OPEN BANKING IS A PANACEA TO INTEGRATION RISKS

Open Banking

Executive Summary

The need to build a connected world has become very imperative. Almost every industry has been upturned by the advent of technology and the internet. From the logistics to the automotive sector, the integration of various devices and services to create an interactive world has made users more efficient while businesses are better able to understand their customers.

The financial services industry has equally been disrupted and there is a great need for the various players in the ecosystem to connect with each other. For that to happen, banks need to integrate with the fintechs and other third parties using Application Programme Interfaces (APIs) as the primary means of connectivity and data sharing.

However, these technical integrations, especially in financial institutions, are associated with certain risks such as data breaches or hacks. These invariably lead to embarrassment, fines from regulations and / or damages from lawsuits filed by aggrieved customers as well as brand erosion.

Open banking is a new wave that promises to transform the way banking is currently done globally, creating a seamless user experience for customers and providing a solution to the current risks of integration. It will do this through the adoption of a common API standard which banks will use to build API gateways that will enable fintechs to connect with them in an easier, quicker and more secure manner.

Nigeria, which commenced its Open Banking journey in 2017 and is backed by a non-profit, has made significant progress in the development of a common API standard. This would be a panacea to the chronic risks that are associated with API integrations within the Nigerian financial services industry. The advocacy efforts for Open Banking in Nigeria have been very effective such that The Central Bank of Nigeria (CBN) has pencilled the implementation of Open Banking in its next Payment System Vision strategy that is expected to start from January 2020.

Why do banks need integration?

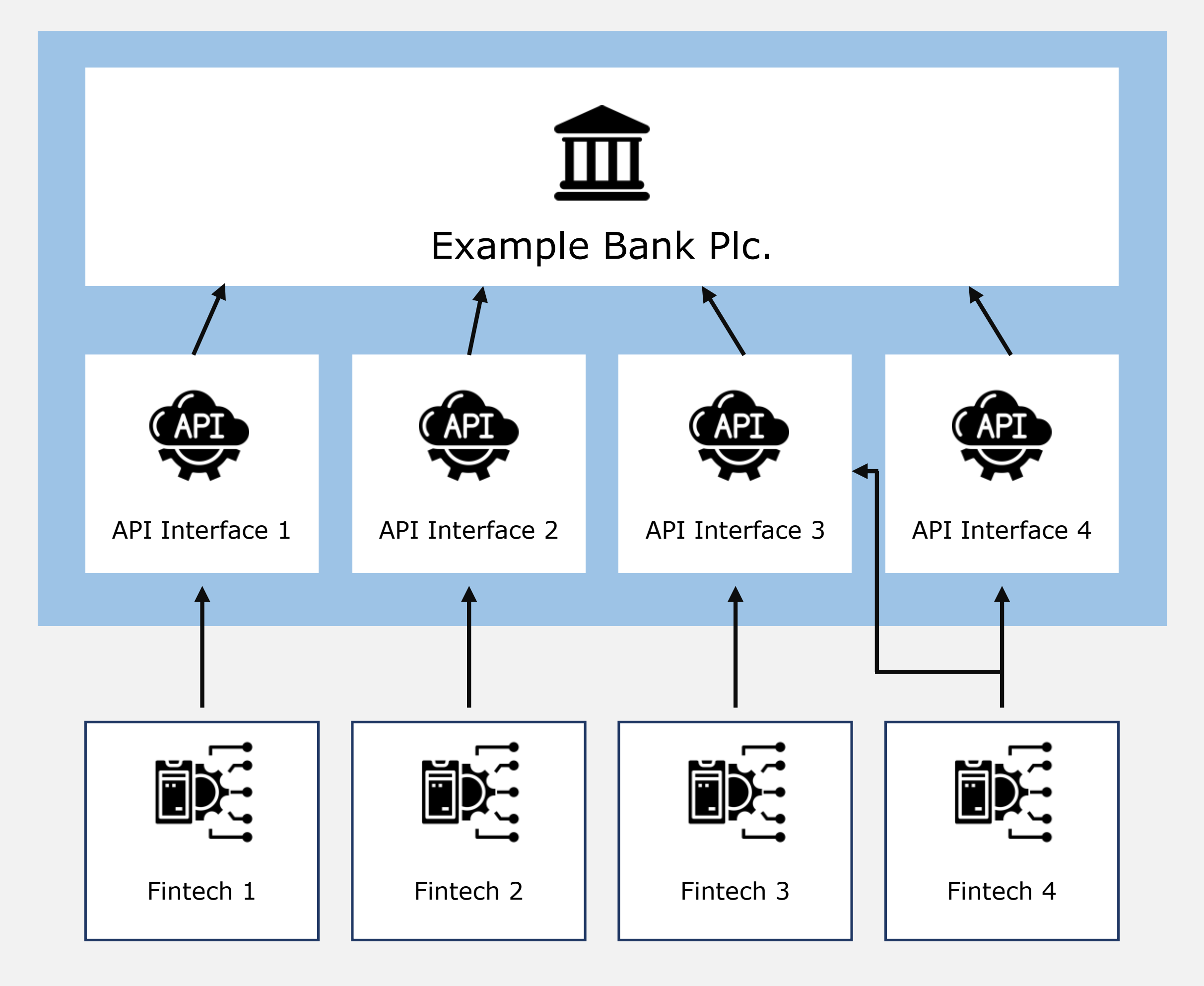
APIs are the language of interconnectivity which allow for sharing of data between financial institutions so that users can access third party applications without having to disclose their password details. Historically, most traditional banks operate in silos, having separate processes and different APIs for their various services.

These APIs need to be secured but because they vary from service to service, the security process requires significant time and effort. As a result, communication and information sharing has been difficult, limiting the banks’ ability to provide the range of services expected by customers.

The disruption awakened the need for the traditional banks to integrate with trusted partners and other third-party providers (TPPs) such as fintechs in order for them to meet the rapidly evolving customer needs and create a better customer experience.

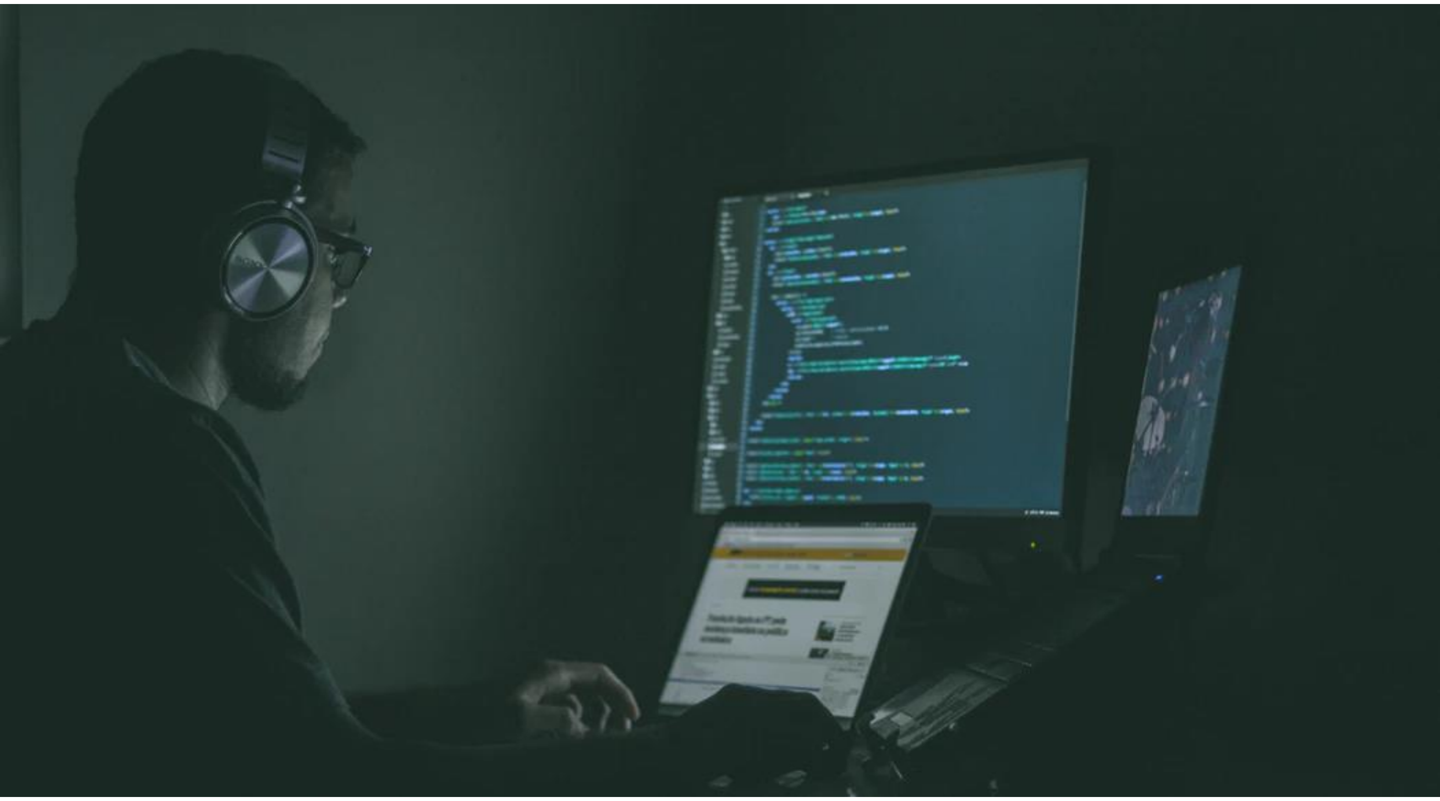
Current approach to integration between Nigerian banks and fintechs

Banks and fintechs currently integrate with each other one at a time using distinct API interfaces (see Figure 1 below), which require that each integration project is specific and tailored to suit the participating institutions. As a result, the process becomes very slow and cumbersome because it is non-standardised.



An additional constraint, to the already slow approach, is the fact that the APIs of traditional banks are usually not public as connections are usually made over private VPN or VPN tunnels via open internet.

For several other banks, there is the issue of an in-coherent and, sometimes, non-existent API strategy which complicates the integration process. The absence of a useful guide for API integration has caused some projects to fail or take longer than planned, rendering them obsolete even before they become operational.



Why is the current approach a security risk?

The current integration approach discussed above presents clear security risks around data protection and potential data breaches as it becomes increasingly difficult, probably impossible, to adequately secure each unique API. Also, because banks develop multiple API interfaces that have overlapping functionalities, security tends to be compromised when data is shared with unauthorised servers.

Vendor lock-in, whereby a particular API becomes functionally dependent on a specific vendor and hinders easy switching amongst the ecosystem, presents another challenge. This lock-in means that a vendor must buy into the, usually different, security services of its partner compromising on overall security. In the future, a common language for integration with all vendors will ease the process and ensure security.

Lastly, the current APIs are hidden behind virtual private networks (VPN), which often do not effectively ensure information is protected outside the network. This has exposed many institutions to hidden and unknown vulnerabilities which are easily exploited by vendors and hackers.

How does Open Banking approach integration?

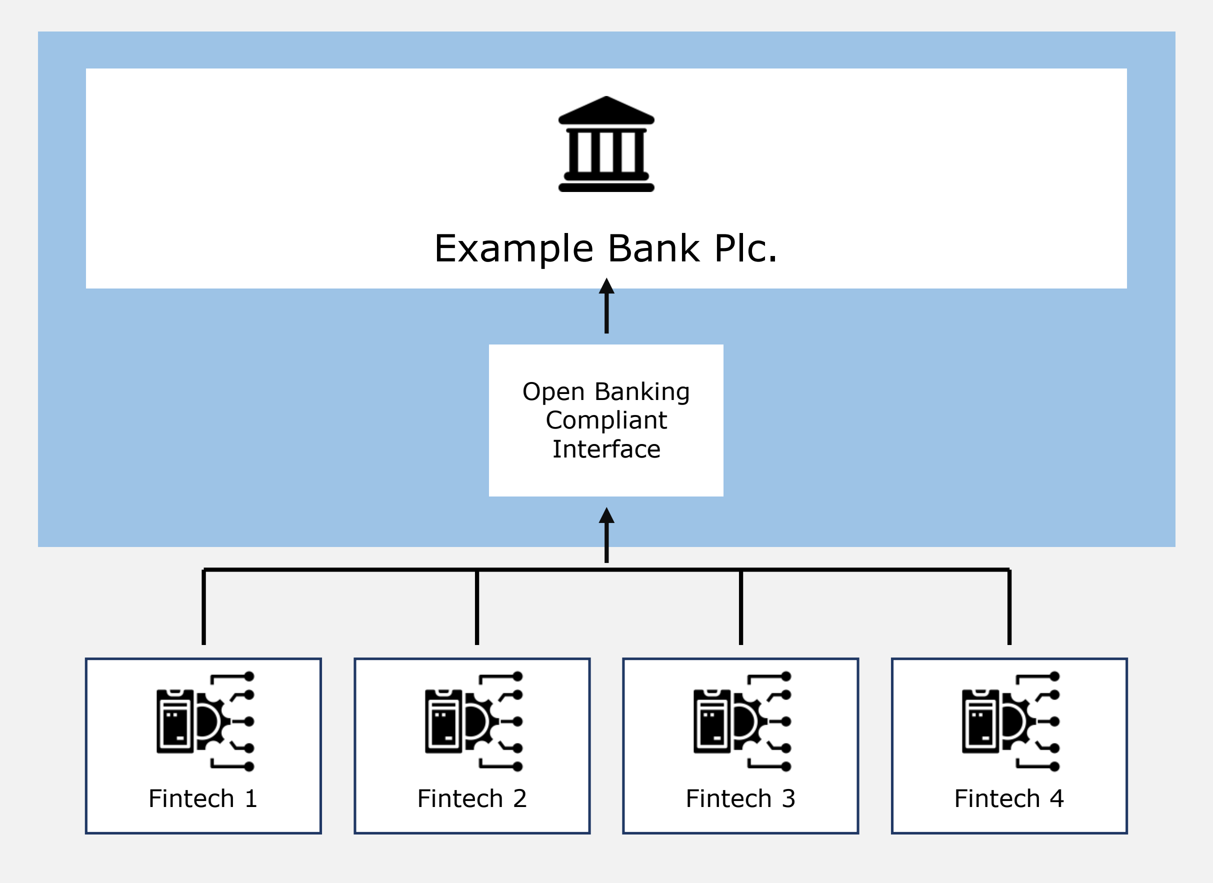
In order for API integration to propagate in the financial services industry, the APIs need to be normalised to fit specific business needs. This is why Open Banking will ensure the adoption of a unified and known industry standard which forms the foundation for banks to seamlessly connect to a broad range of financial institutions in a secure and agile manner. The API standard is open and non-proprietary for any financial institution to implement. While the API standard will be the same, banks will be able to control how fintechs connect or how much they charge for the connection.

Banks will develop these API gateways within demilitarized zones (DMZs) or perimeter networks. When deployed in this manner, the API gateway sits behind control systems like network firewalls which provides them with a unique public routable address in the DMZ and the ability to perform security processing on incoming data such as tracking known attack patterns or checking for anomalies.

Most API gateways will also be to talk to one or more of the available Enterprise Service Bus (ESBs), providing an enhancement to the external integration process that is currently achieved using ESBs.

Why is a single API standard and API gateway more secure for a bank?

The use of the same API standard by all banks to develop their API gateways means that TPPs can connect simply, faster and more securely to these banks via an Open Banking Compliant Interface (see Figure 2 below).



This standard creates a single doorway which provides a consistent interface and means for managing external integrators, thereby reducing risks and threats with ease of visibility and control. This solves the challenge of securing multiple API interfaces as is currently obtainable today.

Moreover, working with multiple gateways breeds a more complex code base as they are usually written using a variety of languages and frameworks. With open banking, simplicity and practicality will be at the very core of the interface to enable faster time to market. While the interface would be standard driven, it will be technologically agnostic, and implementations will be unique to organizations in line with their current or planned offerings.

Security will be built into this standard to increase the confidence of companies, regulators, and other stakeholders using internationally accepted security frameworks. Finally, the freedom from vendor lock-in will allow banks to channel more resources in obtaining the necessary systems and tools to increase the security of their gateways. Banks can focus more on the commercials of partnerships with fintechs than with ad hoc integration

Open Banking's recommendations for banks' approach to security

The adoption of the single API gateway for sharing of customer account data will make it simpler for third parties and fintechs to work with the banks because the API standards will be open and easily implemented by all.

Access to customer data and the ability to do transactions securely are core to Open Banking's principles. It is to this end that Open Banking will ensure that banks adopt a strong authentication process which allows users to confirm to their bank that a request for data sharing from a third party has been approved by them. This authentication process will be enabled by Financial-grade API (FAPI) which uses OAuth 2.0 and OpenID Connect (OIDC) frameworks as its base and adds an extra layer of higher security.

It is no doubt that open banking presents new concerns around fraud risks by scammers or copycat websites, which pretend to be third-party providers, and can gain illegal access to information.

Therefore, to open up data access to other service providers, fraud management is key to ensure customers' trust and confidence is maintained. Banks can implement controls based on advanced analytics designed to detect fraud attacks and abnormal behaviour such as dynamic biometrics where consumer voice, typing and mouse movements are monitored for irregular patterns.[2]

Customer education and creation of awareness around data sharing and privacy is paramount. Customers must be knowledgeable about the power and choice that they have in determining which platforms they agree to share their data or initiate electronic payments with. They should also be aware that they can easily revoke access granted to their data and no data would be released without explicit consent.

Finally, banks should also create a minimum-security benchmark that its partners must meet so integration can occur. This will help to strengthen the overall security of the ecosystem.

The customer authentication feature

The goal of FAPI is to provide an additional layer of security for the applications (to guide the utilization of data stored in their possession) and for users (to control the privacy and security settings). The FAPI verification framework will employ one-time-use tokens or codes that authorize a payment from an end-user payment account to a specific payee. They will be generated after the identity of the end-user has been verified and they have authorized the specific transaction. This feature will be deployed on all smart channels (mobile, web) and tailored to the customers' needs and channel peculiarities.

Liability shift and implications for security

Despite discussing the ways Open Banking will solve the issue of integration, there remains the possibility of things going wrong. Even making it more complicated is the fact that as Open Banking progresses, an increased number of transactions will be done through other third parties, limiting full control of the customer end-to-end journey.

This raises questions such as 'Who is to blame when fintechs go beyond the scope of what is permissible?' 'What happens when a transaction occurs outside the stipulated window that access was granted?' These remain difficult to answer at the moment, especially in Nigeria.

The financial industry in Nigeria can leverage on the UK's progress and mistakes made in its bid to address transaction disputes. In the UK, the Competition and Markets Authority (CMA) in the PSD2 regulation, set out the responsibilities of the participants in the event of a dispute or errors. It has been set out in such a way that the customer never gets caught up in the middle of an issue between banks and TPPs. In the case of unauthorised transactions, the bank must refund the amount of the unauthorised payment transaction to the customer while if the TPP is liable for the unauthorised payment transaction, the TPP must indemnify the bank immediately. In relation to payments initiated via a TPP, the burden lies with the TPP to demonstrate it was not responsible for the error within its 'sphere of influence' as defined by the FCA. Recently, however, controversies have arisen around the established liabilities and there is now a push for an agreement to be collaboratively developed by the TPPs and banks which outlines the terms of payment initiations and account information services offered by the TPP.[3]

Open Banking UK, together with the government, has been developing a Dispute Management System to speed up issue resolution. Participants will sign up to a Code which spells out common best practice standards and principles for the bank and TPPs, such as where a complaint or dispute is taken to. Customers have also been given the right to take a complaint directly to the Financial Ombudsman Service.

Transactional dispute mechanisms for Open Banking Nigeria will leverage on existing underlying frameworks. The CBN established the liability shift guidelines for errors/fraud on card transactions which splits the responsibility between the card issuer, cardholder or channel acquirer depending on the situation.

As no rules currently exist regarding open banking, the banking industry, working with the Central Bank, will need to come together to agree on a common set of rules and procedures that will apply in the case of a fraud/error, specifying the clear responsibilities of each party and liabilities to ensure that all customer issues are resolved.

Next steps for banks in Nigeria

Now that Nigerian banks have come to the realization that APIs are the next logical step towards the evolution of banking, it is imperative that a scalable approach that ensures the standardised APIs are adopted and implemented.

Additionally, efforts have to be made to extend dispute resolution mechanisms and customer authentication measures that are relevant to the new digital systems.

Contacts

Ayowole Popoola

Group Head, IT and Operational Risk
Fidelity Bank
ayowole.popoola@fidelitybank.ng
+234 802 336 2996

Ayowole Popoola serves as the Group Head, Operational & IT Fidelity Bank. Ayowole is an Information Technology and Security professional with strong expertise in IT management, IT security, Business continuity management and IT enterprise architecture.

With a career spanning consulting, financial services and technology, Ayowole leads initiatives on digital transformation, business and technology compliance for the organizations.

Ayowole has bachelor in Engineering Physics, a post graduate diploma in Computer Science and several professional certifications in information security, project and programme management, IT governance, Risk Management and E-business design and innovation.

Abumere Igboa

Chief Information and Security Officer
Stanbic IBTC
Abumere.igboa@stanbicibtc.com
+234 809 808 2340

Abumere is the Chief Information Security Officer for Stanbic IBTC Holdings with over 16 years’ experience and leads a team of information security professionals in protecting the organization's information assets. His experience spans the field of Information Security Risk Assessment and Management, Information Security Compliance Monitoring and Consolidation, Information Security Assurance, Information Security Architecture, and Advisory.

He holds a first degree in Physics and is also an alumnus of the prestigious Lagos Business School where he graduated from the senior management program, (SMP 67). He is also an EC-Council Certified Chief Information Security Officer, a Certified Cyber Security Professional from the Massachusetts Institute of Technology, USA, an ISO 27032 Lead Cyber Security Manager, an ISO 27001 Certified Lead Auditor, an EC-Council Certified Computer Forensic Investigator and holds an MBA degree from the Obafemi Awolowo University, Ile-Ife.

References

1. Flutterwave
2. Raconteur
3. Ashurst
4. Open Banking Expo
5. Central Bank of Nigeria

About Open Banking Nigeria

Open Banking Nigeria, is a legal entity propelling the Open Banking journey in Nigeria. Set up in June 2017 as a non-profit organization, the foundation comprises of industry leaders who recognize the importance of Open Banking in driving the next level of growth in Nigeria’s financial sector. The activities of the foundation are targeted at unlocking growth potentials through the improved collaboration of players within the financial space. A set of standards are being defined as a guidance framework for API integration, data accessibility, and security. An overarching objective of the open banking team is boosting the country’s economy through the reduction of barriers to innovation and consumer’s access to essential financial products and services.

https://openbanking.ng
contact@openbanking.ng

openbankingnigeria

openbanking_ng

openbankingnigeria