G. ELIAS

Open Banking in Nigeria: Regulatory Environment and Pertinent Data Protection Concerns

www.gelias.com

Open Banking in Nigeria: Regulatory Environment and Pertinent Data Protection Concerns

Introduction

In February 2021, the Central Bank of Nigeria ("**CBN**"), acting pursuant to its statutory mandate as the regulator of Nigerian banking, had issued the Regulatory Framework for Open Banking in Nigeria (the "**Framework**"). The CBN further consolidated its regulation of the open banking space by issuing the Operational Guidelines for Open Banking in Nigeria (the "**Guidelines**") in May 2022.

The issuance of the Framework by the CBN was the culmination of a long and dogged effort by FinTechs, and other players in the financial services space, who consistently lobbied the CBN for an innovative regulatory framework setting the ground rules for open banking operations in Nigeria. The Framework has now been further complemented by the Guidelines, which bring about greater specificity and clarity in the regulatory matters contemplated in the Framework.

The demand by industry stakeholders for regulatory guidance on open banking in Nigeria followed the trend in other jurisdictions where there was either already existing a full-blown open banking system in place or the clamour for open banking was picking up steam. With the introduction of the Framework (and more recently, the Guidelines), Nigeria has become the pioneer jurisdiction on open banking in Africa.

The Framework aims to "outline baseline requirements and standards for the exchange of data and services among participants in the financial services sector."[1] Open banking's top attraction is that it results in troves of consumers' financial data being shared by banks, FinTechs, financial institutions and other entities. As a result, open banking has implications for the treatment of the financial information of consumers.

This article explores pertinent provisions of the regulatory guidance on open banking in Nigeria (namely the Framework and Guidelines) and the impact of the Nigeria Data Protection Regulation, 2019 ("**NDPR**") provisions as they relate to the protection of personal data in the Nigerian open banking environment. This article also addresses some of the concerns that attend to the remarkable regime of open banking operations in Nigeria.

Open Banking – What Is It?

Outside of the enclosed spaces of financial technology and retail banking, "open banking" is anything but an everyday term. In this regard, a brief attempt at an explanation of the term is in order.

Open banking is a system which permits and enables the sharing of financial information of customers by a bank or other financial institutions with Third Party Players ("**TPPs**") through an electronic medium. The technical infrastructure that facilitates open banking is application programming interfaces ("**APIs**"). In simple terms, an API is a software

[1] Framework, s. 2.0.

intermediary that enables two or more different applications to communicate with each other.

Under open banking, banks share their customers' transactional data through their APIs with TPPs (FinTechs and other eligible players) to enable the TPPs develop new and innovative financial products and services, with the aim of enhancing customer satisfaction and promoting financial inclusion.

In a nutshell, what open banking entails is that banks and other financial services providers make available to each other and TPPs, using APIs, the financial data of customers in their custody. These include data acquired by banks in the course of complying with extant Know Your Customer ("**KYC**") requirements during account-opening exercises or during the period of the customer-banker relationship between the customer and the bank. Such financial data may be further analyzed or algorithmicized to reveal intricate financial details of a customer, such as a customer's withdrawal patterns, account inflow sources and spending patterns.

With precious financial data like these being exchanged in the financial industry, it becomes easier for players in that scene, individually or collaboratively, to mine the shared financial data with a view to developing bespoke financial products and services tailored for the needs – or the appetites – of identified customers.

A Glance at the Framework and Guidelines

Both the Framework and Guidelines were issued by the CBN in order to foster the sharing and leveraging of financial data by banks with TPPs and build solutions and services that provide efficiency, greater financial transparency and options for account holders. They are aimed at generally enhancing access to financial services in Nigeria under a regulated regime.[2]

The financial services covered by the Framework are deposit-taking, remittances services and allied banking products.[3] The CBN may add, from time to time, other services to the above list.

The Framework notably creates categories of customer data which can be shared under the open banking system (and apportion risk levels to these categories), with access being given to TPPs to these categories of data depending on their respective risk profiles. These categories of data are (i) Product Information and Service Touchpoints ("**PIST**"), whose risk rating is low; (ii) Market Insight Transactions ("**MIT**"), whose risk rating is moderate; (iii) Personal Information and Financial Transactions ("**PIFT**"), whose risk rating is high; and (iv) Profile, Analytics and Scoring Transactions ("**PAST**"), whose risk rating is high and sensitive.[4] The Guidelines retain the above-mentioned categorization for the purpose of onboarding players into the open banking ecosystem.[5]

[2] Framework, s. 1; Guidelines, s. 3.0.
[3] Framework, s. 3.
[4] Framework, s. 4.2.
[5] Guidelines, s. 6.1.

PIST is in respect of information on products provided by banks and other financial institutions to customers, such as ATM locations, service codes, loan tenors, bank charges and the likes.[6] All players in the open banking space, including those without CBN licences, can access PIST, due to its low-risk rating.[7]

MIT includes statistical data siloed on the basis of products, services and similar considerations but not associated to any individual customer or account.[8] With a moderate risk rating, all players in the open banking space, including those without CBN licences, can also access MIT.[9]

PIFT includes data at the individual customer level either on general information gleaned by a bank through KYC or related processes or data acquired by the bank during the pendency of the customer-banker relationship.[10] Due to its high risk rating, unlike PIST and MIT, not all participants in the open banking space can access PIFT; in particular, only participants through the CBN regulatory sandbox,[11] licensed payments service providers ("**PSPs**"), other financial institutions ("**OFIs**"), and deposit money banks ("**DMBs**") can access PIFT.[12]

Last but not the least, there is PAST, which essentially includes information on a customer which analyzes, scores or opines on a customer.[13] A classic example is a customer's credit score. PAST's risk rating is understandably high and sensitive.[14] As a result, it can only be accessed by PSPs, OFIs and DMBs.[15]

The Framework further stipulates principles guiding API specifications, standards for data specifications, guidance on information security specifications, and guidance on operational rules.[16] It also outlines the responsibilities of various stakeholders, the rights of customers and a framework for redress in the event of the breach of a customer's rights.[17] Complimenting the Framework are the Guidelines, which provide for the creation of an open banking registry (which is a public repository of details of the open banking participants) within the CBN,[18] specify minimum standards for the storage of the open banking system configurations items,[19] mandate documented commercial arrangements between API providers and consumers to contractually regulate transacted data,[20] set out performance monitoring mechanisms in relation to an API

[6] Framework, s. 4.1.
[7] Framework, s. 5.1.
[8] Framework, s. 4.1.
[9] Framework, s. 5.1.
[10] Framework, s. 4.1.
[11] A "sandbox," as used in this technical context, is a formal process for FinTechs to conduct live tests of new, innovative products, services, delivery channels, or business models in a controlled environment, with regulatory oversight, subject to appropriate conditions and safeguards.
[12] Framework, s. 5.1.
[13] Framework, s. 4.1.
[14] Framework, s. 4.1.
[15] Framework, s. 5.1.
[16] Framework, s. 6.
[17] Framework, ss. 7, 8 and 10.
[18] Guidelines, s. 6.0.
[19] Guidelines, s. 8.1.
[20] Guidelines, s. 8.1.2.

producer,[21] define data ethics and governing principles,[22] and lay out a regulatory framework for sharing of information between API producers and consumers.[23]

Compliance with the Nigerian Data Protection Regulation 2019

Both the Framework and the Guidelines are emphatic that participants in the open banking system (*i.e.*, banks and TPPs) are expected to comply with the provisions of data privacy and protection laws and regulations. The Nigerian Data Protection Regulation 2019 ("**NDPR**"), which is the primary and most comprehensive legislation on data protection in Nigeria, applies to all transactions intended for the processing of personal data. It applies to the processing of personal data notwithstanding how the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria.[24] Since open banking involves the collection and processing of personal data, its operation and implementation must be done in compliance with the provisions of the NDPR.[25]

Although the Framework has adopted some provisions of the NDPR such as the need to obtain the consent of the customer, the NDPR contain further comprehensive data protection provisions that should be noted and taken into consideration.[26]

One of the major provisions to be complied with is the need to obtain the consent of the owner of the data sought to be obtained and processed. The NDPR imposes an obligation on the data controller[27] to obtain the consent of the customer whose data is to be collected, and such consent must be obtained without fraud, coercion or undue influence.[28] The Framework further provides that the consent must be revalidated annually.[29] The specific purpose for the collection and processing of the data (which must be legitimate and lawful) must also be made known to the customer at the time of obtaining the consent.[30] It is therefore imperative that open banking players obtain the voluntary consent of the customers before sharing their data and inform them of the purpose for the collection and sharing of such data.

In addition to the above, the NDPR grants data subjects the right to object to the processing of their personal data.[31] The data subject is also entitled to access to his personal data with the data controller, the erasure and rectification of such personal

[21] Guidelines, s. 8.2.3.
[22] Guidelines, s. 9.1.
[23] Guidelines, s. 11.
[24] NDPR, reg 1.2,
[25] The provisions of the NDPR should be read together with the NDPR Implementation Framework 2020 for better application.
[26] Framework, s. 10.
[27] Data Controller under the NDPR means a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed. In the open banking space, the data controller refers to the banks and other financial institutions. See NDPR, reg 1.3
[28] NDPR, reg 2.3(2).
[29] Framework, s. 10.0 and Guideline, s. 11.
[30] NDPR, reg 2.1(1) (a), 2.3(1), 3(7).
[31] NDPR, reg 2.8

data and the transfer of his data to a specified TPP where technically feasible.[32] Thus, where a customer has requested that its personal data with a bank be deleted or rectified, the bank is obligated to inform other open banking players to whom the customers data has been shared to do the same unless it is impossible or involves disproportionate effort.

The bank is also obligated to share the customers' data with any specified TPP at the request of the customer. In addition to fulfilling other criteria outlined in the Guidelines, the approval of the CBN must be sought and obtained before a bank or any TPP can share a customer's data to an outsourced service provider.

There is also an obligation to ensure that the TPPs prepare and publish a privacy policy on their sites or other medium of data collection within three months of commencement of business operation. The privacy policy must be simple, conspicuous, and easy to understand.[33]

Open banking participants must also ensure that they develop competent security systems to ensure the protection of data in their possession as well as securing against all foreseeable hazards and breaches to the customers data.[34] As an additional protection of customers' data, the NDPR provides that data processing by a TPP shall be governed by a written contract between the TPP and the data controller. The data controller shall ensure that such TPP adheres to the provisions of the NDPR and does not have a record of violating the provisions of the NDPR.[35] In this case, banks and other financial institutions are to undertake comprehensive due diligence on all parties to whom data will be shared before onboarding them as they will be held liable for the actions of those TPPs to whom they grant access to the personal data of their customers.

In order to improve the chances of compliance with the provisions of the NDPR in relation to the processing of personal data of customers, organizations that process personal data are required to have a data protection officer or outsource their data protection exercise to a Data Protection Compliance Organization ("**DPCO**"), a certified data protection professional. Organizations who process personal data are also required to conduct a detailed annual audit of their privacy and data protection practices and submit the report to the National Information Technology Development Agency ("**NITDA**").[36]

Open banking participants should therefore endeavour to employ a data protection officer or DPCO to enable the reduce the risk of non-compliance with the data protection laws. It is also mandatory to regularly train members of senior management and employees responsible for collecting or processing personal data in the course of their duty on relevant data protection laws and practices[37].

[32] NDPR, reg 3.1(7)(13)(15),
[33] NDPR, reg 2.5, NDPR Implementation Framework, art. 3.2(iii)(iv)
[34] NDPR, reg 2.6, 2.2(1)(d)
[35] NDPR, reg 2.4(b), 2.7
[36] NDPR, reg 4.1. Also see Annexure A of the NDPR Implementation Framework for an Audit template for NDPR Compliance.
[37] NDPR Implementation Framework, art. 3.2(xiv)

TPPs are required to notify the NITDA of personal data breaches within 72 hours of becoming aware of such breach.[38] Failure to comply with the provisions of the NDPR in relation to the data privacy rights of a data subject shall attract civil and/or criminal penalty. For a data controller dealing with more than 10,000 data subjects, the penalty for breach will be the payment of a fine of 2% of the annual gross revenue of the preceding year or the payment of the sum of ₦10 million, whichever is greater. In the case of a data controller dealing with less than ten thousand data subjects, payment of the fine of 1% of the annual gross revenue for the preceding year or payment of the sum of ₦2 million, whichever is greater.[39]

Cause for Concern

The immediate gains and flaws alike of open banking are well-documented.[40] For one, open banking is billed to help bring about the CBN's often-stated goal of financial inclusion. Open banking will also, no doubt, lead to more innovation in the financial industry, as banks and TPPs will by virtue of open banking being able better to mine available financial data further to meet the banking needs of the Nigerian public. The open banking system will also encourage healthy competition in the financial services sector.

The above gains notwithstanding, there are data protection concerns that attend to the open banking regime in Nigeria as umpired by the Framework and Guidelines[41]. For one, both secondary legislations allow access to precious financial data on consumers by entities that are not regulated by the CBN. The Guidelines literally permit fast-moving consumer goods entities and other retailers to access data shared by banks and other financial institutions in the open banking space.[42] Both PIFT and MIT can be accessed by all players in the open banking space, including entities without regulatory licences. This is worrisome, as the CBN's power to sanction such non-regulated entities for undesirable processing of acquired financial data is doubtful.

The CBN opening up data access to entities outside its statutory regulatory purview, therefore, invites concern that the CBN may be powerless to apply appropriate measures should such entities violate extant law in accessing and mining PIFT and MIT. Whilst PIFT and MIT have low and moderate risk ratings respectively, they still encompass data that when maliciously utilized, might put an unwitting consumer in harm's way. There would have been more comfort if the Framework or Guidelines restricted access to all financial data to entities under the CBN's regulatory ambit.

This perceived shortcoming is also prevalent in open banking jurisdictions across the world, with the notable exception of the United Kingdom, where the Payment Services Regulations provide for the sharing of customers information only among authorized

[38] NDPR Implementation Framework, art. 3.2(ix)
[39] NDPR, reg 2.10
[40] Audrey Ottevanger, 'Open Banking: What Do Business Leaders Need to Know?' << https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2021/07/27/open-banking-what-do-business-leaders-need-to-know/?sh=4548babc204e>> Accessed August 18, 2021.
[41] Guidelines, s. 2 of Appendix II.
[42] Guidelines, s. 4.1.

payment institutions within the regulatory control of the Financial Conduct Authority ("**FCA**")[43]. Therefore, TPPs which are not regulated by the FCA are exempted from the open banking playing field.

Furthermore, observers have expressed concern about open banking's possible impact on competition and the structure of the financial sector in the short to medium term.[44] While open banking means that financial data can be shared by and with various entities, there are no corresponding laws, as of today, in other (non-financial) sectors mandating or even enabling the sharing of data held in such other sectors. This could result in non-financial entities leveraging on open banking to access new financial data and having, in the process, unfair advantage over entities in the financial industry.[45]

In addition, under the present gain-driven capitalist culture in which open banking thrives, TPPs may resort to algorithmizing harvested data to carry out predatory lending and/or create financial products that tap into a prodigal customer's financial vices and weaknesses. Other obvious risks as identified by the Guidelines include cybersecurity, data privacy and integrity, money laundering and regulatory and compliance risks.[46]

Policymakers in other jurisdictions are yet to enact clear ground rules in response to these issues. Thus, it remains of poignant concern that open banking potentially (i) gives non-financial entities an unfair advantage over entities in the financial industry and (ii) fosters a consumer culture that preys on customers' financial vices.

Conclusion

Open banking is a well-intentioned concept that has a propensity to bring about banking services to the underbanked and unbanked Nigerian demographic. As a stabilizer of intra-sector rivalry, open banking's role in mitigating unhealthy rivalry among the traditional banks and TPPs is to be applauded.

The present regulatory environment on open banking in Nigeria, however, has certain implications for the consumer, which future regulations of the CBN should address. For one, to ensure comfort to the members of the public whose financial data open banking applies to, access to financial data should be limited to entities regulated by the CBN and who are compliant with CBN's prudential requirements as laid out in extant regulations. Furthermore, CBN should liaise with the regulators of other (non-financial) sectors to also develop parallel open data frameworks on terms not inimical to their respective sectors, in order to allow for fair competition between entities in the financial sector and those outside of it. Finally, by way of consumer protection, the CBN should develop a mechanism by which TPPs and banks do not develop financial products that pander to the human or corporate weaknesses of the customers.

Based on the foregoing, while the CBN's regulation of the open banking space (as demonstrated by the issuance of both the Framework and the Guidelines) is a step in

[43] The regulator of the financial services industry in the UK.
[44] Edward Corcoran, 'Open Banking Regulation around the World' <https://www.bbva.com/en/open-banking-regulation-around-the-world/> Accessed August 18, 2021.
[45] *Ibid.*
[46] Guidelines, s. 2 of Appendix II.

the right direction and is very much in line with developments in other jurisdictions, there is a need for the CBN to take further steps to improve the open banking regulatory environment for the purpose of assuaging the concerns raised in this article.

Ebimobowei Jikenghan
SENIOR ASSOCIATE
ebi.jikenghan@gelias.com

Oluwafunmilayo Mayowa
ASSOCIATE
marian.asuenimhen@gelias.com

Fidelis Oguche
ASSOCIATE
fidelis.oguche@gelias.com

LOCATIONS

LAGOS OFFICE
6 Broad Street
Lagos, Nigeria

T: +234 (1) 460 7890
E: gelias@gelias.com

ABUJA OFFICE
2nd Floor, Abia House,
Plot 979, First Avenue,
Central Business District
F.C.T, Abuja.
T: +234 (1) 888 8881

● Corporate ● Mergers and Acquisitions ● Securities Offerings ● Project and Structured Finance ● Tax ● Litigation and Arbitration ● Privatization ● Intellectual Property ● Employment ● Compliance ● Insurance ● Pensions ●Private Equity ● Oil and Gas ● Electricity ● Food and Healthcare ● Trade and Industry ● Media and Entertainment ● Telecommunications and Technology ● Real Estate and Construction ● Infrastructure ●Transport and Logistics ●

www.gelias.com