 https://doi.org/10.53982/apblj.2019.0301.04-j

REGULATION OF OPEN BANKING IN NIGERIA: BALANCING INNOVATION AND PRIVACY

By

Oghomwen Rita Ohiro*, Keseme Phillip Odudu**

ABSTRACT

Open banking has become a game-changing strategy in the financial sector, aimed at improving innovation, competition, and overall customer experience. This study explores the possibility of introducing technological advancements in banking through open banking systems while ensuring privacy protection. It examines the legal aspects of regulating open banking in Nigeria and emphasizes the importance of achieving a balanced approach that encourages innovation while maintaining rigorous regulatory standards. This paper employs a doctrinal research methodology, combining legal analysis and comparative studies to assess Nigeria's current regulatory landscape and identify any gaps. Drawing on the United Kingdom's regulatory model as a benchmark, the paper evaluates the effectiveness of Nigeria's regulations governing open banking. The findings emphasize the necessity of enhancing the regulatory framework to address the unique challenges posed by open banking in Nigeria. By providing insights and recommendations, this paper seeks to guide policymakers in striking a harmonious balance between innovation and privacy within the Nigerian open banking ecosystem.

Keywords: *Open Banking, Innovation, Privacy, Financial*

1.0 Introduction

The financial sector worldwide has undergone a paradigm shift driven by technological advances and regulatory changes, popularly known as open banking.[1] This financial innovation is a transformative approach that enables third-party financial service providers to access bank data through Application

* Oghomwen Rita Ohiro Lecturer. Department of Public Law, Faculty of Law, University of Benin, Benin City, Nigeria. Email: oghomwen.igbinedion@uniben.edu tel: +2347062368221

** Keseme Phillip Odudu Lecturer, Department of Jurisprudence and International Law, Faculty of Law, University of Benin, Benin City, Nigeria. Email:keseme.odudu@uniben.edu Tel:+2348032340738

[1] The Economist Intelligence Unit, 'Open Banking: Revolution or Evolution?' <https://www.temenos.com/wp-content/uploads/2021/02/Temenos-Open-banking-VFinal-1.pdf> accessed 23 October 2023

https://doi.org/10.53982/apblj.2019.0301.04-j

Programming Interfaces (APIs).[2] Open banking has the potential to revolutionize the financial industry by promoting competition, enhancing customer experience, and fostering financial inclusion.[3] However, as data flows become more open, concerns about data protection and privacy become paramount. While open banking has the potential to significantly benefit customers, by spurring innovation and creating new markets for competition between banks and other financial institutions, it also has the potential to shift banks' duties significantly.[4] Therefore, there is a need for financial institutions to closely monitor data protection and privacy concerns associated with open banking to ensure that customer interests are safeguarded to ensure trust and confidence in the open banking ecosystem.[5]

The emergence of open banking has brought to the forefront the issue of data privacy, a subject of paramount importance, particularly in the context of all businesses that rely on customer-generated data, including social media and technology.[6] Of note is the sensitivity of customer financial data, which is a unique characteristic of open banking that adds an additional layer of complexity to the issue.[7] It is therefore imperative that measures are taken to address it to ensure that customer financial data is adequately protected. Financial institutions must also develop and implement robust systems and policies to ensure compliance with the relevant open banking regulations and laws. Open banking presents immense opportunities for the financial industry, but its effective implementation requires a comprehensive approach that considers the interests of all stakeholders while ensuring compliance with relevant regulations.[8]

---

2 G. Singh and S. Singh and P. Singh, *Financial Technology (Fintech): New Way of Doing Business,* (Ink of Knowledge, 2023), 56

3 S. Farell, *Banking on Data: Evaluating Open Banking and Data Rights in Banking Law,* (Wolters Kluwer 2023),

4 Banks' duty to protect customers' data becomes paramount due to the inherent risks of technology, there is a possibility of personal data breaches through cyberattacks. See R. Sahay and others, The Promise of FinTech: Financial Inclusion in the COVID Era (International Monetary Fund, 2020) 3

5 Singh and Singh and Singh, Financial Technology (Fintech): New Way of Doing Business, (n.2) 57

6 L. Jeng, *Open Banking,* (Oxford University Press, 2022) 3

7 ibid

8 L. Brosky and L Oakes, 'Data Sharing and Open Banking' <https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking> accessed 18 August 2023

The concept of open banking is associated with a host of benefits; however, the primary concern relates to the balance between innovation and the protection of individuals' data privacy rights. In Nigeria, where the significance of personal data protection is on the rise, the emergence of open banking necessitates a comprehensive assessment of its effects on personal data privacy rights.

2.0 Definition of Open Banking

It has been argued that open banking has no accepted legal definition, describing open banking rather than defining it is more common.[9] It has been described as banks sharing customer-permitted data with third-party companies and developers to create applications and services that provide real-time payments, more open options for account holders, and cross-selling opportunities. [10] An application programming interface (API), a sophisticated channel that enables the controlled yet smooth flow of data between systems, is frequently used to share data between systems.[11] Open banking is the use of open technology by third-party providers (TPPs) to deliver financial services (FS), and it offers guidelines for TPPs on how to access and use customer bank data in a standard format to enhance transparency and competitiveness in banking services.[12]

Three basic issues are presented by the current definitions of open banking: perspective bias, discipline bias, and purpose bias. On the issue of perspective bias, open banking involves three parties: the data owner, the custodian, and a third party that accesses the data.[13] It has been submitted that any definition of open banking must consider these three parties.[14] A generalised definition of open banking and its four applications (business model, fintech, data-sharing, and regulation) have been proposed.[15]

---

9 Farell, *Banking on Data* (n.3)

10 Bank for International Settlement, 'Report on Open Banking and Application Programming Interfaces'
< https://www.bis.org/bcbs/publ/d486.pdf>accessed 2 August 2023

11 Brosky and Oakes, 'Data Sharing and Open Banking' (n.8)

12 PWC, 'The Case for Open Banking in Nigeria'.
<https://www.pwc.com/ng/en/assets/pdf/case-open-banking-nigeria.pdf> accessed 18 August 2023.

13 G. K. B. de Araluze and N. C. Plaza 'Open banking: A Bibliometric Analysis-Driven Definition'
PLoS ONE [2022] 17(10), 4.

14 Ibid

15 Ibid, 2

A broad definition of open banking must be able to include all its usage contexts, not just one. Giving open banking an objective other than the original one which is to boost competition in retail banking by enabling the entrance of new competitors is the final aspect of the purpose bias issue.[16] A major restriction on the growth of open banking is that, given the combined impact of the three biases, the definitions that have been put up thus far prevent the creation of reliable and broadly applicable knowledge about the issue.[17]

Open banking has been defined as a generally regulated framework that enables banking customers to share their data with third parties, commonly through standardized interfaces such as APIs, to increase competition in the financial sector.[18] Open banking refers to a system that enables the secure sharing of customer banking data with third-party providers via application programming interfaces (APIs), subject to explicit consent and control of the customer.[19] It is a major shift from a closed structure to one in which data is shared within the banking ecosystem with the customer's consent.[20] Open banking empowers customers to effortlessly view and manage all their financial accounts and products from a single, unified platform, irrespective of the number of accounts they hold.[21]

Open banking allows customers to share their data with third parties which are usually Fintech companies.[22] The relationship between fintech and open banking promotes innovation, competition, and better customer experiences in the financial sector. The data-sharing capabilities of open banking are used by fintech companies to develop innovative, customer-focused services and upend established banking paradigms. The financial industry could change because of this synergy, ultimately delivering more options and superior services to consumers.

The Federal Government of Nigeria has made concerted efforts to enhance the ease of doing business and promote financial inclusion.[23] However, it has been

16 Ibid
17 Ibid
18 Ibid, 13
19 Farell, *Banking on Data* (n.3).
20 PWC, 'The Case for Open Banking in Nigeria'(n.12)
21 ibid
22 Singh and Singh and Singh, *Financial Technology (Fintech): New Way of Doing Business,* (n.2) 56
23 See National Financial Inclusion

observed that innovative financial services technology firms, commonly known as FinTech firms, are confronted with increasingly difficult barriers in providing services and applications to consumers.[24] This situation poses significant challenges to the growth and sustainability of the FinTech industry, which plays a crucial role in driving financial inclusion and economic development in Nigeria.[25] Therefore, there is a need to address the existing challenges and create an enabling environment that encourages FinTech innovation and growth in the country.

Open banking is designed to give financial service providers a uniform standard. While banks may utilize the same banking software, such as Finacle or Flexcube, their technical strategies can vary due to customized elements in each implementation.[26] Such nuances can pose communication challenges for Financial Service providers.[27] This is where open banking comes into play, as it provides a common standard and language within the industry to address these issues.[28] The notion of open banking has been in existence for some time, as financial institutions strive for a more straightforward means of

---

Strategy (Revised), 2018, <https://www.cbn.gov.ng/out/2019/ccd/national%20financial%20inclusion%20strategy.pdf> accessed 23 October 2023

24 PWC, 'The Case for Open Banking in Nigeria'(n.12). FinTech are technology-enabled innovations in financial services that could result in new business models, applications, processes, or products with an associated material effect on the provision of financial services. While financial inclusion means access to financial services. See R. Sahay and others, *The Promise of FinTech: Financial Inclusion in the COVID Era* (n.4) ix. When adult Nigerians have simple access to a variety of formal financial services that satisfy their needs at reasonable prices, financial inclusion has been accomplished. See National Financial Inclusion Strategy (Revised), 2018, <https://www.cbn.gov.ng/out/2019/ccd/national%20financial%20inclusion%20strategy.pdf> accessed 23 October 2023

25 Enhanced financial inclusion is a social benefit of financial technology advancement. See. E. X. Liu, 'Stay Competitive in the Digital Age: The Future of Bank' IMF Working Paper, 11, <https://www.google.com.ng/books/edition/Stay_Competitive_in_the_Digital_Age_The/DLsoEAAAQBAJ?hl=en&gbpv=1&dq=While+open+banking+has+the+potential+to+significantly+benefit+customers,+by+spurring+innovation+and+creating+new+markets+for+competition+between+banks+and+other+financial+institutions,+it+also+has+the+potential+to+shift+banks%27+duties+significantly.&printsec=frontcover> accessed 23 October 2023

26 ibid

27 ibid

28 ibid

transmitting data within their network.[29] The achievement of the Central Bank of Nigeria's financial inclusion goal and the newly published directives for the formation of Payment Service Banks (PSB) depend largely on the seamless flow of information between PSBs and external service providers.[30]

Open banking is a transformative concept that holds significant potential for all stakeholders in the financial services sector. By leveraging the power of data, organizations can gain an enhanced understanding of consumer financial behaviour and trends.[31] This information enables banks and other financial services firms to assess a borrower's probability of loan repayment, financial position, goals, and purchasing preferences.[32] Moreover, consumers can use this data to gain insights into their behavioural patterns and interests, empowering them to make informed decisions to safeguard their interests and promote a more robust competitive landscape.[33] The availability of greater bank data can also foster innovation, with service providers devising novel approaches to understand and improve financial behaviour and outcomes.[34] Overall, open banking represents a promising avenue for financial institutions to optimize their operations and enhance customer experiences.[35]

The nascent open banking landscape in Nigeria has garnered early support from key stakeholders, including but not limited to esteemed entities such as Sterling Bank, along with prominent professional services firms like KPMG, PwC, Paystack. Wallet Africa, OnePipe and EY.[36] The foundational support extended by these entities underscores the strategic importance and collaborative ethos of the open banking paradigm within the Nigerian financial ecosystem. Noteworthy additions to this coalition, encompassing entities like Mono, Switch, Lendsqr, Palmpay, Carbon, and Trium, manifest a broadening consortium that reflects the evolving and dynamic nature of the open banking initiative in the Nigerian context.[37] This burgeoning alliance signifies a

29 ibid
30 ibid
31 Singh and Singh and Singh, Financial Technology (Fintech): New Way of Doing Business, (n.2) 57
32 PWC, 'The Case for Open Banking in Nigeria' (n.12)
33 ibid
34 Singh and Singh and Singh, Financial Technology (Fintech): New Way of Doing Business, (n.2) 57
35 PWC, 'The Case for Open Banking in Nigeria' (n.12)
36 H, Moses-Ashike, 'Explainer What to Know About Open Banking' (*BusinessDay* March 9 2023) <https://businessday.ng/news/article/explainer-what-to-know-about-open-banking/> accessed 8 November 2023
37 ibid

concerted effort to cultivate an environment conducive to financial innovation, interconnectivity, and the advancement of the financial technology landscape in Nigeria.

The institutionalization of the Nigerian Open Banking APIs by the apex regulatory body, the Central Bank of Nigeria (CBN), constitutes a pivotal stride towards fostering a standardized interface.[38] This interface serves as a conduit, affording third-party providers the sanctioned means to systematically access customer data resident within banking institutions. This regulatory framework not only engenders a paradigm shift in the modus operandi of financial data accessibility but also lays the groundwork for a structured and secure ecosystem wherein the tenets of open banking are methodically upheld. The introduction of such standardized APIs by the CBN epitomizes a concerted effort to cultivate an environment characterized by interoperability, transparency, and the judicious exchange of financial information within the Nigerian financial landscape. Some of the top five API providers in Nigeria include Paystack, Flutterwave, Blochq, GetAnchor, and Maplerad,[39]

3.0 Can Privacy and Innovation Co-exist?

Open banking's potential is undeniable. Increased competition fosters innovative financial products and services, enhancing consumer choice and experiences. Imagine personalized budgeting apps, streamlined loan applications, or automated investment solutions – all powered by open banking data. These benefits can be substantial.[40] Yet, this convenience comes at a cost. Sharing sensitive financial data raises privacy concerns.[41] Data breaches are a constant threat, exposing individuals to financial fraud, identity theft, and reputational damage.[42] The implementation of open banking and the consequent increase in data sharing have been associated with a rise in data

---

[38] CBN, 'Issuance of Regulatory Framework for Open Banking in Nigeria' <https://www.cbn.gov.ng/out/2021/psmd/circular%20on%20the%20regulatory%20framework%20on%20open%20banking%20in%20nigeria.pdf> accessed 8 November 2023

[39] BillsAfrica 'Top 5 Bank Transfer API Providers for Nigerian Businesses' <https://bills.africa/blog/top-5-bank-transfer-api-providers-for-nigerian/> accessed 8 November 2023

[40] N. Ayantoye, 'Data Privacy at the Core of Open Banking in Nigeria' <https://spaajibade.com/data-privacy-at-the-core-of-open-banking-in-nigeria/> accessed 20 February 2024

[41] C. Winch 'Are Data Protection and Open Banking Compatible?' <https://www.ukfinance.org.uk/news-and-insight/blogs/are-data-protection-and-open-banking-compatible> accessed 20 February 2024

[42] A. O. Oloveze and others, 'Effect of Bank Customers' Privacy Concern on Intention To Adopt Open Banking' *Nigerian Journal of Management Sciences,* (2023) 24(2b), 116-126

breaches, fraudulent activities, and phishing attacks.[43] According to a recent report by the Nigeria Inter-Bank Settlement System Plc (NIBSS), as more people get financially integrated into various payment systems, more opportunities are opening up for fraudsters to engage in their illicit activities.[44] According to the report, between 2019 and 2021, fraud attempts on mobile payment channels, Web portals, and Point of Sale (PoS) terminals increased by 173 per cent and 215 per cent annually.[45]

Some risks involved in open banking have been identified as discriminatory or exploitative use of data, data exclusion and digital capability, and vulnerable consumers.[46] Concerning discriminatory or exploitative use of data, it is critical to ensure the protection of data gathered via open banking to prevent any potential misuse. Any unauthorised use of consumer data by banks or third-party providers could result in privacy violations and mishandling of personal information. Such scenarios could prove harmful to the consumer, and therefore, safeguarding their data must remain a top priority. The inappropriate utilisation of data for exploitation constitutes a grave concern, specifically for consumer groups that are more susceptible to exploitation, such as individuals afflicted with mental illness.[47]

How then can innovation be balanced with privacy within the open banking ecosystem? Babin and Smith emphasise the importance of giving consumers security and protection through a consistent framework when implementing open banking.[48] Governments may face difficulty in adopting a uniform framework that offers consumers the security and safeguards they require while also allowing for innovation and optimisation of financial services using the open banking model.[49]

---

43 PWC, 'The Case for Open Banking in Nigeria' (n.12), The Nigeria Inter-Bank Settlement System Plc (NIBSS) 'NIBSS Insight: Fraud in the Nigeria Financial Services' <https://nibss-plc.com.ng/nibss-insight-fraud-in-the-nigeria-financial-services/page/10/?et_blog> accessed 18 August 2023

44 B. Dada 'Fraud up by 330% in Nigeria, says NIBSS' <https://www.benjamindada.com/nibss-financial-fraud-report/> accessed 18 August 2023

45 ibid

46 E. Leong and J. Gardner 'Open Banking in the UK and Singapore: Open Possibilities for Enhancing Financial Inclusion' Journal of Business Law [2021] 5, 15

47 ibid

48 R. Babin and D Smith, 'Open Banking Regulation: Please Advise the Government' *Journal of Information Technology Teaching Cases* [2022] 12(2) 108-114

49 Ibid, 108

Tackling the impact of open banking on privacy necessitates a careful and nuanced strategy.[50] It is submitted that focusing solely on minimizing breaches might be like playing whack-a-mole – reactive and never fully effective. Instead, Nigeria should strive for proactive privacy protection which consists of measures that prevent data breaches from occurring.[51] This entails several factors, firstly, strong legal frameworks defining data ownership, access rights, and security standards are crucial. Nigeria's Data Protection Act 2023 and regulations on open banking can provide a foundation. Secondly, data security should be embedded throughout the open banking ecosystem. APIs enable the real-time exchange of financial data between parties in Open Banking.[52] But their direct access to sensitive financial data also makes them a prime target for cyber threats.[53] Therefore, proactive privacy data measures such as secure APIs, encryption, and regular security audits are vital. This approach involves identifying any weaknesses or vulnerabilities within the system by searching for loopholes.[54] Once these potential weak points are discovered, they are addressed and corrected to prevent them from being exposed and taken advantage of.[55]

This issue of privacy breaches has sparked a wide-ranging debate about the ethical implications of data-driven decision-making and the need for regulatory frameworks to prevent abuses of power. For instance, a study underscores the imperative of preserving the sanctity of customer data, advocating for corporate entities to conscientiously collect and deploy such data judiciously.[56] The study posits a call to action for organisations to adhere to stringent data-security protocols, incorporating robust encryption

---

50 A. Acquisti and C. Taylor and Wagman, 'The Economics of Privacy' *Journal of Economic Perspectives,* (2016) 30(2), 3-28

51 A. Sharma 'Is a Proactive Approach Best for Data Privacy and Cybersecurity?' <https://www.dataversity.net/is-a-proactive-approach-best-for-data-privacy-and-cybersecurity/> accessed 20 February 2024. See also A. Anjaiah and others 'The Importance of Proactive Data Privacy and Cyber Security from Attacks' *International Journal of Advance Research in Computer Science and Management Studies*, (2019) 9(10), 10-12

52 Zendatta, 'Data Privacy in Open Banking' <https://www.zendata.dev/post/data-privacy-in-open-banking> accessed 20 February 2024

53 ibid

54 Sharma 'Is a Proactive Approach Best for Data Privacy and Cybersecurity?' (n)

55 ibid

56 H. H. H. Aldboush and M. Ferdous, 'Building Trust in Fintech: An Analysis of Ethical and Privacy Considerations in the Intersection of Big Data, AI, and Customer Trust' *International Journal of Financial Studies,* [2023] 11(3), 90

methodologies.[57] Additionally, it recommends a periodic and comprehensive review and enhancement of extant data-protection policies as indispensable measures in maintaining the integrity and confidentiality of customer data.[58] Consumers must have clear, understandable information about data use and granular control over what they share. Transparency reports, opt-out mechanisms, and easily accessible privacy settings are essential. To ensure open banking data aggregation operates with transparency, it is crucial to consider the long-term impact of sharing consumer data. Although there may be short-term benefits for consumers, such as improved access to financial services, there are potential risks associated with aggregate data that could negatively affect their risk profiles and decision-making processes.[59]

It has been postulated that the open banking environment is characterized by data asymmetry, which renders customers the most disadvantaged group.[60] It is essential to establish trust between customers and participants within the open banking ecosystem. To achieve this, scholars recommend implementing strategies such as Corporate Digital Responsibility (CDR).[61] This approach focuses on promoting ethical and responsible practices in the use of data and technological innovations.[62] With CDR, companies can build trust with their customers and ensure they are using their technology safely and ethically.[63]

Three sets of policy questions are typically raised by open banking for regulators: the first is about how to foster and capitalise on the benefits of competition and innovation; the second is about data protection and privacy; and the third is about whether and how to regulate third parties who have access to customer data.[64] This paper analyses the legal framework for open banking in Nigeria intending to determine whether there is a balance between innovation and privacy.

4.0 Legal Framework for Open Banking in Nigeria

---

57 ibid

58 ibid

59 Aldboush and Ferdous, 'Building Trust in Fintech' (n.)

60 ibid

61 L. Lobschat and others, 'Corporate Digital Responsibility' *Journal of Business Research* 2021 122 (c),875 -888

62 ibid

63 ibid

64 H. Natarajan 'Regulatory Aspects of Open Banking: The Experience thus Far' <https://european-economy.eu/2022/regulatory-aspects-of-open-banking-the-experience-thus-far/> accessed 16 August 2023

This paper investigates the effects of open banking on data privacy, bearing in mind the paramount importance of preserving the confidentiality of sensitive information. Consequently, it becomes imperative to scrutinize the legal framework for data privacy in Nigeria, to assess its adequacy in safeguarding the privacy rights of individuals. The Nigeria Data Protection Act 2023 (NDPA)[65] defines personal data as any information relating to a person, that is, one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that person.[66]

Financial data can include how much money we have in our account, how much money we owe, how much money we make and what our investments are. Financial data encompasses a broad range of information, including but not limited to an individual's current account balance, outstanding debts, earnings, and investments.[67] These are very sensitive and commercially viable information, financial data also covers, account login username and password. [68] It has been posited that to achieve a balance between the commercial interests and personal rights associated with open banking, it is imperative to establish a universally accepted set of data protections and rights that align with customer expectations.[69]

Article 12 of the Universal Declaration of Human Rights posits that no individual shall be subject to arbitrary interference with their privacy, family, home, or correspondence, nor shall they be subjected to attacks on their honour and reputation.[70] This provision is a fundamental pillar of human rights law, as it recognizes and protects every individual's inherent right to privacy. The International Covenant on Civil and Political Rights (ICCPR)[71] and the European Convention on Human Rights and Fundamental Freedoms (ECHR)[72] also recognize the right to privacy as a fundamental human right.[73]

---

65 The Nigeria Data Protection Act 2023 Federal Republic of Nigeria Official Gazette No.119 Vol. 110 (1 July 2023)

66 NDPA 2023, s.65

67 Jeng, *Open Banking*, (n.6) 2

68 ibid

69 Jeng, *Open Banking*, (n.6) 4

70 Universal Declaration of Human Rights, 10 December 1948, UN General Assembly

71 U.N. General Assembly Resolution 2200A (XXI) of 16th Dec. 1966; in force 23rd March 1976

72 European Treaty Series No. 5; opened for signature 4th Nov. 1950; in force 3rd Sept. 1953

73 ICCPR, art.17 and the ECHR, art.8

In Nigeria, Section 37 of the 1999 Constitution of the Federal Republic of Nigeria (as amended) provides that 'the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.' The NDPA 2023 is Nigeria's data protection legislation. It applies to the processing of personal data where the data controller is resident, domiciled in or operating in Nigeria, where the processing occurs in Nigeria, or even when the data controller is not resident or domiciled in Nigeria but is processing the personal data of a data subject in Nigeria.[74] This means that open banking must comply with the provisions of the NDPA 2023. The NDPA 2023 provides for basic principles of data protection which data controllers must comply and they include lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security) and accountability.[75]

The efficient operation of open banking services, including FinTech firms, is heavily reliant on the availability of data.[76] Such entities are contractually bound to provide specific products and services that are solely dependent on the availability of data.[77] Therefore, the unavailability of data can significantly impede the provision of such services. It is imperative for banks to retain their traditional role as custodians of customers' financial data, without compromising on its security.[78] This paper submits that as the financial sector continues to evolve, the importance of data protection and privacy cannot be overstated. Banks are expected to uphold their fiduciary duty towards their customers by safeguarding their sensitive financial data.[79] Any breach of this responsibility could result in severe financial and reputational damage, which could be detrimental to the bank's long-term success.[80] Therefore, banks must remain vigilant and adopt robust security measures to protect their customers' financial data.

The customer must consent to the sharing of his data with third parties. The NDPA 2023 specifies consent as one of the legal basis for processing personal data.[81] Data controllers must adhere to the requirements for obtaining the

---

74 NDPA 2023, s.2
75 Ibid, s.24(1), (2) and (3)
76 Jeng, *Open Banking,* (n.6) 6
77 ibid
78 Jeng, *Open Banking,* (n.6) 2
79 P. Gupta and M. Tham, *Fintech: The New DNA of Financial Services* (Walter de Gruyter Inc, 2019) 162
80 ibid
81 NDPA 2023, s.25(1) (a)

consent of data subjects under the Act; for example, requests for consent must be in an accessible format and in clear and simple language.[82] The NDPA 2023 also requires the data controller to prove that the data subject gave consent for the processing.[83] The ability of the customers (data subject) to revoke consent at any time should also be made clear to them, before the granting of such consent.[84] By the NDPA 2023, customers may withdraw consent at any time; operators of open banking have the responsibility of ensuring that the process for withdrawal of consent is seamless.[85] The Act provides for several rights of the data subject such as the right to be informed, the right to access personal data, the right to rectification, the right to erasure, the right to restrict processing, and the right to data portability among others.[86]

4.1 Duties of Financial Institutions as Data Controllers under the Nigeria Data Protection Act

The duties of data controllers which will be operators of open banking in this case, are also listed in the NDPA 2023 to include: establishing organisational and technical safeguards to guarantee the security, integrity, and confidentiality of personal data in its possession, among others.[87] Where a data controller engages the services of a third party to process the personal data of data subjects, the data controller is obligated to take appropriate precautions to make sure that the other party complies with the principles and obligations outlined in the Act.[88] These provisions require banking institutions to exercise due diligence before sharing customer data with third parties. It also means that they will be held accountable for the actions of such third parties.[89] Other duties under the other regulations on open banking will be discussed below.

4.2 Other Regulations on Open Banking in Nigeria

Apart from the NDPA 2023, there are other specific regulations on open banking in Nigeria. On February 7, 2021, the Central Bank of Nigeria (CBN) released the open banking regulatory framework for Nigeria, setting the stage for an industry group to publish the Exposure Draft of the Operational Guidelines for Open Banking in Nigeria (the Draft Operational Guidelines) in

82 Ibid, s.26(6)
83 Ibid, s.26(1)
84 Ibid, s.26(4)
85 Ibid, s.30
86 See NDPA 2023, pt.VI
87 Ibid, s.39
88 Ibid, s.29
89 Ibid, s.29(1)(d)

May 2022.[90] On 7 March 2023, the Central Bank of Nigeria issued Operational Guidelines for open banking in Nigeria to foster the sharing of customer-permissioned data between banks and third-party firms to enable building customer-focused products and services.[91] Developing robust frameworks and governance to underpin technical connections is critical due to inherent risks in data sharing.[92] There is therefore need for an adequate legal framework for open banking to protect the customer's right to data privacy.

The Operational Guidelines for Open Banking in the country were released by the CBN to promote competition and innovation in the banking industry and expand the variety of financial services available to bank customers.[93] This is in line with the objectives of open banking. The Guidelines apply to banking and other associated financial services as defined and determined by the CBN in the Regulatory Framework for Open Banking in Nigeria.[94] Any organisation that holds client data that can be shared with other organisations to offer cutting-edge financial services in Nigeria is qualified to participate in the open banking ecosystem.[95] The following roles that participants in the open banking ecosystem may play are used to categorise them:[96]

1. An Application Programme Interface Provider (AP) is a participant who makes data or services available to other participants using APIs. An authorised financial institution or service provider, a Fast-Moving Consumer Goods (FMCG) Company, another retailer, a Payroll Service Bureau, etc. are all examples of API Providers.
2. A participant who uses an API that has been made available by an API provider is referred to as an API Consumer (AC). An authorised financial institution, service provider, retailer of FMCG products or other goods, payroll service bureau, etc. are all examples of API Consumers.

---

90 Open Banking Nigeria, 'Open Banking Regulation in Nigeria is now Approved by the CBN' <https://www.openbanking.ng/open-banking-regulation-in-nigeria-is-now-approved-by-the-cbn/> accessed 8 August 2023

91 See Operational Guidelines for Open Banking in Nigeria <https://www.cbn.gov.ng/Out/2023/CCD/Operational%20Guidelines%20for%20Open%20Banking%20in%20Nigeria.pdf> accessed 2 August 2023

92 Brosky and Oakes, 'Data Sharing and Open Banking' (n.8) 3

93 See the preamble to the Guidelines and art..3.0

94 Ibid, art.4.0

95 Ibid, art.4.1

96 ibid

3. Customer: This term refers to the data owner and end-user who may be asked for their permission before their data is released to access financial services.

4.2.1 Safeguards in the Guidelines

The Guidelines contain some provisions to ensure transparency within the open banking system in Nigeria. The CBN is mandated to open and maintain an Open Banking Registry (OBR) for the industry which is a public database with participant registration information.[97] The Guidelines also contain some accreditation criteria for onboarding into the OBR.[98] Those who can participate in open banking in Nigeria include, Participants without regulatory licence (Tier 0 PIST and MIT), Participants through CBN Regulatory Sandbox (Tier 1), Licenced Payments Service Providers and OFIs (Tier 2) and Deposit Money Banks (Tier 3).[99] Tier 0 must be sponsored by Tier 2 or 3 participants and requires a risk assessment report from the sponsor's Chief Risk Officer.[100] Tier 1 must be admitted to the regulatory sandbox by CBN. Additional enrollment criteria may apply.[101] While Tier 2 and 3 require a valid CBN license and risk assessment report from two Tier 2 or 3 partners (KYC, financial strength, risk management).[102]

Key points to note from an overview of the enrollment process for each tier in Nigeria's Open Banking Registry are: Tiers 2 and 3 play a crucial role in enrolling other participants by conducting risk assessments and sponsoring Tier 0 participants. All tiers (except Tier 1) need to submit risk assessment reports focusing on Know Your Partner (KYC) protocols, financial strength, and risk management practices. Partner participants conducting risk assessments must be Tier 2 or 3 themselves.[103] The purpose of the Registry is to oversee participation through regulation, to increase transparency in open banking activities' and to guarantee that only registered organisations operate within the open banking system. Customers must give their consent before their data may be used by a service provider to offer them financial products and services.[104] The AP may only share the customer's information with an

97 Guidelines, art.6.0
98 Ibid, art. 7.0
99 Regulatory Framework, art. 5.1
100 Ibid, art.5.2.1
101 Ibid, art.5.2.2
102 Ibid, art.5.2.3, art.5.2.4
103 Regulatory Framework, art.5.2
104 Guidelines, art.7.0

AC when a consumer presents valid evidence of consent, and only after authenticating that the customer gave that consent.[105]

To ensure consumer consent, the AC must provide specific details such as the AC's full and legal name, accreditation/registration number, business registration number with the CAC, compliance with access levels, nature of the request, and information on customer consent withdrawal.[106] When the AP receives the customer's consent to share the customer's data with an AC, it must confirm that the consumer gave the consent, this requires 2-factor Authentication (2FA) of the end-user to verify the consent.[107] This is in line with the provisions of the NDPA.

However, it has been submitted that consent-based access to data although allowing for innovation may also raise several policy questions.[108] One of which is how to protect the privacy of customers' data. Therefore ensuring adequate data protection and privacy safeguards is essential in building trust and giving customers a certain level of control over their data thus boosting the use of digital financial products which will in effect strengthen the economy.[109] The other data protection considerations that are relevant in open banking are data governance and enforcement, cybersecurity and data security.[110] Although the legal and regulatory framework for open banking is fundamentally based on consent, there is frequently a lack of clear procedures on how to implement it. It has been submitted that general standards on consent provisions may not fully consider open banking's use of technology and the current state of the market.[111]

Consent on its own is insufficient to guarantee data protection but if properly designed and implemented, it is an effective tool in granting customers control over their data.[112] robust data- and consumer-protection framework is required to adequately protect consumers under open-banking schemes, and consent should be viewed as one component of a larger all-encompassing strategy for

105 Ibid, art.11.1
106 ibid
107 Ibid, art.11.2
108 Natarajan 'Regulatory Aspects of Open Banking: The Experience thus Far' (n.64)
109 ibid
110 ibid
111 ibid
112 ibid

https://doi.org/10.53982/apblj.2019.0301.04-j

safeguarding their interests.[113] These include regulatory oversight, privacy by design, effective dispute regulation and enforcement mechanisms.

The Guidelines provide that the API providers and the API consumers are to execute a Service Level Agreement (SLA) to govern the relationships between them. The SLA should include provisions relating to accounting and settlement, fee structure, reconciliation of bills, registration and sponsorship responsibilities.[114] All operators of open banking must ensure that all systems required for open banking are made available with minimum standards specified in the guideline. [115] API providers are obligated to monitor infrastructural and API levels performance this entails monitoring hardware, operating systems etc. at the functional level, collecting performance metrics for all API transactions and implementing alert monitoring processes.[116] API providers are obligated to implement incident management procedures, while APs are obligated to monitor performance.[117] The Guidelines prohibit APs from engaging in unethical and unprofessional conduct.[118] The Guidelines stipulate that APs are to provide monthly reports to the ACs indicating performance metrics, statistics of incidents and problems, SLA adherence, and the quantity and kind of fraud and disputes, among others.[119] Customers who have subscribed to one or more ACs must receive certain reports from APs, especially when an AC accesses their account(s) or wallet(s).[120] Participants in open banking are to develop customer complaint procedures, redress mechanisms, dispute resolution and liability appropriation models.[121]

ACs must provide monthly returns to CBN on transaction volume, value, user count, success/failure rates, security incidents, fraud, downtime reports, and other requirements.[122] Customers can escalate complaints to the Consumer Protection Department of CBN if they have exhausted the Participant's Internal Dispute Resolution, where the participant fails to resolve the complaint within 14 days, is not undergoing resolution, or where the

113 ibid
114 Guidelines, para.8.1.2
115 Ibid, para.8.2
116 Ibid, para.8.2.1
117 Ibid, paras.8.2.2.2 and 8.2.3
118 Ibid, para.8.9
119 Ibid, para. 8.8.1
120 Ibid, para. 8.8.2
121 Ibid, para.4.4.1
122 Ibid, para.9.4

complaint is not under litigation or adjudicated by a court.[123] Thus the CBN acts as an oversight body over participants in open banking, this is relevant considering that to a reasonable extent, the success, security, and ethical functioning of open banking are to a large extent hinged on oversight. In the open banking ecosystem, regulators are more equipped than consumers to hold operators accountable and halt systematic abuses due to their skill and financial resources.[124]

The Guidelines contain some provisions relating to data ethics and data privacy. It requires that a committee of the board of directors, or at the very least the executive management committee of the AC, must establish a Data Governance Policy.[125] The policy must make sure that all data is properly managed and complies with legal and regulatory obligations. The AC must implement a clear data governance policy, procedures, and mechanisms which must include a systematic approach to gathering, assembling, storing, and retrieving data that complies with legal requirements and regulations, the consideration of data interplay with algorithmic systems, and the unintended consequences of data-driven services on customers and society.[126] Under the Guidelines, ACs must have a data ethics framework, guiding personal data acquisition, collection, analysis, use, and sharing, ensuring consistent processes, compliance with laws, and producing fair reports for customers and society.[127] This is commendable because an effective data ethics framework ensures that customer data is handled with the highest standards of privacy and security. [128] Secondly, customers are more inclined to use open banking services if they feel sure that their data is being treated properly and ethically, which may be achieved by having a clearly defined ethics framework.

To ensure the protection of customers, ACs are required to comply with data protection laws and any CBN-issued data protection regulations for financial institutions.[129] All participants of open banking are required to implement Information Security controls, ensure effective Information Security management, and establish protections against data breaches.[130] ACs are also

123 Ibid, para.5.0
124 Natarajan 'Regulatory Aspects of Open Banking: The Experience thus Far' (n.64)
125 The Guidelines, para.9.1
126 ibid
127 Ibid, para.9.1.1
128 I. Marcovitcha and E. Rancourtb, 'A Data Ethics Framework for Responsible Responsive Organizations in the Digital World' *Statistical Journal of the IAOS* (2022) 38 1161–1172
129 The Guidelines, para.9.3, 9.3.1 and 9.3.2
130 Ibid, para.9.3

required to maintain a data breach policy and comply with Technical Security Standards.[131]

It is submitted that by addressing ethical and privacy concerns, the Guidelines facilitate the long-term viability of open banking in Nigeria. It decreases the possibility of public backlash or regulatory crackdowns brought on by privacy abuses, which would otherwise threaten or derail the entire open banking system. It has been submitted that with the release of the Guidelines, the CBN is cognizant of the risks of open banking and has made significant provisions to minimise them.[132] Therefore, the Guidelines will guarantee the safe operation of Open Banking in Nigeria if thoroughly implemented.[133]

It is also important to consider the challenges banks may face in adopting open banking. Before providing open data, it is imperative for banks to prudently evaluate the potential risks and challenges that may arise.[134] Doing so will enable them to take necessary measures to mitigate any unfavourable outcomes and ensure a successful implementation. In the realm of open banking, where financial institutions are expected to share customer data with third-party providers, ensuring the security of such data is paramount. Banks must therefore meticulously consider the measures they put in place to safeguard customer data, given the potential implications of a security breach in this context.[135] It is submitted that the quality of security must be commensurate with the magnitude of the risk involved. Therefore, banks need to implement robust security protocols that can withstand a variety of threats, such as cyberattacks, data breaches, and identity theft. By doing so, they can not only protect their customers' sensitive financial information but also maintain their credibility and reputation within the industry.

5.0 Analysis of the United Kingdom Open Banking Legal Framework

This paper uses the legal framework for open banking in the United Kingdom (UK) to compare that of Nigeria to draw lessons that will benefit Nigeria. The United Kingdom's standing as a world pioneer in open banking, closely followed by nearly 30 other nations, serves as the primary impetus for the

131 Ibid, paras. 9.3.3 and 9.3.3.2

132 T. Osazuwa and P. Pere and M. Poopola 'Overview of the Operational Guidelines for Open Banking in Nigeria' <https://www.mondaq.com/nigeria/financial-services/1297644/overview-of-the-operational-guidelines-for-open-banking-in-nigeria> accessed 7 August 2023

133 ibid

134 Gupta and Tham, *Fintech: The New DNA of Financial Services,* (n.79) 162

135 ibid

present comparative analysis.[136] This comparative study aims to provide a comprehensive and objective assessment of the UK's open banking system's performance, highlighting its successes and shortcomings while benchmarking it against comparable systems worldwide. The study seeks to establish a clear understanding of the UK's open banking system and its role in the global financial industry.

The publication of a report by the Competition and Markets Authority (CMA) in 2016 saw the beginning of open banking in the UK.[137] To improve competition in retail banking, the report suggested the implementation of open banking.[138] The CMA highlighted a lack of innovation and competition in the retail banking sector and offered solutions to give consumers more control and promote competition.[139] The CMA then issued an Order establishing a series of open banking-related remedies, mandating the adoption of 'open application programming interface ("API") banking standards' by the UK's nine largest banks also the publication of data following these standards.[140] The Open Banking Implementation Entity (OBIE), an independent organisation in charge of planning and carrying out the open banking project, was created as a result of the CMA findings.[141] The OBIE also published standards technical standards and security protocols that operators in the open banking ecosystem must adhere to.

The Second Payment Services Directive (PSD2) of the EU, which advances earlier initiatives to create a digital single market, has an impact on the growth

---

136 Competition and Market Authority, 'The Future of Oversight of the CMA's Open Banking Remedies' <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1086515/Consultation_response_publication.pdf> accessed 10 August 2023

137 CMA, 'Retail Banking Market Investigation: Final Report' (9 August 2016), <https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf> accessed 10 August 2023

138 Leong and Gardner 'Open Banking in the UK and Singapore' (n.48) 427. Competition and Market Authority, 'Retail Banking Market Investigation' <https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk> accessed 11 August 2023

139 Open Banking Limited 'The Origins of Open Banking' <https://www.openbanking.org.uk/about-us/> accessed 11 August 2023

140 Competition and Market Authority, 'Retail Banking Market Investigation' (n.130)

141 GOV.UK 'Millions of Customers Benefit as Open Banking Reaches Milestone' <https://www.gov.uk/government/news/millions-of-customers-benefit-as-open-banking-reaches-milestone> accessed 10 August 2023

https://doi.org/10.53982/apblj.2019.0301.04-j

of open banking in the UK.[142] PSD2 addresses the explosive rise of mobile and electronic payments as well as innovative payment services.[143] The PSD2 was implemented in the UK by virtue of the Payment Services Regulations 2017 (PSRs).[144] Customers have the option to request certain services from third parties by virtue of the PSRs, such as: making payments on their behalf via Payment Initiation Services (PIS) and accessing their financial information by means of Account Information Services (AIS).[145] In line with the PSRs, banks and other payment service providers are required to allow third-party providers access to their systems with the customer's explicit consent.[146] Payment service providers are required to establish and implement adequate and effective procedures for complaint resolution, aimed at settling any complaints from payment service users concerning their rights and obligations.[147]

The Financial Conduct Authority (FCA) is the primary authority which regulates open banking in the UK. The FCA is required to have proper arrangements in place to allow payment service users and other concerned parties to lodge complaints regarding any breach of a requirement imposed by or under Parts 2 to 7 of these Regulations by a payment service provider.[148] Open banking APIs can only be accessed by businesses that have been approved by the FCA to make payments or access financial data on behalf of customers.[149]

Adapting and tailoring the principles and strategies of the UK's open banking regulatory framework could be beneficial for Nigeria's financial ecosystem, technology landscape, and customer requirements. Nigeria, like many other

142 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, recital 29

143 Ibid, recital 3

144 The Payment Services Regulations 2017, available at <https://www.legislation.gov.uk/uksi/2017/752/regulation/1/made> accessed 11 August 2023

145 Ibid, regs. 69 and 70

146 Ibid, reg.67

147 Ibid, reg.101(2)

148 Ibid, reg.117.

149 Ibid, reg.4.

countries, has been influenced by the UK's Open Banking approach.[150] The open banking regulations in Nigeria differ significantly from those in the UK. [151] Unlike the UK's focus on AISP and PISP players, Nigeria's implementation revolves around the domains of 'API Consumer' and 'API Provider.'[152]

The Central Bank of Nigeria has implemented a more inclusive approach to API providers. Under this approach, an API provider can be a licensed financial institution or service provider, a fast-moving consumer goods (FMCG) company, a retailer, or a payroll service bureau. This is a broader scope compared to the approach in Europe. In contrast to the regulatory framework in Nigeria, which mandates third-party providers to obtain a license from the CBN, it is discerned that a particular registration mechanism akin to the United Kingdom's Open Banking Standard is notably absent. The UK's Open Banking Standard, by contrast, imposes a stringent regimen of comprehensive testing and registration as prerequisites for third-party providers to access customer data.[153] This disparity engenders the possibility of a disparity in the standards of security and dependability, potentially culminating in a relatively lower standard amongst third-party providers operating within the Nigerian context. To ensure a high level of security and reliability, it has been recommended that it is advisable to establish a rigorous and impartial registration process for third-party providers.[154]
In the UK, there is no tiered system, all participants register directly with Open Banking Implementation Entities (OBIEs).[155] Participants are to apply for authorisation or registration with their Competent Authority for the role(s)

---

150 E. Duncan, 'Feature: How has Nigeria approached Open Banking?' <https://www.openbankingexpo.com/features/feature-how-has-nigeria-approached-open-banking/> accessed 20 October 2023

151 Ibid.

152 Ibid.

153 UK Open Banking Standard < https://standards.openbanking.org.uk/> accessed 16 November 2023

154 The Legal 500 'Open Banking in Nigeria Legal Considerations for Data Sharing in Financial Services' <https://www.legal500.com/developments/thought-leadership/open-banking-in-nigeria-legal-considerations-for-data-sharing-in-financial-services/> accessed 10 November 2023

155 'How Do I Enrol with the Open Banking Implementation Entity for Read/Write Data' <https://directory.openbanking.org.uk/obieservicedesk/s/article/Enrolling-with-the-Open-Banking-Implementation-Entity-for-Read-Write-Data> accessed 26 February 2024

they wish to perform.[156] All participants need to perform thorough application and security testing that is suitable for their organization and the services they intend to offer.[157] TPPs (Third Party Providers) conduct self-assessments against security and technical standards.[158] There is emphasis on compliance with PSD2 (Payment Services Directive 2) regulations and Open Banking standards.[159] The UK's emphasis on self-assessment and compliance with established standards seems efficient. Nigeria could explore incorporating elements of this approach, potentially empowering participants to take greater responsibility for security and compliance while reducing reliance on partner assessments. Secondly, the UK's single-entry point for all participants might be worth considering in Nigeria. This could potentially reduce complexity and expedite entry for new participants, especially Tier 0 and Tier 1, fostering wider adoption.

The Nigerian framework also requires API providers and clients to sign Service Level Agreements (SLAs), which would set the terms of their interactions.[160] This is not the situation in Europe, where contracts with TPPs are not specifically required by ASPSPs, albeit in practice there may be requirements for API performance. Open banking regulation Regulations governing open banking permit third-party providers in the UK to use bank APIs with a one-off authorisation from the national regulator, without the need for protracted negotiations or contractual agreements.[161]

---

156 Open Banking Limited 'Open Banking: Guidelines for Read/Write Participants' 17, https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Read-Write-Participants.pdf> accessed 26 February 2024

157 Ibid, 22

158 ibid

159 Ibid, 16

160 Guidelines, para.8.1.2.

161 H. Eroglu, 'The art of Open Banking regulation' (Finextra Blog, 28 August 2018) <https://www.finextra.com/blogposting/15715/the-art-of-open-banking-regulation> accessed 20 October 2023.

5.1 Lessons for Nigeria

Although many emerging nations value the UK's approach, they believe it is too rigid and inflexible to meet the unique requirements of the African financial system.[162] However, this does not dispute the fact that when developing and implementing its open banking strategies to ensure a balance between innovation and the need to secure the protection of consumers' data, Nigeria can learn a few lessons from the UK's open banking regulatory framework, and they include:

1. **Improved Regulatory Oversight:** Clear regulatory monitoring and oversight greatly enhanced the UK's open banking regulatory framework.[163] Over the years, organisations like the Financial Conduct Authority (FCA) and the Competition and Markets Authority (CMA) have provided the UK's open banking system with clear regulatory oversight and direction.[164] To maintain uniformity, compliance, and accountability, it may be helpful to have a specific regulatory agency body oversee open banking activities in Nigeria. In the UK, to plan and oversee the next of open banking, the Joint Regulatory Oversight Committee, which includes the Treasury and the Competition and Markets Authority (CMA) as members and the Financial Conduct Authority (FCA) and the Payment Systems Regulator (PSR) as co-chairs, was established in March 2022.[165]
2. **Effective Technical and Security Measures:** There is an obvious lack of provisions for a unified set of technical standards and security protocols to ensure data protection in the Open Banking Guidelines in Nigeria. The Open Banking Implementation Entity (OBIE) is a dedicated implementation body, and it has established a standardized AP in the UK.[166] The UK's Open Banking Implementation Entity (OBIE) was instrumental in developing API security protocols and technical standards. To promote safe and uniform/standardized data sharing between financial

---

162 Duncan, 'Feature: How has Nigeria approached Open Banking?' (n.142)

163 Joint Regulatory Oversight Committee, 'Recommendations for the Next Phase of Open Banking in the United Kingdom' 10 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1150988/JROC_report_recommendations_and_actions_paper_April_2023.pdf> accessed 10 November 2023

164 ibid

165 Ibid, 3

166 European Commission, 'Commission Staff Working Document: Impact Assessment Report' 16 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2023:0231:FIN:EN:PDF> accessed 11 August 2023

institutions and third-party providers, Nigeria could gain by implementing similar technical standards and security measures.

3. **Innovation and Competition:** The main objective of open banking is to promote innovation and competition in the financial industry. Nigeria should support the creation of innovative financial products and services while also making sure that conventional financial institutions and new Fintech companies have an equal opportunity to compete. In the UK, the priority is the establishment of a resilient and competitive underpinning for the continuous evolution of the open banking ecosystem, with a view toward its expansion beyond its present scope and the concomitant delivery of enhanced advantages to end users.[167] This imperatively involves the fortification of the fundamental infrastructure of the ecosystem and the facilitation of novel commercial agreements, thereby engendering an environment conducive to its sustainable growth and development.[168]

   Since the technological and financial environment are both evolving rapidly, Nigeria's open banking ecosystem needs to be flexible enough to adapt to new technological developments and market shifts while ensuring regulatory stability. Over 7 million consumers and businesses in the UK use innovative open banking-enabled products and services to manage their money and make payments, of which 750,000 are small to medium-sized firms (SMEs).[169] However, there must be adequate provisions for safeguards for the protection of customers' personal data to guarantee enhanced data collection and sharing which is the cornerstone of open banking.[170]
4. **Customer Education and Awareness**: Although Nigeria just passed a data protection law, it is equally crucial to educate customers about the advantages, risks, and security measures associated with open banking. Nigeria can create educational programmes to assist people in understanding the idea of open banking, data security, and their rights to data privacy.
5. **Implementation Strategy:** A phased implementation strategy of open banking may help with risk management and enable stakeholders to progressively adapt in Nigeria. Before establishing a long-term regulatory

---

167 Joint Regulatory Oversight Committee, 'Recommendations for the Next Phase of Open Banking' (n.163) 13

168 ibid

169 Ibid, 3

170 Ibid, 14

https://doi.org/10.53982/apblj.2019.0301.04-j

framework for open banking in Nigeria, it may be helpful to outline a strategy that can be implemented in phases. The Joint Regulatory Oversight Committee in the United Kingdom has proposed a delivery strategy for open banking that consists of three phases.[171] This approach is aimed at promoting the growth and sustainability of open banking within the next two years pending when a long-term regulatory framework is established.[172] The JCA plans to improve understanding and visibility of financial crime in open banking, enhance ecosystem functionality, prevent fraud, and enable the development of commercial and liability frameworks.[173] They aim to achieve this by improving data sharing, consistent error messaging, and information flows to TPPs on API calls and payment messages.[174] The JCA expects to pilot a sustainable commercial model and new innovative business models in the following year.[175] It is submitted that the proposed three-phase delivery strategy by the Joint Regulatory Oversight Committee (JCA) can serve as a valuable template and source of strategic insights for Nigeria. The UK's phased approach to open banking regulation can provide Nigeria with a roadmap to tailor its regulatory framework, improve security, enhance ecosystem functionality, and enable the development of sustainable business models. By learning from the UK's initiatives and strategies, Nigeria can foster growth, sustainability, and resilience against financial crimes in its open banking ecosystem.

7. **Effective Enforcement Mechanisms:** To ensure financial institutions and third-party providers comply with data privacy laws, it is important to conduct routine audits and compliance checks. Penalties for non-compliance ought to be severe enough to discourage any negligent conduct. In pursuit of industry-wide compliance with prescribed standards and guidelines, it is submitted that the main regulator of open banking in Nigeria, the CBN undertakes the ongoing task of vigilantly monitoring and aggregating data pertinent to open banking ecosystem performance in Nigeria, as is envisioned in the UK.[176] Furthermore, the CBN should take on the pivotal role of providing and upholding critical services and

171 Ibid, 6
172 ibid
173 ibid
174 ibid
175 ibid
176 Ibid, 18

technical infrastructure, thereby sustaining the industry's alignment with established benchmarks. [177]

6.0 Conclusion

It's important to understand that absolute privacy might not be achievable in an open data-sharing environment. However, by improving regulatory oversight, and effective technical and security standards, employing robust safeguards, fostering user awareness, and continuously striving to minimize breaches, Nigeria can create a balanced open banking system that prioritises both innovation and privacy protection. By doing this, the banking sector can profit from open banking while maintaining the trust of its customers. While acknowledging the commendable progress represented by the Central Bank of Nigeria's (CBN) Guidelines, it is discernible that certain shortcomings become apparent when juxtaposed with the regulatory frameworks of the United Kingdom (UK). These identified lacunae possess the potential to exert a palpable influence on the realms of data security, and protection, and erode customer trust in the system.[178]

[177] Ibid
[178] ibid