



OVERVIEW OF CBN'S DRAFT REGULATIONS ON OPEN BANKING

The Central Bank of Nigeria (“**CBN**”) recently released a draft regulatory framework for open banking in Nigeria. If issued, the “Regulatory Framework for Open Banking in Nigeria” (the “**Framework**”) will set out rules under which the sharing of financial data can occur. The CBN believes open banking will increase financial inclusion and stabilise Nigeria's financial infrastructure ecosystem, and from a market perspective this is a welcome step in the right direction.

In this newsletter, we outline the highlights of the Framework and how this improves the way we bank in Nigeria.

WHAT IS OPEN BANKING?

Open Banking is generally understood as the practice of sharing financial data with the consent of customers for use by third party providers in order to tailor services and applications. This gives financial institutions the opportunity to increase their revenue streams by cross-selling their products, whilst also providing smaller companies with the opportunity to reach a larger customer base by partnering with larger banks to sell their products. For customers, open banking could provide them a wide range of benefits previously not available to them such as; the ability to obtain a credit score based on a wholistic view of all bank accounts and financial services such as treasury management and financial advisory.

The sharing of data is enabled by the use of open APIs (application programming interfaces). APIs allow for the transmission of data by allowing vendors with different technology platforms to interact with one another.

With the growing use of fintech applications for the provision of financial services such as trading, saving, and investments; the use of open banking allows banks and other financial institutions to maximise their resources. The CBN states that the draft Framework is intended to regulate the use of APIs and promote competition.

Already widely used in the UK, the EU and the US, open banking allows third parties to use shared financial data to provide a plethora of new options to the customer such as personalised services based on customer usage, centralised account management services and other financial management services including enhanced personal advice based on the customer's trends thereby improving the general customer experience.

For example, in the UK and the US, several banks (both traditional and digital) have entered into strategic partnerships with accounting and insurance software providers such as Xero and FreeAgent to provide

Key Contacts



ZELDA AKINDELE
Partner

zelda.akindele@templars-law.com



BENITA OGBODO
Associate

benita.ogbodo@templars-law.com

seamless and integrated accounting and insurance services for their business banking customers. As a result, customers no longer need to hire separate accountants and insurance brokers to provide personalised advice.

The CBN's Framework is specifically aimed at banking and other financial institutions providing services such as payments and remittances, collection and deposit taking, treasury management, mortgage provision and other services as determined by the CBN.

DATA CATEGORIES AND ACCESS LEVELS

The Framework sets out 4 categories of data that can be exchanged using APIs and has attributed a risk rating to each category:

- 1) Product Information and Service Touchpoints (“**PIST**”) – **low risk**. This includes information provided by participants to customers and information on access points available for customers to access service for example ATM locations, website addresses, charges and rates etc.
- 2) Market Insight Transactions (“**MIT**”) – **moderate risk**. This is statistical information on products, services and segments. MIT data is not associated with an individual customer and is shared on an aggregate basis.
- 3) Personal Information and Financial Transaction (“**PIFT**”) – **high risk**. This is individual customer data providing general information on the customer including personal data such as total number of accounts and transaction data such as account balances, direct debits, recurring transactions and other bill payments.
- 4) Profile, Analytics and Scoring Transaction (“**PAST**”) – **high and sensitive risk**. This is personalised scoring customer data such as income ratings and credit scores.

The Framework goes further to set out the access levels of open banking participants. The access levels are set out as follows:

- 1) **Tier 0** – applicable to open banking participants operating without a license. Tier 0 participants can only access PIST and MIT data.
- 2) **Tier 1** – applicable to open banking participants operating through CBN's regulatory sandbox. Tier 1 participants can access PIST, MIT and PIFT data.
- 3) **Tier 2** – applicable to licensed payment service providers and other financial institutions. Tier 2 participants can access all categories of data.
- 4) **Tier 3** – applicable to deposit money banks. Tier 3 participants can access all categories of data.

ACCESS REQUIREMENTS

Tier 0 Requirements

Tier 0 participants can only operate when sponsored by a Tier 2 or Tier 3 participant. On-boarding of a Tier 0 participant requires the completion of a comprehensive risk assessment report signed by the Chief Risk Officer of the sponsoring participant on the registration of the Tier 0 participant on the Open Banking Registry within 3 working days.

Tier 1 Requirements

As noted, Tier 1 participants are participants already admitted into CBN's regulatory sandbox, and as such, no additional requirements are necessary other than listing on the Open Banking Registry.

Tier 2 and 3 Requirements

Tier 2 and 3 participants are required to hold a valid license from the CBN, provide a satisfactory risk assessment report by at least 2 partner participants (from Tier 2 and 3 each) and list on the Open Banking Registry.

KEY PARTICIPANTS

Under the Framework Key Participants are split into 4 categories which describe the roles and responsibilities of each Participant in relation to Open Banking:

- 1) **Providers** – participants that use API to provide data or services to another participant. Providers shall (amongst other responsibilities set out in the Framework), establish data access agreements and service level agreements, certify that partner participants ensure the customer understands the implication of granting consent to the storage of its data, maintain logs on the adoption and usage of APIs and maintain a 24/7 customer service to resolve complaints.
- 2) **Consumers** (i.e. the API users) – participants that use API released by the providers to access the data or service.
Consumers are required to execute data access agreements and service level agreements, highlight to the customer the implications of granting consent to the storage of its data and comply with data privacy laws and consumer protection regulations in place.
- 3) **Fintechs** – typically, they are consumers of API, but the Framework recognizes that Fintechs are also Providers. Fintech companies shall leverage API to innovate interoperable products and solutions that are interoperable.
- 4) **Developer Communities** – individuals and entities that develop APIs for participants based on their requirements. Developer Communities are to ensure secure coding and development standards are employed.

GUIDING PRINCIPLES AND TECHNICAL SPECIFICATIONS FOR APIs

Whilst the Framework provides a list of existing standards that may be adopted, the CBN has also been tasked with the development of a common Banking Industry API standard within 12 months of issuing the Framework. The common Banking Industry API standards will outline specifications for technical design, data and information security standards taking into account principles such as the openness, reusability, interoperability and security of data.

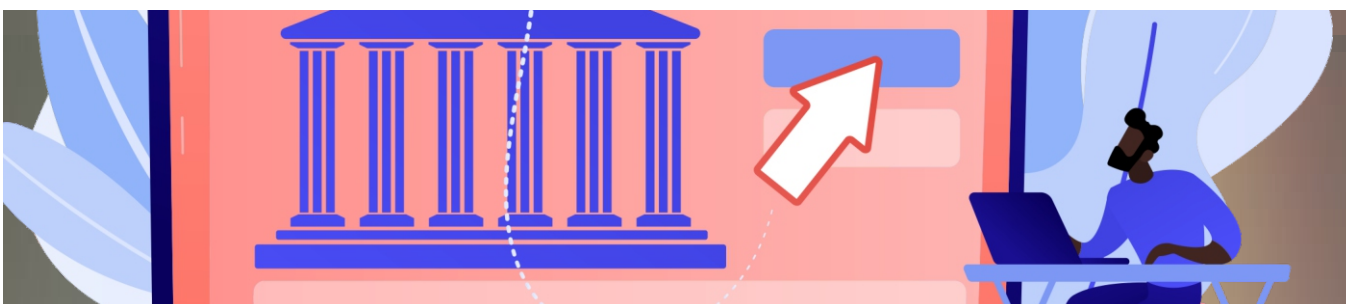
OTHER KEY PROVISIONS

Customer Rights

The Framework sets out several guidelines for the protection of the customer whilst using open banking. Most notably, participants are required to ensure that the protection of the customer is paramount to their services and adhere to the provisions of the CBN Consumer Protection Framework.

Additionally, agreements presented to the customers should be in the customer's preferred language and consent shall be given in the same of as the agreement and re-validated annually (or where the service has not been used for 180 days).

Finally, participants (and their partners) are jointly responsible and required to bear the liability of any loss to the customer (unless such loss was as a result of the wilful negligence or fraud against the customer).



CONCLUSION

Open banking has been encouraged in jurisdictions such as the UK and the EU and, with the increased capacity for data sharing, open banking gives financial institutions the opportunity to generate additional income whilst allowing smaller companies to reach a larger target market. For open banking to truly be successful in Nigeria however, it requires third party providers to operate using standardised operating systems. For example, the success of services such as the ATM, interbank transfers and the use of POS machines can largely be attributed to the achievement of a common standard for banks and financial institutions to ensure acceptance at all terminals. Whilst the Framework has outlined standards with respect to API, data and information security, it is vital that the CBN ensures that banks and other financial institutions work together to ensure that these standards are met.

In addition to concerns around standardised systems, there are other considerations to implementing open banking in Nigeria. For example, the Framework does not go into detail on how participants will be sanctioned following breaches such as unauthorised access or inadequate protection or storage of data. Whilst the CBN has provided risk categories for the different types of data, it has not stated whether different sanctions will be applicable for infractions at the different category levels. In today's data-centric world, customers are more protective of their data privacy and breaches would have serious implications for both the companies and the customer. Secondly, given that the use of open banking involves the analysis and transfer of the personal data of individuals, Providers and Consumers would fall within the scope of the Nigerian Data Protection Regulation (the “**NITDA Regulations**”), but this has not been noted in the Framework despite data privacy requirements being an essential element of any regulatory framework on open banking. Furthermore, under the NITDA Regulations, additional restrictions and measures are put in place for the foreign transfer of personal data (such as under the supervision of the Attorney General of the Federation, with the informed consent of the Customer or pursuant to one of the prescribed exceptions in the NITDA Regulations) which may have an effect on interactions Providers and Consumers have with partners (particularly technical partners) based in other jurisdictions. It is therefore important for the CBN to ensure that whilst engaging with financial institutions and fintech solution providers, it also engages key stakeholders in the industry to ensure that the monitoring of compliance with the Framework also addresses concerns around data privacy and data breaches. Nevertheless, the highly anticipated Framework addresses the key aspects of open banking and aims to take advantage of the opportunities open banking can provide whilst addressing the minimum standards required to spearhead the initiative.

