POSITION PAPER

BY THE

GOVERNING COUNCIL

OF

THE CHARTERED INSTITUTE OF BANKERS OF NIGERIA

ON

OPEN BANKING IN NIGERIA

POSITION PAPER ON OPEN BANKING IN NIGERIA

TABLE OF CONTENTS

REPORT OF SUB-COMMITTEE ON POSITION PAPER ON OPEN BANKING IN NIGERIA

1.0 What is Open Banking?

Open banking is regarded as one of the most significant recent technological developments in retail finance where third party firms (FinTechs and others) access consumers' data and offer various services. Open banking involves the transfer of data held by banks (data transferors) to third parties (data recipients) to allow the data recipient to provide a service to the consumer.

"Open Banking enables personal customers and small businesses to share their data securely with other banks and with third parties, allowing them to compare products on the basis of their own requirements and to manage their accounts without having to use their bank" (Open Banking, 2017).

Functionally, open banking is about how banks can share customer data with 3rd party providers or FINTECH organisations (i.e. Services, functionality and data) with the consent of the customer, in a secure and resilient way.

It represents a significant revolution in retail banking driven by technology-enabled innovation, changing consumer preferences and regulatory changes. In the past, banking model was a closed one where a financial institution retained and controlled the information it collected about its customers. Presently, this has evolved into an open model that focuses on the portability and open availability of customer data, including transactional information. It has the potential to change competition in the sector and also bring about liberalization in the creation of new products and services based on that information gathered from customer data.

The focus of open banking is to enable customers share their financial data between their financial institution and third party providers (and between financial institutions), typically through the use of Application Programming Interfaces (API). APIs are set of routines, protocols and tools for building software applications. APIs can also be defined as a method of communication between software application and components without a required need to understand or know the entire application structure. Application Programming Interface would only interact with the functions or services exposed to it

2.0 The Opportunities and Benefits

A brick-and-mortar retail bank has its own products, back-office operations and distribution channels (such as branches, contact centers, and digital channels). The emergence of financial technology (FinTech) in general coupled with regulatory drive for more competition are disaggregating and opening the banking closed value chain. In the open banking world, participants can specialize in one or more sub-steps of the end-to-end process. That allows banks to focus on areas where they have a clear competitive advantage and leverage the scale and efficiency that partnerships with other players provides. Consequently, open banking allows financial institutions to specialize in the specific segments of the supply chain.

Therefore, the potential benefits of open banking include improved customer experience, new revenue streams, and a sustainable service model for traditionally underserved markets thereby enhancing financial inclusion which is expected to boost economic growth. It could also give customers a more detailed understanding of their products and help them find new ways to add value and make the most of their money. The resultant offering of

new products and services to customers and small to medium-sized businesses will in turn increase competition, lower prices through cheaper and easier payment systems and boost economic activities .

3.0 Rationale for Open Banking

Data is powerful. With the help of modern technologies, it helps organisation understand human behaviour. Financial services firms use data to assess a borrower's likelihood of repaying loans, financial position and goals and purchasing preferences. Consumers can also use data to understand their own behaviour and interests. Empowering consumers to make better decisions is appealing both to help protect consumers' interests and to drive more robust competition.

Consumers have a 'comprehensive right' to their data. Among this right's many components would be the ability for consumers to request and direct the transfer of their data from a data transferor to a third party. This right would enable consumers leverage the power of their data from across the economy. Economy-wide open data could see consumers empowered to exercise better choices in areas such as telecommunications, energy, social media, consumer goods as well as financial services.

The availability of Bank data could help drive innovation. Service providers may develop innovative ways of understanding and improving financial behaviour and outcomes. Because data is valuable open banking could underpin the business models and practices of new and existing firms. Being able to use the data that others have collected would clearly lower barriers to entry for a range of actors, large and small. In doing this, though, the transfer of data from one competitor to another (at the consumer's request) could see a basis of commercial advantage shifted, potentially without a corresponding value transfer.

4.0 The Challenges and Risks

Generally, all FinTech-based disruptive applications create new value for consumers of the financial services and new opportunities for both incumbent and non-incumbent companies. However, it also creates new challenges and risks to both incumbent players, regulators and the economy as a whole. The whole system is trying to understand how to properly supervise the emerging solutions, encourage innovation and collaboration while adequately protecting consumers of the relevant service.

Another challenge is due to the fact that the ability of open data to help consumers and change markets is largely unproven in practice. For example, in the UK where open banking is the most advanced, research by Accenture Payments concerning the attitudes of UK consumers indicates about 70% prefer to trust a bank with their data. This indicates that the propensity of consumers to share data outside of banks may be relatively low.

Open banking promises a great deal of benefit to end users as well as to banks and nonbanks while ushering in an entirely new financial services ecosystem with significant overhaul of banks' roles. Some of the issues that arise concern regulation of this emerging concept and data privacy, which led to why several jurisdictions took varying approaches to governance. That has led to the disparate levels of progress.

Specifically, open banking can present many regulatory challenges. First, there are several security and privacy concerns since it is based on the sharing of highly sensitive personal data across many platforms. Second, open banking would potentially involve the dissemination of personal bank data through actors that sit outside the regulated banking environment. This means that bank-level data security requirements may not apply to data that

consumers have hitherto trusted as secure. Although such actors might not be regulated, if data is being sourced from a regulated entity then such entity should be mandated to extend any due diligence being conducted to include compliance by these actors with Data Privacy (DP) rules and have policies and controls that ensure the right degree of attention is being paid to DP security. These actors will be indirectly regulated by issuing a regulation to the regulated entities. Third, a major threat of all internet-enabled applications is cyber risk and security vulnerability which could undermine the entire ecosystem.

5.0 Types and Models (Considerations for Implementation) of Open Banking

Open banking could be implemented through several models, which include the dimensions of how consumers could benefit from open banking, the data sets that should be opened up, mechanisms for transmitting the data and possible regulatory frameworks. Therefore, there are many permutations for open banking.

5.1 Use Cases/Data for Open Banking

The consumer use cases in increasing data complexity for open banking are:

i. **Generic comparisons of products/services**
   Consumers could compare fees and interest rates across bank products and services. The comparison would not take into account the consumer's individual circumstances
ii. **Personalised comparisons of products/services**
   Consumers could use data concerning their individual circumstances to identify the product or service that might best meet the consumer's specific needs (ie product use disclosure)
iii. **Basic financial management**
   Consumers could use point-in-time data concerning their income and expenses to identify ways of saving more money
iv. **Complex financial management**
   Consumers could use real-time data concerning their income, expenses and exposures to continuously understand their financial position in detail (e.g. categories of spending, benefit of offset account on mortgage, projected savings/deficits)
v. **Apply for credit**
   Consumers could use point-in-time data concerning their income and expenses to support an application for a loan

Some common use cases that have not been included are know-your-customer (KYC) assessments, account switching and consumer purchasing propensity analysis.

5.2 Transfer mechanism

These use cases could be facilitated using product attribute data delivered through public APIs and summary transaction data delivered through either direct transfer of a CSV file to a data recipient or permissioned API. There are four basic transfer mechanisms that could be used to send the data from the data transferor to the data recipient. These are arranged below from simplest to most complex. Another transfer mechanism that could be possible is the blockchain but may take substantial effort to establish.

i. Download CSV file of transaction data

The simplest way of getting transaction data to consumers is to allow them to download a CSV file of their transaction data from their secure internet banking portal. This is already being done by several banks for their customers. The data could be sent by the customer to a third party data recipient.

This transfer mechanism can support the use cases of personalised comparison and basic financial management. However, it should be noted that CSV files are capable of being manipulated. Therefore, this method is not ideal when data integrity is a vital goal.

ii. Transmit CSV file of transaction data

Banks could amend their internet banking function to allow consumers to transmit the file to a third party data recipient instead of the consumer downloading a file to their home computer. The bank data transferor would send the file directly to the data recipient via secure file transfer protocol once authorised by the consumer.

For this mechanism to work, the bank as the data transferor presents consumers with a list of authorised data recipients. The regulatory framework could include a registration mechanism whereby data recipients need to hold a licence. Banks could use this licence to know which data recipients are safe to list.

In this option, there is no need for the consumer to do anything more than specify who they would like to receive their data. It would also remove the risk that data is compromised while on the consumer's home computer or mistakenly sent to the wrong party by the consumer.

Again, this type of mechanism would support the use cases of personalised comparison and basic financial management.

iii. Public API

A public application programming interface (API) would allow any entity to develop software that can access and download the data. The standards for the API would be publicly available. Third party developers could use those standards to write programs to access and then incorporate the data in their offerings.

Public APIs would allow banks to continuously make their product attribute data available and update it as they see fit. This would enable both generic and personalised comparisons by allowing product/service comparison sites to display the current offerings from banks and others.

iv. Permissioned API

APIs could be used to expose transaction data if they were structured to only allow authorised data recipients to access designated data packets. In addition to the API, a system would be needed to accredit data recipients in respect of specific data packets from specific customers who have consented to the data recipient accessing the data. This form of mechanism would likely be necessary to enable complex financial management use cases that depend on real-time access to consumer bank data. However, an API designed to grant real-time access to consumer bank data will heighten exposure to cyber security risk to the Bank, measures to mitigate such cyber security breach risk should be first considered before adoption in Nigeria.

6.0 Why API

APIs can be seen as interfaces between software applications, both within as well as between organisations. In their simplest form, APIs are standardised sets of requirements that govern how one software application can talk to another. More specifically: APIs enable communication between software applications where one application calls upon the functionality of another application.

The growing interest in API technologies and open banking may be seen in the light of a need to resolve the mismatch between reach and conversion, i.e. a lack of a connection between the services and the payment/banking infrastructure layers. Digital companies (e.g. Amazon, Google, Twitter, Facebook and Apple) and also increasingly banks, seek to connect with innovative firms outside of their organisation to deliver attractive services to their customers, when and where the customer needs them.

In the past decade digital companies outside of the financial industry (e.g. Amazon, LinkedIn and Twitter) have proven this strategy to be successful. Many traditional business models across a variety of industries have already experienced dramatic and positive change driven by APIs.

Successful APIs are based on a good governance model. Recent years have seen the number of industry initiatives with the aim to create standards for APIs grow in the payments industry. Some of the main initiatives include:

i. The UK Open Banking Working Group, UK, set out an Open Banking Standard to address technical design and infrastructure issues, as well as formalising an approach to sensitive customer issues such as consent, delegation of access rights, authorisation and authentication, vetting, accreditation and governance. There are 121 parties involved with diverse backgrounds.
ii. The CAPS framework consists of three layers: PSD2 Layer (TPPs can connect to many AS-PSPs through one API standard, banks are compliant with PSD2 regulation). Founding members are Equens SE, Nets and VocaLink other members: SIBS, PayPal, Fidor, Bankgirot, Isabel Group, Open Bank Project.
iii. Open Bank Project: Open API and App store to build innovative applications and services based on the account holders' transaction data. Founded by Simon Redfern and led by TESOBE.
iv. Open API initiative: Open, technical community that focuses on creating, evolving and promoting a vendor neutral, portable and open source description format. It was Created by a consortium under the Linux Foundation.
v. Open Financial Exchange (OFX): Standard to allow exchange of data between software and banks. Enables features such as access to transaction data, initiating payments and transfers, and recently multi-factor authentication, but does not support secure third party delegation. It was a US – Created initiative in 1997 by Microsoft, Intuit and CheckFree. Aimed at the US and supported by over 5500 banks and brokerages.

7.0 Issues to Resolve for Open Banking in Nigeria

1. How can the scope and understanding of consent be developed?

Consumers must be educated to understand what they are consenting to and the consequences of providing that consent. The devil is in the details, however. What knowledge does the user need to be considered educated? Who should provide that education? What responsibilities does the user have to become educated?

2. Should the consent process be standardized?

Terms and conditions must be clear, simple and not misleading. Consent should be retractable at any time. There should also be a way to make sure that consent is sustained throughout the use of the consumer's data. In order words, the consumer must be at the centre of the process and it must be beneficial for them. It should also be clear what the consumer is consenting to: is it the business model or the data transaction for the data to be shared with the third party. The contentious area was on how standardized the consent process should be between apps.

A standardized consent process would make it easier for the end user to know what they are consenting to. It should be noted that standardization could suppress innovation. Nevertheless, the medium for providing consent should also be made easy and seamless.

3. Should a "white list" of authorized players that have met a required level of standards proportionate to the nature and size of the product or service be created?

An 'authorised' white list could be created by a regulator, which would hold a list of firms that are regulated and will set the rules and implement sanctions if these are not followed. Would the white list take into account financial soundness of the company? How would it address privacy and security? Authorized players would need to adhere to privacy and security standards, but what are those standards? Who makes sure these are followed?

Whilst 'authorised' white list is highly encouraged in order not to stifle innovation, allowance should also be made for those who do not fall into this bucket and whose services the customer's risk appetite is able to permit access to data due to their service need. However there can be a restriction on the level of information that would be made available i.e extent of Personal Information available can be tiered.

4. Should we consider consumer data rights (eg "open data" more broadly) where Open Banking is the first use-case?

There are complexities around what data and applications are in the scope of Open Banking. Should Open Banking be restricted to payments, as in some other jurisdictions (noting that these jurisdictions may add use cases in the future, with Australia already publishing a time-table for delivery)? With Open Banking, Nigeria could use the opportunity to develop an *Open Data Consumer Rights Act*, where Open Banking would be its first use-case. Should the government rather be considering Open Data policy more broadly, where Open Banking is simply one portion of a larger Open Data discussion?

8.0 Country Experience

Given that the pace and scope of open banking reform differs by jurisdiction, it is helpful to look at several different ones on an individual level.

The **European Union** has been quick to adapt to change. The EU is looking at expanding Open Banking to functions beyond simple payments. They strive to ensure consumer protection. Since May 2018 the EU has been implementing a new Data Protection initiative. In Europe, the Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR), which have been designed to regulate financial innovation, are driving Europe towards an open banking standard. Specifically, PSD2 enables bank customers to allow third-party providers access to their account data, which, for example, could enable third-party providers to manage a customer's finances. The **European Banking Authority (EBA)** has released an Opinion and draft Guidelines to provide clarity to market participants on the implementation of the technical standards on strong customer authentication and common and secure communication under PSD2. A number of jurisdictions have either mandated or encouraged open banking.

The **United Kingdom** has also been actively mandating open banking, pursuant to an order from the Competition and Markets Authority (CMA) requiring the UK's largest banks to share customer data with third parties. The Financial Conduct Authority (FCA) has recently stated that they plan to consult on changes to their guidance and

rules to reflect the recently issued EBA Opinion and draft Guidelines. The UK has taken the lead in open banking initiatives, in producing an open banking framework that could enable the open banking standard in the UK. This has also prompted the CMA to draft the recommendations in its final report released in 2016. According to the report, large banks are to adopt and maintain a common standard for open APIs, to address the lack of innovative and competitive products in the financial market. For the UK, the new directive set out by the CMA will force the country's nine biggest banks to share customer data (with permission) to third parties. Open Banking forces the UK's nine biggest banks – HSBC, Barclays, RBS, Santander, Bank of Ireland, Allied Irish Bank, Danske, Lloyds and Nationwide – to release their data in a secure, standardised form, so that it can be shared more easily between authorised organisations online.

Open Banking has been implemented in **Australia** since November 2017 and is already undertaking a review process. Banks and large financial institutions have already announced initiatives to increase data sharing and expand services with Open Banking. That was following its review into open banking, but in this case as part of a broader move to implement a Consumer Data Right "to give Australians greater control over their data, empowering customers to choose to share their data with trusted recipients only for the purposes that they have authorised". The Consumer Data Right will be implemented first in the banking industry followed by the energy and telecommunications industries, and thereafter followed by other industries.

In **Hong Kong**, the Hong Kong Monetary Authority has issued an Open API framework for public consultation.

Japan has introduced legislation on open banking.

In **Singapore**, instead of mandating open banking, the Monetary Authority of Singapore (MAS) has been encouraging financial institutions to develop APIs openly so they can work with service providers to enhance customer experience. Singapore is attempting to implement a different type of regulatory framework, with a less aggressive and more organic approach. It is not planning on forcing regulations on financial institutions. The Monetary Authority of Singapore will be working towards guidelines for ethical usages of data and artificial intelligence that would work for all players within the ecosystem.

Other markets such as the US, Latin America and Asia have been experimenting with open banking in pockets and have expressed strong interest in pursuing technological advancements in the financial services industry.

9.0 **Analyses of the implications and challenges of confidentiality and security breaches of customer data privacy**.

We are in a global world where information sharing is inevitable, but sharing customer's financial information with third party companies must be done with great caution.

It is the believe in the recent days that important data breaches only happen via the electronic channels and the figures tend to bear that out, credentials are being bought and sold on the dark web. Cyber-attack is also in rampage where hackers use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.

It was published on the Techworld (https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/) websites that Tesco Bank, the consumer finance wing of the British supermarket giant on the 1St of

October 2018 paid a fine of £16.4 million for breach of customer data which led to over 20,000 customers had money stolen from their accounts, well over 40,000 accounts were compromised.

Every new innovation comes with its good and bad sides, the concept of Open Banking is not an exception, and most organizations did not have Open Banking in mind when they designed their APIs and security platforms. They now need to find secure ways to expose their APIs, many of which are likely running on top of legacy platforms, FIs will have to overhaul their systems and processes if they don't want to cease to be competitive.

Indeed, with the advent of Open Banking innovation, FIs will need to collaborate and partner with FinTechs companies which will lead to FIs exposing large amount their customers' data (customer's information and financial data), as such is a great need to increase security and structure surrounding the transfer of data between partners (FIs and FinTechs) an harmonized regulation/policy would be required for Nigeria. In Europe, the most recent regulation on open banking is PSD2 (Payment Service Directive version 2).

PSD2 (Payment Service Directive version 2) mandates that financial institutions (FI) must enforce Strong Customer Authentication (SCA) when customers perform certain actions and this includes Open Banking.

Typically, when considering authentication mechanisms we consider three factors: knowledge (something you know), possession (something you have) and inherence (something you are).

The FIs in Nigeria put partnering with FinTechs in their strategy, however, for FIs customer to really embrace the conception of Open Banking, FIs need to do the following:

a) Gain Customers Loyalty – by improving customer experience
b) Build customer's trust – In case of fraud, will the FI still be standing
c) Attract customer buy. – Once (a) and (b) in the above is cleared, the rest is business as usual.

10.0 **Customer's Protection**

Digitalization will shape banking into a lifestyle platform for its customers. Insights from data gathered through voluntary user sign up or opt in processes are harnessed to drive engagement and customer experience through the entire banking product lifecycle. The advent of open banking would expose some laxity in our data protection and data privacy laws. Banks would have to collaborate with third party providers thereby exposing the banks, customer and even the nation to various security risk and threats such as;

1. Customer vulnerability to identity theft and fraud
2. Customer get targeted with unsolicited messages and spam due to abuse of information shared to 3rd Party Providers
3. Bank system and security compromise
4. Reputational damage is inherent for the banks
5. Customer distrust and loss of customer confidence in Banks

6. Ransomware targeted at customer account lockout through compromised 3rd party providers
7. Denial of Service (DOS) attacks
8. API Injection attacks
9. Authentication/Session compromise

These risks can be adequately mitigated through;

1. Adoption of API standards between Banks and 3rd party providers
2. Multiple Factor Authentication
3. Predictive risk analysis of behavioral pattern
4. Adoption of Unified Data Privacy and Protection Law
5. Compliance with standard security management framework for data sharing and processing
6. Adoption of a standard industry-wide cyber defense approach and threat intelligence
7. Enforcing a regulatory and structured approach to operation by the FINTECH companies i.e. Corporate Governance
8. Adoption of standard access control protocols for authorization
9. Continuous User Education and Sensitization by banks on the implications of open banking products and services.

Data shared with 3rd party providers by banks shall be initiated by the customer and only data points consented to by customer are shared.

Bank shall keep consent approval from customer for audit purposes.

Customer can easily opt in or out of any 3rd party provider service with option to request for data purge from the 3rd party provider platform, in cases where shared data are stored.

Banks must ensure 3rd party provider operations, adhere to stipulated security standards with constant monitoring and independent audit carried out periodically. A certification with a renewal cycle is proposed.

11.0 Benefits of Open Banking and Other Ways in which the Banking Industry could Advantageously Exist in the Financial Technology Space.

Open Banking innovation comes with lots of benefits depending on the use cases adopted. The primary beneficiary is the customer, with more options to access their financial information on bank agnostic platform, get actionable insights and choose the best fit or fit for purpose services without entering a banking hall or interfacing with bank staff.

Open Banking gives the customer full control of the products they want and the choice to access it through their desired 3rd party provider. A few use cases for open banking which would be beneficial to customers are;

1. Cash access through mobile device

2. Card-less transaction
3. Voice assisted payments through voice assistant such as Alexa, Siri
4. Robo-advisors/Finance advisors

Banks have been custodian of customer information but with little or no innovation around these data. The banks have become Data Rich but Insight Poor creating product and services which are not tailored to the need of their customers. Banks would need to change the narrative by analysing customer data, identify behavioural financial/service patterns, and creating products/ services that best fit the customer's profile.

'However, the major opportunity of Open Banking is enabling a sharing economy, that would not only serve or be beneficial to financial services but other sectors like supply chain, education, healthcare, trade finance, ecommerce etc.' (Samiksha Seth).

12.0 **Security Implications and Standards of Operation for Fintech Companies**

Protecting customers' interests in open banking ecosystems requires a defined structure for the Fintech companies that suitably mitigates the involved operational risks and provides compensation to customers in case of breaches. The following are structure that should be adopted.

- Provision of a regulatory body for third party companies involved in the open banking ecosystem. If no new regulatory body can be carved out, the Fintech companies can be designated under the regulation of either the CBN or NDIC.
- Third-party service providers to undertake security, data protection and business continuity policies, procedures and controls that are consistent with these already in place in the financial sector and proportionate to the services provided and the information accessed.
- Third-party service providers to hold adequate resources to deal with customer damages that result in financial losses. These resources can be in the form of operational risk capital like their FI counterparts or it could be in the form of professional liability insurance or some equivalent guarantee. The resources is termed adequate if it commensurate to the number of customers, the volume of operations and the type of rendered.
- Provision of complaint platform by Fintechs for aggrieved or unsatisfied customers to remit their grievances. In addition, an auto escalation process to be incorporated in cases where the issues are not resolved within a defined time frame. The escalation should be to the regulating body in charge of the FinTechs and possible to the involved banks that provided the funds.
- Provision of a standard procedures to resolve potential disputes between all acting parties, including between financial institutions and third-party service providers when there is a disagreement over the responsibility of an unauthorized transaction or defective payment. Considering that the target customers may not have the ways and means to fight in a situation of unauthorized use of the shared data, the framework for the arbitration of dispute and penalty burden of unauthorized use of the customer data should be clearly spelt.

13.0 **Legal Implications of Open Banking in the Financial Services Industry in Nigeria**

The key threat to open banking is its security vulnerability. This is fueled by lack or inadequate legal framework to guide the process, protect payment initiation and account information, among others. Hence there is a need for a clearly define statutory direction as well as contractual relationship between parties with defined process of redress.

13.1 Contractual Relationship between parties

The concept of Open banking infringes on some other legal principles and there is need to guide against issues that could emanate from such. For instance, Open Banking works contrary to the policy of confidentiality between a bank and customer which is jealously entrenched in various Statutes, Guidelines and Codes, etc . The solution to this, in the interim is a clear, well understood agreement between the bank and customer granting the bank right to share the customer's data with a third party.

In addition to Agreements, there should be clearly worded guidelines/ terms and condition for the relationship, providing obligations, protections and redress.

13.2 Existing Data Protection Statues

Relevant Data Protection Statutes and their applicability to Open Banking in Nigeria

i. Constitution of the Federal Republic of Nigeria

Section 37 of the Nigerian Constitution (1999) provides that "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected".

However, neither detailed nor specific provisions exist with regard to the protection and privacy of financial data of the country's citizens.

ii. National Information Technology Development Agency Data Protection Guidelines

The National Information Technology Development Agency (NITDA) is the national authority that is responsible for planning, developing, and promoting the use of information technology in Nigeria. NITDA was established by the National Information Technology Development Agency (NITDA) Act, 2007 as the statutory agency with responsibility to develop information technology in Nigeria

In performing this duty, the NITDA issues guidelines which prescribe the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for information.

Section 1.3 of the Guidelines state that "these guidelines are mandatory for Federal, State and Local Government Agencies and institutions as well as other organizations which own, use or deploy information systems within Federal Republic of Nigeria"

Also by virtue of section 4 of the Guidelines, all Data Controllers are required to implement technical and organizational measures to ensure security of personal data.

The Guidelines however lacks authenticity and originality and seems to be a miniature version of the EU General Data Protection Regulation (GDPR) as it fails to take into account, the peculiarity of the Nigerian technological space. The Guideline also fails to clearly state if NITDA will act as the supervisory authority, coupled with the fact there is no penal or administrative fine regime for violation.

iii. Cybercrimes Act 2015

The Cybercrimes Act 2015 is the first legislation in Nigeria that deals specifically with cyber security and focuses on crimes in which a computer is the object of the crime or is used as a tool to commit an offense.

The Act places a duty of care on financial institutions and service providers to ensure the protection of confidentiality and the verification of transactions.

However, the Act is too ambiguous in its reach as it makes provisions for vices such as; identity theft, child pornography offences, Cyber-stalking, Cyber-bullying racist and xenophobic material but is lacking when required to pointedly address open banking issues.

iv. Digital Rights and Freedom Bill 2016

Another key dynamic in the fight for data protection, will be the Digital Rights and Freedom Bill which has been passed by the House of Assembly and awaiting presidential assent. The Bill, if enacted into law will offer a better protective shell around data handling, collection and use in Nigeria.

The Bill seeks to minimize unwanted and undisclosed surveillance of individual's communications, as well as guarantee confidentiality of personal data and information of citizens. Other key areas touched on by the proposed Act include; identity protection, periodic accountability, monitoring and surveillance and whistle blower protection.

The Bill has however been described as lacking interoperability that would give it locus for global competitiveness, as opposed to a more comprehensive coverage in the mode of Europe's GDPR. Other shortcomings of the Bill include; ambiguity and utilization of many undefined terms as well as any provision that addresses the obligations of Data controllers, Processors and Service Providers on the issue of Data Breach.

v. Proposed Guidelines for the CBN

The financial industry is currently awaiting an exposure draft of the framework on open banking from the Central Bank of Nigeria, which would supposedly include the roles of the banks, fintechs and other players in the sub-sector as well as the risk management system.

CBN and banks still need to come up with a framework for data classification and sensitivity that would help the customers to determine the extent and amount of data they would like to share with a third-party.

vi. Inclusion of Electronic Evidence in the Evidence Act 2011

It is significant to note that in a bid to keep abreast of various advancements in information and communication technologies, the Evidence Act, 2011 was enacted with a view to correcting some of the difficulties encountered in the admissibility of electronically generated evidence.

To this end, Section 84 of the Evidence Act 2011 provides that a statement contained in a document produced via a computer, which statement is relevant to the facts in issue, is admissible as evidence. While, Section 258 (1)(d) of the Evidence Act, 2011 defines a document to include "any device by means of which information is recorded, stored or retrievable including computer output".

The Act only catered for admissibility of electronic document which is just a very small part of the legal requirement of Open banking.

vii. Proficiency of Judges in handling Financial Technology Disputes

In light of the impact of Information and Communication Technology on the Law and Court Process as well as the sensitivity and technicality of Open Banking and financial technology as a whole, there is need to ensure that Judges are stoutly equipped to take on the rigors of adjudicating on Fintech related disputes.

To this end it is of utmost importance to ensure that Judges undergo requisite training to adequately equip them for the task.

As alluded to above, even though statutes like the Constitution, NITDA Guidelines, Cyber-Crime Act and the proposed Digital Rights and Freedom Bill all possess clauses that serve to enhance security and confidentiality of data, the overwhelming view is that none of the aforementioned exhaustively tackles the intricacies and challenges associated with Open Banking but instead focus on the telecommunications industry.

For adoption in Nigeria of open banking, there should be first an amendment to address the deficiencies identified on the above legal frameworks in Nigeria, more importantly the NITDA Guideline to provide for penal or administrative fine regime for violation.

14.0 Recommendations

i. The consumer must be the focus of open banking. A well-designed system of Open Banking puts the consumer at the centre of their information through increased transparency and the introduction of new products that will lower costs, give consumers more options, and enhance global competitiveness and accelerate innovation.

ii. Consumers must provide informed consent before any data is shared and must have the ability to retract consent at any time.

iii. The data security risks of open banking need to be managed

iv. An evolving financial services market may create new or enhanced risks, understanding that some of the risks are unknown; government, the private sector, and consumer advocates should collaboratively develop mechanisms to mitigate and reduce risks.

v. Economy-wide open data should be the end-state of open banking. Open banking should be used as a short-term pathway towards safe economy-wide open data.

vi. Common standards, including API standards, must be created to ensure interoperability, avoid fragmentation and drive safe adoption. Those standards should be developed by public and private sectors collaboratively.

vii. Technical standards around authentication and data sharing should comply with ISO and global standards, as closely as possible, to match rules in other jurisdictions since the issues are universal. The template for customer data sharing should be regulator-defined and industry-uniformed.

viii. Before rules and standards are put in place, regulators must consider the impact they will have on inclusive innovation and consumer rights.

ix. When designing rules and standards, ethical considerations need to be taken into account on how data can be used.

x. Despite the impending Guidelines from the regulators, there is a need for a specialized Act of the National Assembly that focuses solely on addressing financial data protection in view of the sensitive nature of the subject matter.

xi. CIBN in collaboration with NJI should organize a well-structured training programmes for Judges by renowned Fintech experts. The Judges with the statutory responsibility to interpret and adjudicate laws should be strategically trained to handle this very important role.

15.0 **Conclusion**

Technological developments as we know are disrupting all facets of human endeavor and thus shapes, the way we live and transacts with one another. ICT in all ramifications has increased our computing ability, information availability and accessibility. Tearing down boundaries and in the wake spurred innovation that improved living standards of the citizens of the globe. These giant strides, however does not come without serious security risk and challenges.

The concept of open banking- sharing of customers financial data between financial institution and third party through the use of API interfaces is a welcome development as it has been lauded to improve customer experience, aid understanding of behavior dynamics for a sustainable service model for the traditionally underserved markets thereby enhancing financial inclusion which is expected to boost economic growth, the heartbeat of the Government. Most importantly it will lower cost and give consumers the leverage to use it in a way and manner they choose to. Also, the technology for the interface should be uniform for all the players to ensure security standard and compliance.

The downside, however, remains security challenge, seemingly trust deficit in the process and perhaps regulatory issues more especially on data privacy and cyber risk.

Finally, given the pace and scope of open banking reforms and adoption by different jurisdiction, we posit that our adoptions should take into cognizance our country's specific requirements to align with our broad macroeconomic stability. Central Bank should guide the process of instituting a framework for transparent adoption of after collaboration with key stakeholders.

We support this initiative and further add that only certified PCIDSS should be allowed to operate Open Banking in Nigeria, this is to enable the regulators guide the operators of open banking and adequately protect the industry.