GBENGA
BIOBAKU & CO
BARRISTERS & SOLICITORS

OVERVIEW OF THE CENTRAL BANK OF NIGERIA's OPEN BANKING GUIDELINES

Introduction

On March 7th, 2023, the Central Bank of Nigeria (CBN) announced the issuance of the Operational Guidelines for Open Banking in Nigeria, aligning with its mandate to uphold financial system stability and growth. These guidelines facilitate the seamless sharing of customer-authorized data between banks and third-party firms, thus fostering the development of innovative customer-authorized products and services. This change is expected to enhance the efficiency, competitiveness, and accessibility of financial services in Nigeria. Open banking is a system that provides access to financial data held by banks to third-party application developers via an Application Programming Interface ("API"). The API is a software intermediary that enables technology platforms or applications to communicate with each other. It recognizes consumers' ownership and management of data, as well as their right to issue authorizations to service providers in order to get access to new financial products and services. Open Banking has emerged as a game-changer in the financial industry, offering numerous benefits such as increased competition, improved customer experience, and innovation. But what exactly are the roles of these participants?

Open Banking in Nigeria is closely overseen by the Central Bank of Nigeria (CBN), which plays a crucial regulatory role. The CBN is responsible for ensuring the safe and effective operation of the system while also promoting competition and innovation in the financial sector. API Providers (AP) are participants that uses APIs to provide data to another participant. An API provider can be a licensed financial institution / Service provider, a Fast-moving Consumer Goods (FMCG), retailer, payroll service Bureau that shares data with other institutions, including banks, insurance companies, and other interested parties. Their primary function is to deploy and implement automated monitoring systems to evaluate their system's vulnerability and manage fraud. API Consumers (AC) are participants that use or have access to the data released by the API Providers, such as fintech companies. However, to maintain the security and trust of the system, API Consumers must actively cooperate with API Providers to ensure proper monitoring. Obtaining clear and explicit consent from the end-users (customers) for each action is a fundamental responsibility of API Consumers.

Customers are the owners of the data whose consent will be required for the release of data by API Providers to API Consumers in order to access financial services. Any unauthorized transfer without consent is a serious breach of data privacy, and API Providers and Consumers have a responsibility to ensure the security and confidentiality of customer data at all times. As Open Banking continues to gain traction in Nigeria, understanding the roles and responsibilities of the key players is crucial. By working together, the Central Bank, API Providers, API Consumers, and Customers can create a more secure and innovative financial system for all. Open banking is all about empowering customers with the ability to access a wider range of financial services and products. This is made possible through the use of Application Programming Interfaces (APIs), which allow different financial institutions and service providers to connect and share data with each other. With open banking, customers are in control of their data, and can choose to share it securely with third-party providers who can then offer personalized financial solutions. The key to open banking is customer consent, as it is the customer who decides which third-party providers can access their data. The guidelines for open banking aim to ensure that customer data is protected at all times, and that all parties involved in the process adhere to best practices for data security and privacy.

Open Banking Registry (OBR)

To promote transparency in the open banking sector in Nigeria, the Central Bank of Nigeria (CBN) is required to establish an open banking registry (OBR). The OBR shall be a public repository for details of registered participants. Each participant shall be identified by its CAC business registration number, which shall be the unique key across the OBR system. This registry serves as a regulatory oversight on participants, ensuring that only registered institutions operate within the open banking sector. In addition, the OBR would have an interface which would serve as the primary means by which API providers manage the registration of their API Consumers.

Data Governance

Open banking relies heavily on data, making data protection and compliance with regulations essential. The Open Banking Guidelines emphasize the importance of data oversight and governance, as well as compliance with relevant legal and regulatory provisions. However, the relevant laws applicable for Open banking are the laws on data protection, consumer rights and fair practices such as the Nigeria Data Protection Regulation 2019, which is particularly relevant for open banking. This Regulations ensure that a customer's personal data is protected and used responsibly by all parties involved and this includes obtaining, holding, use or disclosure of such information to protect such information from inappropriate access, and use.

To ensure the protection of data, the guidelines stress the necessity of using the best data security standards possible. All parties engaged in open banking must implement robust security measures to prevent unauthorized access or disclosure of data.

Consent Management

In the world of open banking, your consent is critical. Without it, banks, providers, and consumers can't share or receive data. That is why the Open Banking Guidelines emphasize the importance of customer consent when it comes to accessing open banking products and services. The Guidelines state that consent must be obtained from customers whose data is needed to enable them to access open banking products and services. This means you have control over who can access your data and for what purpose. It also places a responsibility on all participants in the open banking sector to comply with the provisions highlighted. This includes banks, providers, and consumers of APIs.

Consent Management Stages

It is the responsibility of all the participants to provide protection to customers. However, the customer has to consent to using the interface. The framework outlines the stages of consent management; it includes the consent stage, authentication stage and authorization stage. The consent stage highlights the need of informing consumers about the type and purpose of data sought, and notifying clients precisely of the time-bound permission offered. The guidelines emphasize the need of communicating with clients in a clear and concise manner. The authentication and authorization stage ensures secure access to customer data. Key points include requirements for authentication mechanisms (biometrics, email and OTP), customer authentication method (multi-factor authentication), and guidelines for authorization processes. The guidelines emphasize the importance of providing customers with clear and concise information about data access, as well as ensuring that customers are able to easily enable or revoke permissions for account access. Overall, the guidelines strive to ensure that customers are adequately informed and in control of their data, and that access to customer data is safe.

Service Level Agreement

The Open Banking Guidelines requires that a Service Level Agreement (SLA) should be executed between API Providers and API Consumers to govern their relationship. The SLA provides a framework for resolving inconsistencies. The SLA should make adequate provision for adopting accounting and settlement practices such as recording of all operations involving the movement of funds within the API provisiders' domain at the account level of the API consumer. And maintain separate principal and fee collection accounts. API Providers and Consumers are responsible for monitoring their hardware and operating systems at a functional level and collecting performance metrics for all API transactions, which must be stored. In the event of inconsistencies, monitoring processes must be in place to alert support personnel and identify suspicious occurrences. All participants are mandated to state their respective fees in the SLA and publicly disclose it on their websites and applications. The SLA should also include the roles and responsibilities of participants and third parties, which must be carried out diligently. Participants are mandated implement event - triggered billing systems to ensure that bills are easily traceable to the activity performed per transaction. This ensures that participants are accountable and transparent in their dealings, and that customers can trust the open banking system.

Incident Management & Problem Management

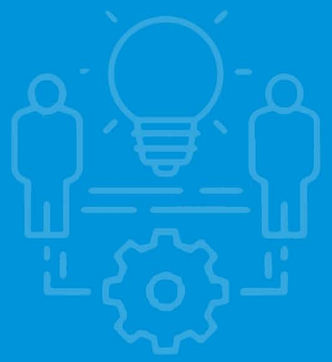
Incidents can happen in any system, but how do you classify them? The Open Banking guideline lays out three classifications of incidents and their corresponding response times. Here's what you need to know:

1. **Functional:** These are incidents that affect vital system functions, this is referred to as "systemic". One of such incidences is the authentication procedure, which may usually be identified by the occurrence of declining metrics. When this happens, the reaction time to the incident is 2 hours, with a resolution time of 4 hours.

2. **Performance:** These incidents affect service levels, such as declining transactions or fluctuating availability. When this happens, the reaction time to the incident is 30 minutes, with a resolution time of 2 hours.

3. **Systemic:** These are incidents that affect the API infrastructure or major system functions, leading to unavailability. When this happens, the response time to the incident is 15 minutes, with a resolution time of 30 minutes. In today's digital world, incidents can happen at any time, particularly in the financial sector. When it comes to open banking, it is crucial to have a clear plan in place for managing incidents. According to the open banking guideline, the first step is to evaluate the impact of the incident before notifying affected parties via the specified communication channel. The API providers and consumers should then work together to evaluate the failover system and restore the service as quickly as possible, with a maximum downtime of Thirty (30) minutes. Finally, a thorough investigation should be conducted to determine the root cause and take appropriate measures to prevent similar incidents from happening. It is crucial that all API Producers/Consumers adhere to the guidelines provided for, especially in the event of an incident. Prompt and effective incident management is essential to maintain the integrity and security of the Open Banking system. To this end, the following guidelines should be adhered to in the event of an incident:

- Create and regularly test an incident response plan
- Provide skilled personnel to monitor and support Open Banking API infrastructure on a 24x7 basis
- Provide contacts of the relevant personnel to API Providers/ Consumers within SLA documentation
- Design and review on a quarterly basis an incident management and response manual on a quarterly basis indicating failover and failback steps to be undertaken for a critical incident.
- Maintain an incident manual with lessons learned from previous critical incidents.



As open banking continues to reshape the financial industry, it is important to have a clear understanding of the metrics provided by API Providers/Consumers. These metrics include 'msg_validation_time' which measures the average time it takes to validate a message, '%_approved' which tracks messages that have achieved their intended function, and 'avg_log_time' which measures the average time it takes to log API calls. With these metrics, API Providers/Consumers can ensure that their services are running smoothly and efficiently. However, when incidents occur and fail to resolve within the SLA, there are further options available. These options involve creating a problem register that outlines the details of the incident and its solutions, including interface requirements, change management, communication management, and reports for both API consumers and customers. By understanding these options and metrics, participants can take proactive measures to ensure the success of their open banking services.

Anti-Competition Practices

The Open banking guidelines not only promote fair and ethical practices in the industry but also address instances of competition. This ensures that all API providers and consumers maintain professional standards and avoid unethical practices such as de-marketing. In the event of the termination of a relationship, a 20-day notice must be given to the other participants. However, in cases instant disconnection due to fraud, API providers must provide a report justifying the disconnection to API consumers within two (2) business days.

Data Ethics

The usage of customer data for illegal activities has become widespread. However, the guidelines state that data should be managed properly and in accordance with regulatory requirements. The regulatory framework should include principles for collecting, analyzing, and exchanging personal data. It is also crucial to bear in mind that data ethics includes the ability to protect client data; this is known as data privacy. Considering it is critical to protect customer data, API providers/ API consumers must comply with the Nigerian Data Protection regulation or any CBN-issued data protection regulation.

Cybersecurity and Data Breach Policy

Safeguarding data is critical in open banking, and failure to do so can have devastating consequences. That's why the open banking guidelines provide detailed measures to ensure the security and protection of data. To prevent data breaches, API consumers must conduct regular staff vetting, implement strong passwords, and provide appropriate staff training. In addition, the guidelines mandate that APs / ACs provide a comprehensive data breach policy that covers prevention, preparation, assessment, containment, communication, review, recovery, and testing of data incidents. Regular risk assessments and incident analysis are critical in preventing data breach incidents in the future. By implementing these measures, API consumers can ensure that data security is a top priority and that customers can trust their services with confidence.

- With regards to cybersecurity, API Providers and consumers are to ensure the following:
- Entrench an appropriate risk management regime;
- Have a secure configuration management system;
- Ensure network security for all connections;
- Ensure appropriate management of access rights and user privileges;
- Conduct user education and awareness;
- Deploy malware prevention and detection tools;
- Implement system monitoring to detect actual or attempted attacks on systems and business services; and
- Restrict use of removable/portable storage media.

Rendition of Accounts

API providers and Consumers are also to render periodic returns such as Volume of transactions, value of transactions, Number of users, success rates, failure rates, Security incidents, and downtime reports, Fraud incidents to CBN using existing channels as specified by the CBN. In February 2021, CBN issued a circular reviewing the timeframe for the submission of returns for Other Financial Institutions (OFIs) to Five (5) days after the last day of each month. As such, OFIs are required to render returns Five (5) days after the end of each month.

Shared Information Framework

The Guidelines set out the requirements for the sharing of customer information between API providers and API consumers. APs shall only share information of a customer with an AC, upon presentation of a valid proof of consent by the customer, and shall authenticate such consent to ensure it emanates from its customer. For consent to be valid, ACs must provide customers with specific information, including their legal name and registration number, the nature of the request, and the duration of consent. The guidelines outline the process for withdrawing consent, the management of redundant data, and the use of authentication mechanisms. In accordance with the Open Banking guidelines, API Providers (APs) are only authorized to share information about their customers with API Consumers (ACs) upon presentation of valid proof of consent by the customer. The AP must authenticate such consent to verify that it is from the customer. A two-factor authentication for users and the validation of information to be shared with the ACs shall be performed directly by the AP using the prescribed authentication mechanism. For example, API providers and Consumers are mandated use strong authentication which includes Multi-Factor Authentication (MFA) to manage access to API systems and implement role-based access control for Personal Information and Financial transaction ("PIFT") and Profile Analytics and Scoring Transactions (PAST). Upon due verification, the API provider shall create a token which shall reflect the details of the rights granted to the API Consumer by the customer. Such token shall be encrypted and securely exchanged with the API Consumer. With regard to the disclosure of customer's data to an outsourced service provider including non- Nigerian participants by an API Provider or Consumer, the approval of the Bank shall be obtained and a statement indicating that the data would be used or disclosed in specific manner.

Dispute Resolution

The Guidelines also outline a mechanism for addressing Open Banking related issues. Customers must be given enough information on how to file complaints and the various dispute resolution processes. Furthermore, the SLAs between Participants must include comprehensive dispute resolution mechanisms. However, if a dispute remains unresolved after exhausting all available procedures, an aggrieved party may file a complaint with the CBN's Consumer Protection Department.

Risks Associated with Open Banking

Open banking presents exciting opportunities for financial institutions and consumers alike. However, with new opportunities come new risks. The rise of cybersecurity threats, data privacy concerns, and regulatory compliance issues have left financial institutions with more to consider than ever before. The sharing of data, while beneficial, can also lead to vulnerability, exposing financial institutions to risks such as data breaches, hacking, and phishing scams. Even the SLA between API Providers and API Consumers comes with its risks, such as non-fulfillment of the terms of the contract. Despite these risks, a regulatory framework is in place to cover losses. As open banking continues to grow, it is the responsibility of all participants to address these risks and work together to ensure the safe and secure sharing of financial information.

CONCLUSION

In today's fast-paced world, online financial services have become increasingly popular due to their convenience. However, with the growing number of online transactions, personal data protection has become a major concern for customers. To address this issue, the Open Banking Guidelines were introduced to provide a regulatory framework that safeguards users' information while still allowing third-party providers access to customer data with their explicit consent. By providing a stable and secure platform for innovation, the Open Banking Guidelines will encourage the development of new customer-authorized products and services, thereby contributing to the growth of the Nigerian financial system.

DISCLAIMER

Authors

Adetola Lawal
Senior Associate
alawal@gbc-law.com

Adeola Fayose
Senior Associate
adeolafayose@gbc-law.com

GBENGA BIOBAKU & CO.
Barristers and Solicitors
11 Babafemi Osoba Crescent Off Admiralty Road
Lekki Phase1, Lagos.
234 803 641 0000
+234 1 2717769
+234 1 2707320 (Fax)
info@gbc-law.com
http://www.gbc-law.com

GBENGA BIOBAKU & CO
BARRISTERS & SOLICITORS