessment Report shall include both Tier 2 and Tier 3 participants;

iii. Tier 3 participant shall be listed on the Open Banking Registry

6.0 Guiding Principles for API Specifications

The Central Bank of Nigeria shall regulate the development of a common Banking Industry API standard with technical design standard, data standard, information security standard and operational rules.

The development of a common API standard by the industry and/or by participants shall adhere to the following principles:

i. Openness: accessible to all interested and permissioned parties
ii. Reusability: premised on existing standards and taxonomy of technology
iii. Interoperability: supports exchange of objects across technologies, platforms, and organisations
iv. Modularity: loose coupling with provision for flexible integration
v. Robustness: scalable, improvable, evolvable and transparent
vi. User-Centric: enhances user experience for consumers
vii. Security: ensures data privacy and safe exchanges and transactions

6.1 Guidance on Technical Design Specifications

The development of technical design specifications shall take the following into cognisance:

i. API Design model shall consider the Data and Service Risk Rating in the choice of the appropriate model;

ii. More secure API design model shall apply to PIFT and PAST service categories;

iii. API Design Model shall make adequate provision for proper versioning and change management.

Appendix 1 provides a list of standards that may be adopted in the technical design specification.

6.2 Guidance on Data Specifications

i. Appropriateness of data standard shall be benchmarked on industry wide acceptability, international acceptance, adequate documentation and customisability;

ii. Data standard specifications shall take cognisance of data and service category specified in this framework for appropriateness or fitness of use;

Appendix 1 provides a list of existing standards that may be adopted in the data specifications.

6.3 Guidance on Information Security Specifications

i. Security specification for APIs shall address, authentication, authorisation, encryption, secure hosting and data integrity;

ii. Strong authentication, authorisation, encryption, secure hosting and data integrity shall be required for PIFT and PAST service categories;

iii. Privacy regulation shall be fully complied with in the design of security architecture.

Appendix 1 provides a list of existing information security standards that may be adopted in the information security specification.

6.4 Guidance on Operational Rules

i. Operational rules shall ensure open access rules and its consistent application to all based on RM Maturity levels defined;

ii. Data Access Agreement and Service Level Agreement among participants shall be mandatory;

iii. Dispute resolution protocols among participants shall be codified for basic operational issues;

iv. Operational rules shall discourage dominant party and anti-competition practices.

7.0 Roles and Responsibilities of Participants

7.1 Participants' Roles

Participants may assume the following roles:

i. **Provider:** A provider is a participant that uses API to avail data or service to another participant;

ii. **Consumer:** A consumer is a participant that uses API released by the providers to access data or service;

iii. **Fintechs:** Companies that provide innovative financial solutions, products and services;

iv. **Developer Community:** individuals and entities that develop APIs for participants based on requirements.

7.2 Participants' Responsibilities

The following are role-based responsibilities for participants:

7.2.1 Responsibilities of Providers

The Providers shall:

i. Publish the APIs and define requirements and technical guidelines. It is recommended that the provider shall leverage the common Banking Industry API Standard;

ii. Define the data and services accessible through the APIs;

iii. Comply with the provisions of this framework;

iv. Establish Data Access Agreement and Service Level Agreements with other participants;

v. Carry out Know Your Partner (KYP) due diligence on partner participants which shall include a comprehensive risk assessment on the partner participant duly singed off by the Chief Risk Officer before executing agreements specified in (iv) above;

vi. Share responsibility with the partner participant for any loss to the end-user which did not arise from the wilful negligence or fraudulent act of the end-user;

vii. Ensure that the partner participant that owns the customer interface obtains consent of the end-user based on agreed protocols;

viii. Certify that the partner participants define to the end-user in explicit terms the implication of granting consents to it and give the end-user the option to choose access rights to data granted the partner participant;

ix. Carry out regular monitoring of the control environment of the partner participants and revalidates the agreements in (iv) on an annual basis;

x. Without prejudice to (ix) subscribe to a common industry initiative for regular monitoring and validation of participants;

xi. Deploy and implement automated monitoring system for evaluation of the vulnerability of its systems and environment to partner participant and for the management of fraud or related risks;

xii. Maintain logs on adoption and usage and other metrics on performance of APIs;

xiii. Specify risk metrics and thresholds, the breach of which could lead to a review of the relationship with partner participants;

xiv. Notify the partner participant of intention to terminate relationship within 48hours of breaching the risk thresholds;

xv. Notify the Bank of any terminated relationships with partner participants within 3 business days to update information in the Open Banking Registry where necessary;

xvi. Comply with data privacy laws and regulations;

xvii. Maintain customer service/complaint desk on 24 hours/7 days a week basis for financial institutions to resolve complaints of end-users.

7.2.2 Responsibilities of API Users

API Users shall:

i. Execute a Data Access Agreement and Service Level Agreement with Provider;

ii. Adhere to the requirements and guidelines set by the Provider;

iii. Specify to the end-user the implications of the consent to be given and the actions that may be performed on the account of the end-user;

iv. Obtain consent of the end-user on each action that may be performed on the account of the end user as specified by the provider;

v. Cooperate with the Provider for the regular monitoring of its control environment;

vi. Ensure an annual re-validation of the Data Access Agreement and Service Level Agreement;

vii. Implement any remedial actions as may be indicated by the Provider based on vulnerabilities discovered through the monitoring of its control environment;

viii. Collaborate effectively with the Provider to investigate any breach or fraud;

ix. Comply with data privacy laws and all consumer protection regulations;

x. Maintain customer service/complaint desk on 24 hours/7 days a week basis for financial institutions to resolve complaints of end-users;

xi. Take all reasonable steps to ensure that the end user/customer understands the implication and risk of his/her data to be shared;

xii. Comply with the provisions of this framework;

7.2.3 Responsibilities of Fintechs

Fintechs are usually consumers of APIs, however this framework recognises that there could be occasions for Fintechs to be Providers of API. Fintechs shall therefore assume the responsibilities of either consumer or provider depending on the role they play at any point in time.

In addition, Fintechs shall:

i. Ensure that it leverages API to innovate products and solutions that are interoperable;

ii. Avoid alteration of APIs published by provider without consent of the providers;

iii. Any Modification of published APIs shall be based on the provisions of Data Access Agreement or where necessary an addendum to the agreement. The agreement shall specify rights of the parties to the modified API and commercial terms;

iv. Comply with data privacy laws and regulations;

v. Adhere to the provisions of this framework;

vi. Maintain customer service/complaint desk on 24 hours/7 days a week basis for financial institutions to resolve complaints of end-users.

7.2.4 Responsibilities of Developer Community

The Developer community are persons or entities that may provide programming services for other participants. They shall:

i. Comply with the provisions of this framework;

ii. Execute service agreements with the partner participant outlining the participant's business requirement and technical guidelines;

iii. Employ secure coding and development standards and practices;

iv. Maintain strict avoidance of interaction with the production server of the partner participant;

8.0 Responsibilities of the Central Bank of Nigeria

The Central Bank of Nigeria shall be responsible for the following:

i. Issuance of the Regulatory Framework for Open Banking in Nigeria and its review as it may deem necessary;

ii. Oversight of the implementation and operations of Open Banking in Nigeria;

iii. Enforcement of this framework;

iv. Arbitration of disputes among participants before any litigation or commencement of Judicial process;

v. Application of the Consumer Protection Framework to Open Banking Disputes with end-users;

vi. Facilitation of the following enablers:

   a. Development of Common Banking Industry API Standards within 12 months of the issuance of this framework;

   b. Maintenance of Open Banking Registry.

9.0 Risk Management

Risk Management under the Open Banking Framework shall be the responsibility of all participants. Therefore, participants shall:

i. Have information technology, information security policies and a risk management framework that address APIs;

ii. Designate a Chief Risk Officer who shall be responsible for implementing effective internal control and risk management practices;

iii. Maintain updated API Risk catalogues;

iv. Maintain API Process Control Mapping and Risk Control Matrix;

v. Align incident management processes and procedures with partner institutions clearly outlining responsibilities of each party;

vi. Agree risk management metrics and measurement procedures for APIs operations and deploy appropriate technology to monitor and report on the metrics to partners;

vii. Submit to risk assessment by partner participants as provided in the agreements;

viii. Avail the Bank with risk assessment report on partner participants and provide the Bank with reports on the assessments of its control environment;

ix. Collaborate with partner participants to ensure compliance with data privacy laws and regulation;

x. Maintain updated data footprint mapping in conjunction with partner participants;

xi. Implement fraud monitoring systems and promptly exchange fraud intelligence with partner participants;

xii. Collaborate with partner participants on cyber risks;

xiii. Promptly implement remedial measures to prevent, detect and manage cyberattacks and frauds.

10.0 Customer Rights, Responsibility and Redress Mechanism

The customer is critical to the successful implementation of open banking. Therefore, the protection of the customer shall be the responsibility of all

participants. Participants are therefore required to adhere to the provisions of the Consumer Protection Framework of the Bank in their dealings with customers. Additionally, the following shall apply in the operation of the open banking:

i. The agreements presented to the customer by the participant shall be simple, explicit and in the customer's preferred language;

ii. The agreement shall be presented to the customer's preferred form including written, electronic, video or audio;

iii. Customer's consent shall be obtained in the same form the agreement was presented and a copy of the consent of the customer shall be made available to the customer and preserved by the participant;

iv. The specific rights which the customer will be granting to the participant and the implication of granting those rights to the participant shall be listed for the customer to consent to separately for each right to be given to the participant;

v. The consent of the customer shall be re-validated annually and where the customer had not used the service of the partner for 180 days;

vi. The responsibility of the customer for his/her protection shall be clearly communicated to the customer at the on-boarding stage;

vii. The participant shall avail the customer with security updates regularly in his/her preferred form and language to help him or her conduct transactions safely;

viii. The customer shall adhere to procedures for authenticating transactions and ensure that login and authentication details are not compromised through negligence;

ix. The customer shall comply with preventive protocols and security advise provided by the participant and report any observed discrepancy in his/her accounts or assets;

x. Participant and its partner shall 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;

APPENDIX 1

1. API DESIGN MODEL STANDARDS

- Representational State Transfer (REST)
- Simple Object Access Protocol (SOAP)

2. DATA STANDARDS

- Open Financial Exchange (OFX)
- eXtensible Business Reporting Language (XBRL)
- ISO 9735- Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT)
- Financial product Markup Language (FpML)
- Financial Information Exchange (FIX)
- Market Data Definition Language (MDDL)
- Security Assertion Markup Language (SAML) 2.0
- ISO 20022
- Statistical Data and MetaData eXchange (SDMX)

3. INFORMATION SECURITY STANDARDS

- **Authentication:**
  - OAuth 2.0
  - OpenID Connect
  - FAPI
  - Security Assertion Markup Language (SAML) 2.0

- **Authorisation**
  - OAuth 2.0
  - ISO 10181-3 – Access Control Framework
  - FAPI
- **Encryption**
  - Transport Layer Security (TLS) v 1.2
  - RSA Public/Private Key

    - AES
    - Secure File Transfer Protocol (SFTP)
- **Data Integrity**
    - JSON Web Token (JWT)
    - WS-Security
    - Keyed Hash Message Authentication Code (HMAC)
- **Secure Hosting**
    - ISO 27001
    - ISO 22301
    - PCI DSS