Open Banking

Open Banking Implementation Guidelines

For FinTechs

June 2026

Contents

Open Banking Implementation Guide for Fintechs

Introduction: Open Banking in Nigeria

The Central Bank of Nigeria (CBN) is set to declare Open Banking operational in Nigeria. The earlier released framework and operational guidelines are now transitioning from ‘concept documents’ into regulatory requirements.

Open Banking introduces a structured, consent-driven framework that allows financial data to be shared securely between banks, fintechs, and other regulated players within Nigeria’s financial ecosystem.

While compliance is a key motivator, success in Open Banking requires a perspective beyond just ‘sticking with the rules’. This is necessary to remain relevant in the long run.

- **Rising Customer Expectations:** Customers now demand convenience, personalization, and transparency across all financial interactions.
- **Disintermediation and Competition:** Data sharing democratizes customer information, enabling FinTechs and platforms to compete directly.
- **New Growth Opportunities:** APIs are becoming products; players can monetize data, form strategic partnerships, and participate in ecosystem-driven value chains.
- **Shift in Industry Roles:** Banks evolve from product providers to platform participants and ecosystem enablers.

1.1. Why Open Banking is being introduced now and what problem it solves

1.1.1. Unified and permission-based view of financial data across institutions

It reduces fragmentation by enabling a unified, permission-based view of customer financial data across institutions.

An example of what the landscape looks like now:

- A small fashion retail business with accounts at three different banks struggles to pull together account statements, track inflows, and send documents to apply for credit with a fintech company; they generally lack a unified view of their financial position across banks.
- The Lender they are applying to struggles to assess risk accurately due to scattered, outdated, or unverifiable financial data across banks. The fintech is forced to use unsafe workarounds like screen-scraping (i.e. scraping data off screenshots of financial records) or decline the application altogether.

  Screen-scraping typically involves collecting data from websites or apps by mimicking user behavior. Almost all cases of screen scraping require bank customers to share their usernames and passwords with a fintech (or a data aggregator acting on behalf of a fintech) to obtain access to data.

  Fintechs have typically resorted to screen-scraping out of necessity, not necessarily preference. Without a standardised, API-based channel for accessing customer financial data with consent, screen-scraping has historically been the only practical way to retrieve the bank transaction history needed to make a credit decision. However, it poses significant risks:

  - *Customers who share banking credentials with a third party lose sole control of their account access, creating direct exposure to fraud and unauthorised transactions.*
  - *Collecting and storing login credentials could easily violate the NDPR, which requires that personal data be processed only for defined, lawful purposes using secure and proportionate means.*
  - *Screen-scraped data is unstructured, difficult to verify, and easily manipulated, leaving the lender making a risk decision on data it cannot fully trust.*

How Open Banking will change things:

- Open Banking allows customers to grant permission for their banks to securely share financial data with authorised third parties, or to initiate payments on their behalf, through secure and standardised APIs.
- Lenders are able to use the accurate customer-granted financial data for underwriting loans; this enables more accurate credit assessments, faster loan decisions, and improved visibility into a borrower's financial behaviour.

1.1.2. Standardized framework for data-sharing within the ecosystem

It establishes a safer, standardised framework for data sharing between banks and fintechs, anchored on explicit customer consent.

An example of what the landscape looks like now:

- FinTech A is a CBN-licensed Fintech building a payment gateway that allows merchants to enable account-to-account transfers at checkout. To support this capability, fintech must integrate with multiple banks so that customers can initiate payments directly from their bank accounts.
- Without standardised Open Banking infrastructure, each bank integration can take several months to complete, often requiring bespoke technical work and lengthy onboarding processes.
- Each bank typically exposes different APIs, data formats, and authentication requirements. As a result, fintechs must build and maintain separate connectors for each institution and every connection point adds operational and compliance risk.

How Open Banking will change things:

- Open Banking ensures that APIs are standardized and regulated across the industry; they are bidirectional, secure, and consent-driven. This creates a ‘plug-and-play’ rhythm to integrations across the ecosystem. Fintechs can build integrations once and reuse them across multiple institutions, significantly reducing engineering effort and time to market.

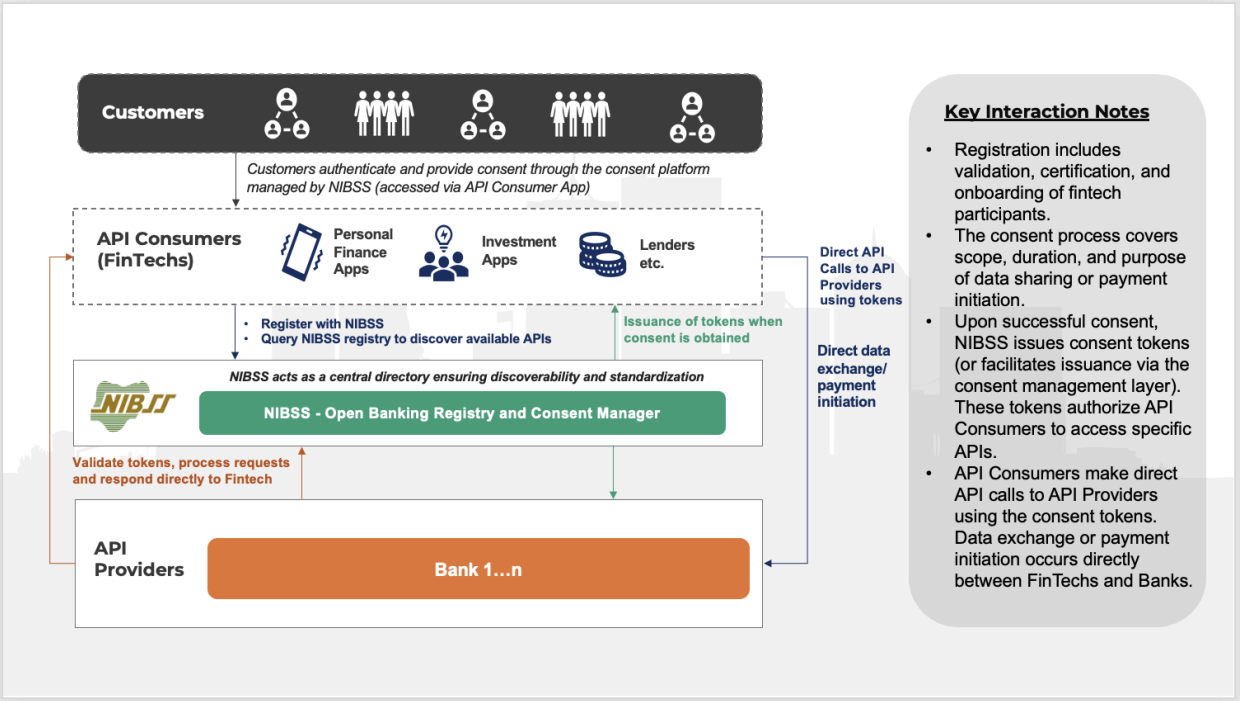


Figure 1.1.2. Open Banking Standardized Model

1.1.3. Lowered barriers for regulated fintechs to build better products

It stimulates competition and innovation by lowering barriers for regulated fintechs to build customer-centric financial products.

What the landscape looks like now:

- Fintech B, building an account aggregation application, would face significant challenges integrating with multiple banks and retrieving the data required to provide customers with a consolidated and up-to-date view of their financial position across accounts.

How Open Banking will change things:

- Fintech B would no longer need to build entirely different integrations to retrieve data from each bank. Instead, they could connect through Open Banking APIs enabling them to deliver a reliable consolidated view across multiple institutions.

1.1.4. Alignment with global Open Banking practices

It adopts applicable global Open Banking practices, technical standards, and regulatory norms, tailored to Nigeria's unique financial ecosystem.

1.2. What Open Banking means in practical terms for fintechs

Open Banking gives fintechs a formal, regulated pathway to access customer-approved banking data across Nigeria's financial system. Rather than relying on screen scraping, shared credentials, or fragile bilateral integrations, fintechs connect to banks through standardised APIs that expose specific services and datasets in a secure, controlled manner. Customer login details are never shared, and access is governed by explicit, time-bound customer consent.

Participation in Open Banking therefore, goes far beyond "plugging into an API." Fintechs must operate as **trusted ecosystem participants**, with readiness across five (5) dimensions:

- **Business readiness –** a clear strategy for monetising Open Banking participation, including API productisation, pricing models, partnership structures, and the ability to translate data access into sustainable revenue-generating products and services.
- **Operational readiness** – clear internal processes for handling customer data, managing incidents, responding to disputes, and supporting consent revocation.
- **Technical readiness** – secure API consumption, token-based authentication, uptime monitoring, and compliance with ecosystem standards.
- **Governance readiness** – documented data usage policies, accountability structures, and the ability to demonstrate compliance to regulators and partner banks.
- **Regulatory readiness** – a working knowledge of the CBN Open Banking Framework, the NDPR, and evolving compliance obligations. Additionally, not all licenses confer the same access. Fintechs must know which API categories they are permitted to consume based on existing licenses, ensure their operations remain within those boundaries, and maintain visibility of any regulatory developments that could affect their access or obligations.

1.3. Purpose of this guide

Open Banking Nigeria has created this guide to

- Help fintechs understand how to participate in Open Banking responsibly and within regulatory expectations.
- Clarify the strategic, technical, operational, and governance decisions required for effective participation.
- Support sustainable, long-term value creation rather than short-term, opportunistic data access or integration practices.

2. The role of fintechs in the Open Banking ecosystem

Open Banking creates a shared financial data environment where banks, fintechs, and other participants each play distinct roles. For fintechs, the opportunity is to build value-adding services on top of the regulated financial infrastructure that banks provide.

2.1. Fintechs as data users, service innovators, and experience layers

Within Nigeria's Open Banking ecosystem, fintechs primarily operate as authorised data users and service innovators, leveraging customer-granted access to banking data through standardised APIs.

With explicit customer consent and within approved use cases, fintechs can:

- Access relevant financial data held by banks
- Initiate permitted actions as defined by Open Banking standards and applicable licences (e.g. payment initiation, verification, account balance retrieval etc.)
- Build value-added products and services on top of regulated banking infrastructure
- Function as aggregators that facilitate standardised, regulated access to the Open Banking ecosystem for external participants.

This positioning allows fintechs to focus on:

- Transforming raw financial data into actionable insights and personalised services
- Designing customer-centred journeys and workflows
- Delivering faster, more intuitive digital financial experiences

In practical terms, fintechs function as the experience and innovation layer of Open Banking – translating regulated banking infrastructure into accessible, everyday financial tools for consumers and businesses.

2.2. How fintechs complement banks in Open Banking

Open Banking is not intended to displace banks or transfer core-banking regulatory responsibilities to fintechs. Instead, it enables a complementary operating model where each participant focuses on its comparative strengths.

Banks provide:

- Regulated access to customer accounts and transaction data
- Secure, resilient financial infrastructure
- Established risk management, compliance, and licensing frameworks

Fintechs complement this by:

- Building customer-facing applications beyond traditional banking interfaces
- Addressing niche, emerging, or underserved use cases
- Enabling faster experimentation, iteration, and product specialisation

This division of responsibilities allows the ecosystem to scale innovation efficiently, without requiring banks to internalise the speed, cost structure, or experimentation cycles typical of fintech-led product development.

3. Open Banking use-cases for fintechs

3.1. Identifying high-value Open Banking use-cases

Not all Open Banking capabilities translate into viable products. Fintechs should evaluate potential use cases using practical, customer-focused criteria.

Strong use cases typically:

- Solve a clearly defined customer problem.
- Deliver meaningful improvements through access to financial data.
- Reduce friction, cost, or uncertainty for the user.
- Can be reliably implemented using available Open Banking APIs.

Use cases that rely solely on novelty or data availability, without tangible customer benefit, are unlikely to gain adoption. Fintechs should assess opportunities based on problem relevance, data dependency, and execution feasibility, **r**ather than technical possibility alone.

Strong use case: Cash-flow–based SME lending

Fintech uses bank transaction data to assess the cash-flow health of small businesses in order to determine repayment capacity.

Weak use case: Data dashboard applications with no clear financial action

An app aggregates bank data and presents charts to businesses but offers no meaningful insights, decision support, or financial actions.

3.2. Possible use-cases for Open Banking

Open Banking expands what fintechs can build, but creating real value requires choosing the right focus. Opportunities generally fall along four interconnected areas, each with distinct trade-offs in complexity, regulation, and scalability. Fintechs should align their strategy with their capabilities, risk appetite, and target customers.

3.2.1. Payments

A merchant building an online checkout today may depend on card payments. Customers must manually input card details, transactions can fail due to authentication or network issues, and

merchants incur card processing fees. Similarly, recurring payments often require customers to repeatedly authorise transactions or depend on ineffective debit mandate systems that can be tough to set up and manage.

Open Banking allows customers to authorise payments directly from their bank accounts through secure APIs. The result is faster payments, lower costs for merchants, and fewer steps for customers during checkout. This enables:

- **Pay-by-bank and account-to-account payments –** This allows customers to make payments directly from their bank accounts without relying on cards or manual transfers. Instead of entering card details, the customer simply authorises the payment through their bank using a secure consent flow.
- **Direct-debit/recurring payment flows –** This, on the other hand, allows customers to authorise a fintech/merchant to debit their account automatically at agreed intervals (e.g. Netflix subscriptions). After the initial consent, payments can be triggered without requiring the customer to manually approve each transaction (This may still be subject to regulatory safeguards and mandate controls however the existing protocol around the GSI gives it a launchpad to take off).
- **Card Management –** Offers APIs for secure access to card-related information, enabling customers to manage their cards within third-party apps.

3.2.2. Credit

An SME applying for a loan today may need to submit months of bank statements and wait several days or weeks for manual review. Even then, lenders may struggle to accurately assess cash-flow stability, leading either to rejected applications or very tough lending limits.

With customer consent, lenders can securely access transaction-level financial data directly from bank accounts. This enables:

- **Cash-flow–based lending –** Fintechs can now assess affordability and risk using real-time transaction data, supporting inclusion for underserved individuals and SMEs. The conversation easily moves from “do you have collateral?” to “does your financial behaviour support repayment?”
- **Real-time Credit Decisioning:** With access to verified financial data from banks, time-to-yes or time-to-no will significantly be shortened reducing the time between application and

decision. Beyond this, lenders will be able to monitor borrower health after disbursement and catch risk early on.

- **Embedded Credit:** This will allow fintechs embed credit products at the point of need e.g. BNPL checkout on e-commerce platforms, inventory financing inside merchant tools etc.
- **Dynamic Credit Limits:** Rather than issuing static loan limits, fintechs can adjust exposure as a borrower's financial position evolves. e.g. increasing limits when income improves or tightening exposure when risk indicators rise.

It is important to note that access to high-quality data alone does not guarantee better underwriting. The effectiveness of credit decisions ultimately depends on the strength of the fintech's internal algorithms, risk models, and benchmarking frameworks.

3.2.3. Identity management and verification

A fintech onboarding a new customer today may request account details, BVN/NIN identification numbers, and manual verification of account ownership. This process can take several steps and may still fail to confirm whether the bank account truly belongs to the applicant due to data quality issues, ecosystem fragmentation, and operational gaps.

Open Banking allows fintechs to verify certain financial attributes directly with the customer's bank, with the customer's consent. This enables:

- **Identity Verification:** Fintechs can leverage secure bank APIs to confirm key identity attributes during onboarding (e.g. account-to-name matching, account status validation, etc.).This service can also be extended to 3rd-party applications that may require customer verification for onboarding.
- **Risk Profiling:** Where permitted and supported by the bank's data capabilities, fintechs may receive structured risk signals (e.g. income indicators, affordability signals, account activity etc.) that support safer customer acquisition and transaction monitoring.

3.2.4. Personal finance management

In the current financial ecosystem, a salaried professional might receive income in one bank account, keep savings in another, and make payments using a third account or digital wallet. To understand their monthly financial position, they would need to check multiple apps and manually combine the information. Similarly, a budgeting application that does not integrate with banks may

require users to manually input expenses, which quickly becomes impractical and leads to incomplete financial records.

With customer consent, Open Banking allows fintechs to securely retrieve account balances and transaction data across multiple banks through standardised APIs. This enables:

- **Account aggregation and financial dashboards** – Provide a unified view of multiple bank accounts, balances, and transactions to reduce fragmentation.
- **Personal finance management and budgeting tools** – Use transaction data to track spending, categorize expenses, set budgets, and deliver actionable insights.
- **Savings and goal-setting tools** – Enable customers to automate savings, monitor progress, and receive contextual guidance.

3.2.5. Enterprise and ecosystem enablement

Here, Fintechs can provide foundational services to other fintechs, enterprises, and institutions.

- **API aggregation and data standardization:** Open Banking standards reduce fragmentation, but integration across multiple banks can still be operationally heavy. Fintechs can provide unified APIs that abstract differences across banks. i.e. the *Mono* model (a Nigerian fintech that provides a unified API layer allowing businesses to connect to multiple banks, access customer-permissioned financial data, and initiate payments through a single integration)
- **Data enrichment and financial intelligence:** Raw transaction data is rarely product ready. Fintechs can deliver cleaned, categorized, and enriched datasets, including behavioral and risk insights, to support faster product development and informed decision-making.
- **Product Aggregation:** Open Banking can also enable product discovery across financial institutions. Fintechs can aggregate savings products across banks, SME loans and credit lines etc. For example, with customer consent, these fintechs can pre-qualify users for suitable loan products and facilitate application flows
- **Treasury Management:** Open Banking significantly improves visibility into multi-bank cash positions for SMEs/Corporates enabling fintechs to build capabilities such as
    - consolidated liquidated dashboards,
    - automated cash sweeps between accounts,
    - vendor/payroll payment scheduling,
    - forecasting tools

    - multi-bank reconciliation engines etc.

3.2.4. Cross-sector and emerging opportunities

This involves applications beyond traditional banking, enabled by Open Banking data.

- **Open finance platforms:** Fintechs can integrate banking data with adjacent financial services such as insurance, pensions, wealth products, and investments to provide customers with a more complete financial view. Potential capabilities include:
    - Unified financial dashboards spanning multiple asset classes
    - Cross-product recommendations based on customer behaviour
    - Automated financial planning tools
    - Embedded investment or insurance journeys
- **SME and informal economy solutions:** Open Banking creates an opportunity to serve segments historically excluded from formal financial tools particularly microbusinesses and informal operators. Fintechs can build:
    - Cash-flow tracking tools using transaction data
    - Automated bookkeeping and tax estimation allowing seamless compliance with tax laws
    - Working capital solutions informed by real revenue patterns
    - Cooperative and group finance tools
- **New business models:** Enable marketplaces, subscription-based services, or embedded financial products in non-financial sectors.

4. Cost structure and revenue opportunities.

4.1. Cost of API access

Open Banking monetization goes beyond charging for data access; it is ultimately driven by the economic value created through its use.

Global experience suggests that Open Banking frequently begins with a form of “freemium” access in order to encourage participation, lower entry barriers, and stimulate innovation. For example, UK regulators required certain mandatory APIs (account information, transaction history, and payment initiation) to be provided free of charge in order to promote competition.

However, access to bank infrastructure rarely remains cost-free over the long term. As participation scales, banks might introduce pricing structures that balance ecosystem adoption with the cost of building and maintaining secure, highly-available APIs.

Common approaches may include:

- Tiered per-call or per-transaction pricing
- Threshold-based fees for higher-volume usage
- Monthly platform or subscription fees for dashboard/API access
- Premium pricing for sensitive or high-risk endpoints
- Outcome-based pricing for verified actions or payments

4.2. Assumptions on Certification and Open Banking Registry (OBR) Registration fees

While no formal guidance has been issued by the Central Bank of Nigeria on certification and OBR fee structures, a number of plausible approaches may be adopted to serve the ecosystem:

- Certification may operate on an annual basis, with a fee structure that scales with institutional size.
- For API consumers (ACs), a flat fee structure may apply reflecting their role and operational scale.
- Tier 0 entities may initially be exempt from certain fees to encourage early-stage innovation and reduce entry barriers.

- Institutions signing on to the OBR may be required to pay a fee. These fees may be administered by NIBSS or another designated operator, which would oversee the technical management of the registry.
- Transactions may continue under existing CBN fee structures, meaning transfers are handled by underlying payment systems such as NIBSS, UP, Interswitch, and Etranzact without change.
- Checks for customer profiles, account details, KYC data, and balances may initially be free, supporting frictionless data sharing.
- Pulling transaction statements may attract a modest fee while the creation of mandates, virtual accounts, and similar features remain free, with transactional activity on these instruments charged according to prevailing CBN rules.

Please Note: The above listed fee structures are educated assumptions on the part of Open Banking Nigeria and in no shape or form constitute a formal guidance on CBN fee structures.

4.3. Revenue opportunities in Open Banking

While the possibility of free/cheap access to certain APIs may spell an advantage for fintechs, a number of factors should be taken into consideration when designing revenue models:

- Competition is likely to be stiffer as access will be democratized in the initial stages.
- Revenue models must shift from being paid for 'access to data' to 'providing insights for decision-making' from said data.
- Anchoring a fintech's business model in API resale, data passthrough or markups on connectivity may work in the short-term but gain is likely to erode fast.
- Fintechs will still have to incur costs that will compress margins e.g. aggregator/connectivity layers, fraud infrastructure etc. Therefore, sustainable margins depend on operating at sufficient scale and maintaining cost efficiency.
- Customer acquisition gets cheaper as users can be onboarded in minutes
- Revenue timing improves as fintechs can now monetise early on in the customer lifecycle i.e. instead of spending months gathering data on customer behaviour, loans can be offered upfront using existing history as a pre-qualifier.
- Revenue models should account for bank access costs in the near future while preserving overall commercial viability.

4.3.1 Outcome-based monetisation

This model focuses incentives on performance and value delivery, rather than technical access. Instead of monetising data itself, fintechs monetise the result the data enables. This ensures that revenue is aligned with measurable value, margins are protected even if API access is cheap/free and the model scales naturally with usage. Examples include:

- Loan origination fees
- Payment success fees
- Investment placements
- Insurance conversions
- Affordability verification for lenders

4.3.2. Intelligence-as-a-service

This model centres on transforming financial data into decision-grade intelligence. As Open Banking matures, access to financial data will increasingly become commoditised, reducing its value as a stand-alone differentiator. Competitive advantage will therefore shift from ‘who has the data’ to ‘who can interpret it most effectively’.

Fintechs that invest in strong analytics capabilities can convert raw transaction data into actionable insights that support faster, safer, and more informed financial decisions for both consumers and businesses. Monetisable intelligence may include:

- Cashflow analysis and income verification
- Creditworthiness and affordability indicators
- Fraud detection and behavioural risk signals
- Spending patterns and financial health insights
- SME performance analytics

4.3.3. Embedded finance participation

Open Banking dramatically lowers the friction required to embed credit, payments, or insurance into everyday customer journeys. Fintechs can now earn a share of financial products delivered inside non-financial platforms. Examples include:

- Credit embedded into e-commerce checkout

- Payroll-linked lending
- Merchant cash advances
- Insurance bundled into travel platforms
- Savings embedded into gig-worker apps

However, due to the partnership requirement of this model, revenue mechanics will have to take into account revenue share with banks, platform commissions, origination fees and float participation (where permitted).

4.3.4. Subscription models for SMEs

Open Banking makes it easier to build high-stickiness tools for businesses that depend on real-time financial insight. Fintechs can convert financial visibility into recurring revenue through a subscription model. Examples include:

- Treasury dashboards
- Multi-bank cash management
- Automated reconciliation
- Tax estimation tools
- Expense intelligence
- Working capital alerts

This model offers predictable recurring revenue, lower volatility than transaction-based income and possibility for strong retention once embedded into the customers workflow.

4.3.5. Fintech-to-Fintech and infrastructure monetisation

Not all Open Banking fintechs need to be customer-facing. Some of the most scalable opportunities exist in providing infrastructure and enablement services to other fintechs and enterprises. These may include:

- Aggregated Open Banking APIs
- Consent management layers
- Data enrichment and categorisation services
- Risk, behavioural, or financial intelligence

4.4. Trust, transparency, and monetisation guardrails

Open Banking operates on explicit customer consent and regulatory trust. Monetisation strategies that undermine these weaken long-term ecosystem viability.Sustainable monetisation models:

- Are transparent and explainable to customers and regulators
- Do not charge customers for access to their own data
- Align incentives across banks, fintechs, and users
- Treat consent as an ongoing relationship, not a one-time event

Fintechs should avoid:

- Hidden fees tied to sensitive financial actions
- Reusing data beyond clearly stated purposes

5. Technology, teams, and operations

Open Banking participation raises the bar for fintechs requiring them to operate as dependable service providers within a regulated financial ecosystem. Beyond technical integration, fintechs must demonstrate operational maturity across their technology, people, and governance structures.

This is particularly important because CBN has historically held banks accountable for risks introduced by their partners. A strong operating posture therefore reassures banks and other ecosystem participants, making them more willing to partner with fintechs.

This section is largely structured around three maturity levels to reflect the increasing requirements from fintechs as they advance on their journey:

- **Baseline:** the minimum required to participate in the Open Banking ecosystem
- **Best-Practice:** capabilities expected of fintechs operating at scale or seeking deeper bank partnerships
- **Advanced Maturity:** standards that distinguish fintechs as high-trust, ecosystem-ready operators

5.1. Technology and tooling capabilities

5.1.1. API integration and orchestration architecture

Baseline Capabilities:

- Ability to integrate with at least one bank via standard Open Banking APIs;
- Automated handling of retries, failures, and timeouts
- Isolation of bank-specific logic from core product systems

Best-Practice Capabilities:

In addition to baseline capabilities, fintechs should be able to:

- Maintain an orchestration layer that enables consistent and resilient integration with multiple financial institutions.
- Manage API versioning and changes without service disruption
- Implementing fallback mechanisms where a bank API fails i.e. falling back to alternative aggregator endpoints, maintaining an API health scoring system per bank endpoint to route

traffic away from unstable endpoints, and ensuring all fallback events are logged and do not bypass consent enforcement.

Advanced Capabilities:

In addition to baseline and best-practice capabilities, fintechs should be able to:

- Manage redundancy planning, traffic routing, and performance optimization.
- *Alternatively – and depending on their strategy – FinTechs may choose to approach this through partnerships with an existing aggregator.*

5.1.2. API architecture security

Fintech integrations should align with modern API security practices so that customer credentials are never exposed and system access is tightly controlled.

Baseline Capabilities:

- OAuth 2.0 / OpenID Connect for delegated, token-based access. This ensures customers authenticate directly with their bank and grant consent without sharing passwords with third parties.
- Mutual TLS (mTLS) for encrypted, certificate-based system-to-system communication. This verifies both parties in the connection and protects against interception or impersonation.
- Environment segregation and secure key management. This will look like separate sandbox and production environments, protected credential storage (no hard-coded keys), and regular certificate rotation.

Best Practice Capabilities:

In addition to baseline capabilities, fintechs should be able to provide:

- Secure token lifecycle management. This will cover short-lived access tokens, secure refresh mechanisms, and immediate revocation upon consent withdrawal.

Advanced Capabilities:

In addition to baseline and best-practice capabilities, fintechs should be able to provide:

- Automated key and certificate management
- Continuous security posture monitoring
- Integration-level threat detection

5.1.2.1. What are banks really looking out for?

- Will this integration expose customer credentials or weaken authentication controls?
- Does this partner understand consent as a security boundary?
- Can they manage tokens, keys, and certificates responsibly?
- If something goes wrong, can they detect, contain, and report it quickly?
- Will connecting to this fintech increase our operational or cyber risk?
- Is data used strictly within the approved purpose scope?
- Is there a risk of purpose drift? (e.g., data used for marketing after consent was granted)
- Will internal systems enforce purpose-based access controls rather than relying solely on role-based controls?

5.1.3. Data protection and privacy compliance

Fintechs must reorient their teams to treat customer data as a regulated asset not merely an engineering input. Participation in Open Banking requires demonstrable discipline in how data is collected, stored, used, and retired.

A number of immediate steps which Fintechs can take to improve their position include:

- Audit of Data Landscape to ensure alignment with The Nigeria Data Protection Regulation (NDPR). This provides a clear lawful basis for data processing, purpose limitation, and respect for customer rights such as access, correction, and deletion.
- Ensuring encryption of data in transit and at rest. Sensitive data should be protected both when moving between systems and while stored internally.
- Documenting defined data retention and deletion standards. Customer data should not be stored indefinitely. Policies must specify what is retained, for how long, and when it is securely disposed of particularly after consent expires or is withdrawn.
- Ensuring named accountability for compliance and data protection obligations. Specific roles or functions should be responsible for regulatory adherence, data protection oversight, and engagement with relevant authorities.
- Ensuring ongoing coordination between compliance, product, and engineering teams. Regulatory considerations should be integrated into product design and technical decisions, rather than addressed only after implementation.

5.1.4. Standardised data and messaging formats

Open Banking Nigeria has defined technical standards that may govern how messages are structured, secured, and exchanged across the Open Banking ecosystem. Fintechs would be required to align with these standards to ensure interoperability and trust with banks and other participants:

- **Message headers.** Every API payload must include a defined set of headers. Several are mandatory, including a unique idempotency key, message signature, and timestamp fields that track the full request-response lifecycle. These headers are not optional formatting conventions; they are how the ecosystem maintains traceability and accountability across every transaction.
- **Message integrity and error recovery.** Where an exchange fails due to a timeout, malformed response, or validation error, you are required to initiate rollback or retry procedures immediately. Retry windows must not exceed six hours, after which unresolved incidents are escalated for manual handling.
- **Idempotency.** All POST and transaction API calls must carry an idempotency key, a unique reference that prevents duplicate processing if a request is retried. Keys must be sufficiently unique and are valid for the lifetime of the connected endpoints.
- **Timeouts.** Maximum timeout periods are defined by API category: 30 seconds for payment operations, 45 seconds for open data, and 90 seconds for registration and directory operations.
- **Data types and formats.** Precise formats are specified for amounts, dates, account numbers, phone numbers, currency codes, and other field types. Fintechs should validate their systems against these standards, particularly the NUBAN account format, ISO 4217 currency codes, and epoch millisecond timestamps used in message headers.
- **Message security.** Messages are signed using SHA-512 hashing of key payload fields to verify authenticity and detect tampering. Full payload encryption is not used by design. Sensitive fields, identifiable by the 'x' prefix, are individually encrypted at the field level. Anti-replay controls are enforced by validating that message timestamps fall within a three-minute window of system time.
- **Event logging.** All API requests and responses must be logged in raw format and retained for a minimum of 180 days. Logs must be captured before any business logic is applied on inbound messages, and immediately after processing on outbound messages.

For full technical specifications can be accessed on the **Open Banking Nigeria API Standards and Security Framework** documentation available at www.openbanking.ng

5.1.5. Monitoring, logging, and incident response

Operational visibility is critical to maintaining trust, enabling accountability, and demonstrating reliability within the Open Banking ecosystem. It enables early intervention and supports transparent post-incident accountability.

Baseline Capabilities:

- Continuous monitoring of API availability and performance. Systems should actively track uptime, latency, and error rates across all bank integrations to enable early detection of service degradation.
- Logging of data access and system activity. Detailed logs should capture when data is accessed, by whom, and through which systems, supporting auditability and post-incident analysis.
- Defined thresholds for incident detection and escalation. Clear criteria should exist to distinguish routine issues from material incidents, with predefined escalation paths for timely response.
- Documented incident response and recovery procedures. Fintechs should maintain practical, well-understood procedures for incident containment, communication, and recovery.

Best Practice Capabilities:

In addition to baseline capabilities, fintechs should be able to provide:

- Latency tracking across all bank integration
- Structured escalation paths distinguishing routine issues from significant incidents
- Post-incident review processes
- Structured external communication protocols for significant incidents

Advanced Capabilities:

In addition to baseline and best-practice capabilities, fintechs should be able to provide:

- Real-time alerting and automated anomaly detection
- An incident response playbook tested through regular drills

5.2. Teams and operational readiness

5.2.1. Engineering and platform ownership

Open Banking requires sustained technical stewardship, not temporary project ownership. Clear engineering and platform ownership ensures stability, resilience, and effective coordination as Open Banking operations scale. Fintechs should assign:

- **Dedicated engineering responsibility for integrations and data pipelines**
  Specific teams or roles should own the development, maintenance, and evolution of Open Banking integrations and data flows.
- **Clear accountability for uptime, performance, and maintenance**
  Ownership should include responsibility for system reliability, ongoing performance monitoring, and issue resolution.
- **Continuity of ownership beyond individual projects or releases**
  Open Banking capabilities should be managed as long-term infrastructure, with ownership that persists as systems and partnerships evolve.

5.2.2. Product and customer experience leadership

While CBN regulation mandates the necessary infrastructure for Open Banking, **in practice**, trust is built less through regulation and more through everyday product experiences. Fintechs that treat product leadership as a risk and trust function not just a growth function will differentiate faster and retain customers longer. This is particularly important in a low-trust environment like Nigeria. To this end, product leadership must ensure:

- **Clear and transparent consent flow.** Customers should be able to understand what data is being accessed, for what purpose, and for how long, with consent presented as an informed choice rather than a technical requirement.
- **Intuitive presentation of Open Banking-enabled features.** Features powered by Open Banking should be easy to discover and use, without exposing customers to underlying technical complexity or banking infrastructure details.
- **User-appropriate error handling and disclosures.** Errors, delays, or data issues should be communicated in clear, non-technical language that helps users understand what has occurred and what action, if any, is required.

- **Alignment between technical capabilities and customer expectations**
  Product design should reflect what systems can reliably deliver, avoiding overpromising functionality that cannot be consistently supported.

5.2.3. Operational ownership of Open Banking activities

Open Banking requires consistent day-to-day operational oversight to ensure reliability, partner alignment, and regulatory confidence.

At a minimum, fintechs should define ownership for:

- **Bank and partner coordination.** Responsibility for managing relationships, communication, and expectations with participating banks and ecosystem partners.
- **API change management.** Ownership of tracking, assessing, and responding to changes in bank APIs to minimise service disruption.
- **Incident handling and reporting.** Clear responsibility for managing operational incidents, including investigation, remediation, and external communication where necessary.
- **Regulatory engagement where required.** Designated ownership for regulatory correspondence (with the CBN, NIBSS and other stakeholders), reporting, and participation in ecosystem-level discussions.

6. Customer trust, consent and experience design

Customer trust is the cornerstone of Open Banking adoption. Consent is not merely a regulatory requirement; it is the mechanism through which customers decide whether Open Banking delivers value or introduces risk. Fintechs must therefore design consent and experience flows that are transparent, intelligible, and demonstrably fair.

6.1. Designing transparent and understandable consent journeys

Consent journeys should enable customers to make informed decisions without ambiguity or pressure.

Fintechs should ensure that consent experiences:

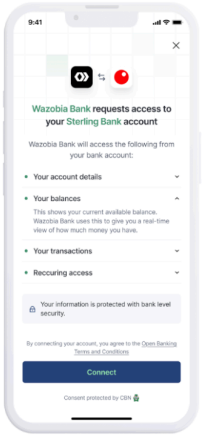
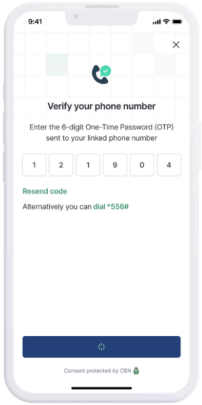
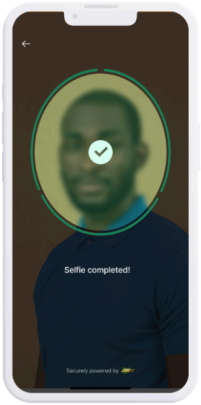
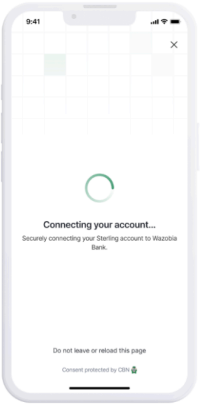
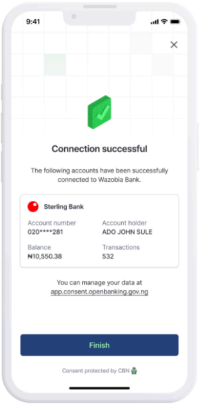
- **Clearly explain what data is being accessed and why**
  Customers should understand the specific data types involved, the purpose of access, and how the data will be used to deliver value.
- **Communicate duration and scope of consent**
  Consent screens should clearly state how long access will last and whether access is one-time or ongoing.
- **Provide visibility into control and revocation**
  Customers should be able to see how consent can be withdrawn and what happens to their data when consent ends.

Consent that is clear and contextual strengthens trust and reduces friction during onboarding.

See sample consent flows below:

Consent via OAuth2 web interface

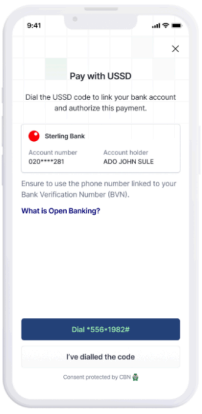
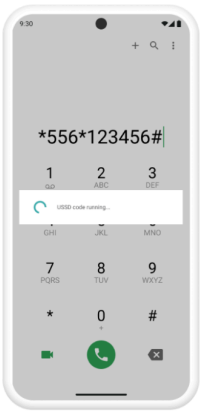
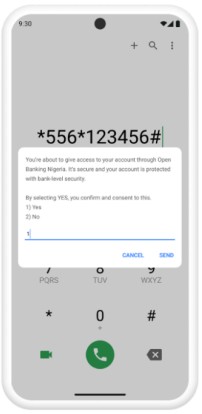
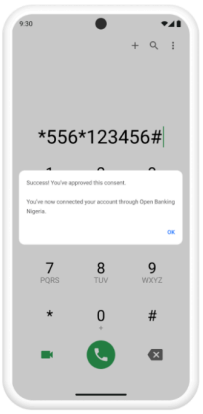
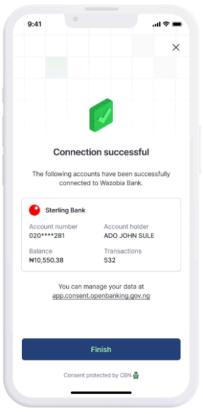
- ACs will make a */oauth2/device/code* API call to the OBCMS, which will return *user_code* and *verification_uri*
- ACs will display the *user_code* to the end user and then redirect them to *verification_uri*, where the following sequence will happen:

OBCMS should inform the End User of what the AC will have access to	End User enters the device_code that was sent to the AC	Optionally, OBCMS may implement proof of life or other identity verification methods	OBCMS will enable the consent and link the End User to the AC	AC will poll the /token endpoint to obtain the status of the operation
				

Consent via an OAuth2 USSD interface

- ACs will make a */oauth2/device/code* API call to the OBCMS, which will return *user_code* and *verification_uri*
- ACs will display the *user_code* to the end user and then redirect them to *verification_uri*, (a USSD string in this case) where the following sequence will happen:

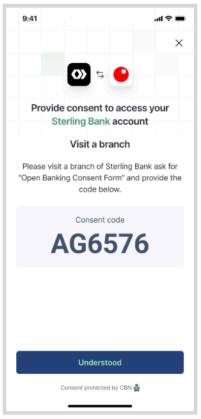
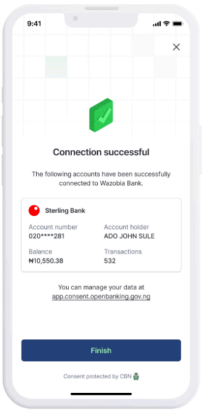
*[**NOTE**: The "123456" here is the user_code from the consent initiation response]*

ACs should display the USSD code they received in verification_uri	The End User will dial the USSD string which includes the user_code	The OBCMS will provide the End User with a confirmation screen	OBCMS will enable the consent and link the End User to the AC	AC will poll the /token endpoint to obtain the status of the operation
				

Consent via “offline” channels (internet banking, branch, etc.)

Especially designed for corporate accounts and low digital literacy use cases

- ACs will make an */oauth2/device/code* API call to the OBCMS, which will return *user_code* and *verification_uri*
- For this scenario, OBCMS will set *consent_validation_method* to OFFLINE, *expires_in* to 259200 (3 days) *interval* to 86400 (1 day)
- ACs will display the *consent_message* (e.g., “Please visit the nearest bank branch to complete form XYZ to grant consent”) to the end user and then redirect them to *verification_uri* (if available)

ACs should display the consent_message and user_code to the user	The End User will do whatever the consent_message says		AC will poll the /token endpoint to obtain the status of the operation
	**Branch or Agent**	**Internet Banking**	
	Visit a branch and fill a form	Access the internet banking provided by their bank or a dedicated portal	
	Branch staff inputs details of the form into a branch tool	Complete an “Open Banking consent form” module	
	Branch tool validates the consent_token and updates the OBCMS	The module validates the consent_token and updates the open banking system	

6.2. Communicating value to encourage data sharing

Customers are more likely to grant consent when the value exchange is explicit and credible. This customer perception is largely influenced by how fintechs communicate with them.

Fintechs should communicate:

- **The direct benefit the customer receives from sharing data**
  This may include improved financial visibility, faster payments, better credit access, or more personalised services. For example, a personal finance application might say:

  “Link your bank accounts to see all your balances and transactions in one place, helping you track spending and manage your finances more easily.”

- **How Open Banking improves outcomes compared to alternatives**
  Messaging should explain why data sharing leads to better results than manual inputs or fragmented tools. For example, a fintech offering SME loans might say:

  “Instead of uploading bank statements and waiting several days for manual review, you can securely connect your account. This allows us to verify your cash flow instantly and provide a faster loan decision.”

- **What the customer does not lose by consenting**
  Clear reassurance around data security, control, and non-exploitative use reduces perceived risk. For example, a fintech might display a message such as:

  "We will only access the transaction data required to provide this service. We cannot move money from your account without your explicit approval, and you can disconnect your account at any time."

6.3. Avoiding misleading or coercive consent patterns

Consent design directly affects trust in Open Banking. Patterns that prioritise conversion, speed, or data capture over customer understanding may increase short-term uptake but undermine long-term adoption and regulatory confidence.

Fintechs should avoid:

- **Bundling consent with unrelated or essential actions**
  Consent to data access should not be a prerequisite for accessing services that do not reasonably require Open Banking. Customers must not feel that consent is the only path to participation. For example:

  A fintech company requires users to connect their bank account through Open Banking simply to create an account or browse available services.

  This creates the perception that data access is mandatory, even when it is not necessary.

- **Using vague, legalistic, or overly technical language**
  Consent explanations should be written in clear, user-appropriate language that enables informed decision-making, rather than relying on complexity to discourage scrutiny. For example, a fintech displays the following message:

  "By continuing, you authorise the transmission and processing of financial data via API-based infrastructure in accordance with applicable regulatory frameworks."

  While technically correct, this wording is too abstract and difficult for most users to interpret.

- **Designing consent flows that limit genuine choice or obscure withdrawal**
  Customers should be able to grant, review, and revoke consent without friction. Consent

must be treated as an ongoing permission, not a one-time, irreversible commitment. For example:

A fintech allows users to grant consent during onboarding but requires them to contact customer support or navigate multiple hidden settings to revoke access.

This creates friction and gives the impression that consent is effectively permanent.

6.4. Lessons from other markets on UX, trust, and adoption

Experiences from established Open Banking markets such as the **UK, Australia, and parts of the EU** show that adoption is driven not only by regulation, but by how clearly value and control are communicated to users.

6.4.1. Simplicity drives participation

Research and practice in the UK indicate that *short, focused consent journeys* significantly increase completion rates compared to long, multi-step flows. Open Banking UX guidelines there emphasise simplicity and clarity in consent screens to reduce user hesitation and drop-off. *(Source: Open Banking Implementation Entity (OBIE insights on consent and customer experience)*

Practical To-Do:

- Design consent flows that ask for *only what's necessary*, use clear, non-technical language, and minimise steps between introduction and approval.

6.4.2. Consistency and transparency build trust

Studies in Australia show that users are more likely to trust and reuse Open Banking-enabled services when they understand what data is being accessed, why it is needed, and how it is protected. Consistent messaging across consent screens, product interfaces, and ongoing communication reduces ambiguity and reinforces confidence.
(Source: Australian Open Banking design and consumer research reports.)

Practical To-Do:

- Use consistent terminology and visual cues about data use across all customer touchpoints.

- Include security reassurance statements (e.g., “Encrypted and consent-controlled access”) where users expect them.

6.4.3. Clear outcomes matter more than feature breadth

European experience shows that products focusing on *one clearly defined outcome* tend to outperform “feature bundles” in early adoption. For example:

- Account aggregation apps that clearly show all balances in one view,
- Payment facilitation tools that simplify a specific payment type, rather than platforms that try to serve many unrelated functions at once.

Practical To-Do:

- Launch with a focused value proposition that solves a *specific customer problem*; expand gradually only after achieving product-market fit.

6.4.4. Feedback loops reinforce confidence

In mature markets, fintechs that implemented real-time notifications (e.g., when data is accessed, when consent is about to expire) saw higher reuse and lower churn. Providing users with control points such as quick consent dashboards and easy revocation contributes to a stronger sense of ownership and safety. *(Source: UX research syntheses from UK/AUS Open Banking experience.)*

Practical takeaway:

- Implement clear notifications and a user-accessible consent dashboard.
- Let users easily see and revoke active consents without friction.

These experiences indicate that thoughtful experience design is a critical adoption lever. Fintechs that prioritise clarity, restraint, and customer understanding are better positioned to build durable trust within the Open Banking ecosystem.

7. Consent management

Consent management is a continuous operational responsibility, not a one-time onboarding step. Effective consent management ensures that data access remains aligned with the customer's original intent and that permissions do not persist beyond their approved purpose, scope, or duration.

The following are possible grey areas in consent management which fintechs must learn to navigate:

7.1. Handling consent as a system and not a UI/UX feature

Many fintechs may make the mistake of stating the consent purpose in UI screens but fail to enforce it technically. Once data enters internal systems, it can unintentionally flow into analytics models, credit engines, marketing tools, or partner platforms.

Banks are regulator-facing and will assess whether fintech architectures prevent purpose drift. NDPR principles around lawful processing will only amplify this expectation. Fintechs should:

- Tag datasets with machine-readable purpose metadata at ingestion.
- Implement purpose-based access controls, not just role-based ones.
- Separate environments for decisioning, marketing and analytics data
- Align their consent flows with bank-side consent infrastructure requirements – specifically capture, verification, registry, enforcement, revocation, and audit, as detailed in Section 5.2.2 of the guide for Banks.

7.2. Automating the consent lifecycle

In this instance, consent may be captured well but expiry and renewal are left to chance. Fintechs may assume that the bank will enforce expiry and so banks stop releasing data but fintechs continue processing previously stored data. Fintechs should:

- Build a consent orchestration service, not a database table.
- Attach expiry timestamps to datasets.
- Trigger automated workflows:
    - Suspend processing
    - Request renewal

    - Delete/anonymise data

7.3. Auditability of consent artefacts

Fintechs may store proof of consent but cannot easily reconstruct the exact approval context months later. This is critical because banks and regulators typically want answers to:

- What exactly did the customer approve?
- Which version of the consent screen was shown?
- What authentication method was used?

The practical approach to this is to store immutable consent artefacts, including:

- Timestamp
- Consent version
- Data scope
- Purpose
- Authentication method
- Channel

8. Partnership strategy and ecosystem participation

Open Banking operates as an ecosystem rather than a standalone value chain. Fintechs must therefore approach partnerships as strategic levers that shape speed, credibility, and scale, rather than as purely technical integrations.

8.1. Types of partners

Fintechs engage with multiple partner categories in Open Banking, each serving a distinct role in enabling access, distribution, or operational resilience. Clarity on partner type helps fintechs structure relationships intentionally.

- **Banks (as data providers and distribution partners)**
  Banks provide regulated access to customer data and, in some cases, act as channels for product distribution or co-creation.
- **Aggregators and Open Banking platforms**
  Aggregators simplify connectivity across multiple institutions, accelerating time-to-market while introducing shared dependency risk.
- **Infrastructure, Security, and Compliance service providers**
  These partners supply foundational capabilities such as identity, consent, monitoring, and security that reduce operational and regulatory burden.

8.2. Build versus Partner Decisions

Open Banking requires fintechs to make explicit choices about ownership. Not all capabilities should be built internally, but those that define competitive advantage and customer value should remain under direct control.

8.2.1. Capabilities Fintechs should own internally

Fintechs should prioritise internal ownership of capabilities that differentiate their core offering in the market and within the Open Banking ecosystem, such as:

- **Product logic and decisioning models**
  The rules, algorithms, and workflows that determine how data is translated into customer outcomes.

- **Customer experience and consent flows**
  The design and behaviour of onboarding, consent, and in-product experiences that directly shape trust and adoption.
- **Data interpretation and enrichment layers**
  How raw Open Banking data is transformed into insights, scores, recommendations, or actions.
- **Business rules and control logic**
  Internal thresholds, validation rules, and safeguards that govern how products respond to data quality or risk signals.
- **Strategic product roadmap and iteration cycles**
  Ownership of product direction, prioritisation, and evolution based on customer and market feedback.

8.2.2. Capabilities better sourced externally

Capabilities that are essential but not differentiating are often more efficiently sourced through partnerships, including:

- **Bank connectivity and API aggregation**
  Technical integration layers that provide access to multiple financial institutions.
- **Compliance and regulatory tooling**
  Consent management utilities, audit tooling, and reporting systems aligned with regulatory expectations.
- **Security infrastructure and monitoring**
  Identity, encryption, logging, and threat detection services that benefit from scale and specialisation.

8.2.3. Evaluating trade-offs

Build-versus-partner decisions should be evaluated across four main dimensions: how they affect launch timelines, strategic flexibility, long-term cost, and dependency exposure.

- **Speed**: Impact on time-to-market and implementation effort
- **Control**: Degree of flexibility and autonomy retained
- **Cost**: Upfront investment versus long-term operational expense

- **Risk**: Dependency exposure and failure impact

9.3. Ecosystem positioning

Open Banking expands what fintechs can do, but not every fintech should try to play every role. The most successful participants are deliberate about where they sit in the value chain, because positioning decisions shape architecture, regulatory exposure, and partnership strategy.

In Nigeria's bank-led regulatory model, where banks retain significant accountability for data sharing, fintech positioning also influences how quickly institutions are willing to connect and collaborate.

9.3.1. Acting as a product company versus a platform enabler

FinTechs can create value in the Open Banking system either as:

- **Product companies**
  Focused on owning the end-customer relationship, delivering differentiated experiences, and competing on outcomes and usability.
- **Platform enablers**
  Providing infrastructure, capabilities, or services to other businesses, competing on reliability, scale, and integration depth.

9.3.2. When to lead product innovation

- You have deep insight into a specific customer problem
- You control the customer experience end-to-end
- Speed and iteration provide a competitive advantage

9.3.3. When to integrate, collaborate, or enable other players

- Distribution, compliance, or scale advantages sit with partners
- Regulation favours shared responsibility
- Value is created through ecosystem-wide participation rather than exclusivity

10. Risk, governance, and operational sustainability

10.1. Integrated governance for Open Banking operations

As Open Banking becomes part of live products, governance must function as an operating discipline, not a policy document. In practice, this means fewer theoretical controls and more clarity about **who decides, who responds, and who carries the risk** when something goes wrong. Your team should be able to answer practical questions such as:

- Who approved the data use?
- Who should stop the flow?
- Who calls the bank?
- Who informs customers?

As mentioned before, banks are often held accountable for ecosystem failures. As a result, they prefer partners that demonstrate operational discipline even if those partners are smaller.

10.1.1. Governance embedded in product development

Do not wait for compliance review after a feature is built. Instead, introduce lightweight checkpoints that confirm:

- If the data request is proportionate to the use case
- If the consent wording is clear
- If access be revoked instantly if needed
- If logs are available for audit

10.1.2. Clear functional ownership

The lightweight nature of fintech teams may serve as an advantage where speed is concerned but may also easily become a governance challenge. While filling multiple roles early on may be impractical, clear ownership must be determined across the following areas:

- **Product:** What data is being requested and why
- **Engineering:** How it is accessed and secured
- **Compliance/Risk:** Whether the use is defensible
- **Operations:** How incidents and disputes are handled

10.1.3. Governance scaling with growth

What works at 5,000 users will very likely fail at 500,000. Early-stage fintechs often rely on founder judgement or informal coordination however this can quickly become fragile once multiple banks are connected and transaction volumes spike. Fintechs are better served introducing:

- structured approval flows
- incident playbooks
- audit trails
- partner reporting routines

10.2. Managing operational and reputational risk at scale

The rise in Open Banking usage will cause risk to shift from isolated incidents to systemic exposure. Fintechs must anticipate how scale amplifies the impact of failures across operations, partners, customers, and public perception.

Managing operational and reputational risk at scale requires fintechs to:

- **Recognise that operational risk increases non-linearly with usage**
    - Small data or service issues can affect large customer segments simultaneously
    - Manual workarounds become less effective as volume grows
    - Incident response speed becomes as important as root-cause resolution
- **Actively manage dependency and concentration risk**
    - Identify critical dependencies on single banks, aggregators, or providers
    - Define fallback options or redundancy for high-impact integrations
    - Regularly reassess whether partner risk has increased with usage growth
- **Treat third-party failures as first-order reputational risk**
    - Assume customers will attribute outages or errors to the fintech, not the partner
    - Align communication and escalation plans with partners in advance
      Avoid public ambiguity around responsibility during incidents
- **Strengthen internal controls as Open Banking becomes business-critical**
    - Move from informal oversight to defined approval and escalation thresholds
    - Introduce clearer operational ownership for high-risk products or flows
    - Ensure controls evolve alongside product adoption and revenue reliance
- **Align growth decisions with operational readiness**

- Pace new use cases and partnerships against system and team capacity
- Avoid scaling products faster than monitoring, support, and risk controls
- Treat reliability and trust as prerequisites for expansion, not outcomes

11. Go-live readiness and continuous evolution

11.1. Assessing go-live readiness through strategic pilots

Before ecosystem regulation is fully operational, we recommend that fintechs approach Open Banking through controlled pilots (two for a start) rather than broad integrations. Early success depends less on scale and more on demonstrating operational discipline and risk awareness. These are factors banks weigh heavily when enabling connectivity.

Fintechs may begin with one anchor bank (at most two) during the pilot phase. Anchor institutions should ideally be digitally progressive and partnership-oriented.

The pilot phase should be viewed as an extended production environment.

11.1.1. Sample pilot: data access and connectivity

Objective: Prove the fintech can connect securely and manage customer data responsibly. Connect with banks (.e.g. Sterling Bank and Stanbic IBTC) and launch a narrow use-case such as:

- Account aggregation
- Transaction retrieval
- Income verification

Control exposure by limiting the pilot to a defined customer cohort (e.g., employees or beta users), enabling close monitoring of system behaviour and customer experience.

Key areas to observe include consent completion rates, data accuracy, latency, support queries, and integration stability.

Progression signal: Expand only when integrations are reliable, consent behaves predictably, and operational teams can confidently support the journey.

11.1.2. Sample pilot: decisioning and controlled financial outcomes

Objective: Demonstrate the ability to act responsibly on Open Banking data in order to enable outcomes. Introduce low-risk, tightly governed financial use cases such as:

- Pre-qualified microloans
- Risk-based onboarding
- Intelligent payment routing

Exposure limits are critical at this stage. Fintechs should maintain fallback decision frameworks rather than relying entirely on newly accessed data, recognising that early ecosystem connectivity may present inconsistencies.

11.1.3. The role of aggregators

Aggregators can accelerate early connectivity by simplifying multi-bank integrations and normalising data formats. However, fintechs should recognise the trade-off between speed and infrastructure control. As a mature player, you may adopt a hybrid approach over time combining aggregator access with selective direct bank integrations.

11.2. Iterating products as standards and regulations evolve

Open Banking standards, regulatory expectations, and ecosystem norms will continue to evolve after go-live. Fintechs should assume change as a constant and design both products and operating models to adapt without disrupting customers or partners.

Rather than treating iteration as an exception, fintechs should institutionalise it as part of normal operations.

Effective iteration in Open Banking requires three disciplines:

- **Designing for change, not permanence**
  Products and integrations should be built with the expectation that APIs, consent requirements, and data standards will change over time. This includes avoiding hard-coded assumptions and enabling modular updates to critical flows.
- **Maintaining regulatory and standards awareness**
  Fintechs should actively track updates to Open Banking standards, regulatory guidance, and ecosystem practices, ensuring that product and operational changes keep pace with evolving expectations.

- **Operationalising controlled updates and improvements**
  Changes to Open Banking functionality, whether driven by regulation, partner updates, or product learning, should follow defined change-management processes that minimise customer disruption and operational risk.

In practice, this means fintechs should be able to:

- Update consent flows and disclosures without redesigning core products
- Adjust data handling or validation logic as standards mature
- Coordinate changes with banks and partners ahead of production deployment
- Test and roll out updates incrementally rather than through disruptive releases

11.3. Planning long-term Open Banking roadmaps

Beyond being a one-time integration or regulatory response, Open Banking should be planned as a long-term business capability. A clear roadmap helps fintechs align product ambition with operational readiness and avoid fragmented or reactive expansion.

In developing a long-term Open Banking roadmap, fintechs must design the roadmap to:

- **Clarify the strategic role of Open Banking in the business**
  - Define whether Open Banking is central to the product offering, a supporting capability, or an enabler for future services
    Ensure Open Banking initiatives are tied to clear business outcomes.
- **Phase use cases deliberately as capability matures**
  - Prioritise use cases that deliver clear value with manageable operational complexity
  - Introduce more advanced or risk-sensitive use cases only as systems, controls, and teams mature
- **Build capabilities incrementally**
  - Invest progressively in data infrastructure, monitoring, risk controls, and operational tooling
    Design components that can be reused across products, partners, and future integrations
- **Anticipate future partnerships and ecosystem roles**
  - Identify where deeper collaboration with banks, platforms, or enterprise partners may be required

    - Structure architecture and commercial arrangements to support expansion without significant rework
- **Review and adjust the roadmap over time**
    - Treat the roadmap as a living plan informed by adoption data, regulatory updates, and market feedback
    - Use learnings from early use cases to refine priorities and sequencing

With a well-defined Open Banking roadmap, fintechs can convert regulatory access into sustained competitive advantage, while scaling responsibly and maintaining operational resilience.