Global Approaches to Open Banking Regulation

Konsentus

Open banking is transforming financial services by enabling consumers to securely share their financial data with third-party providers (TPPs). While the core principles of open banking are consistent (i.e consumer data ownership, interoperability, innovation and fostering competition) the regulatory frameworks governing it vary significantly across the globe. There is a spectrum of regulatory approaches to open banking, from market-driven initiatives to highly prescriptive, government-mandated systems. However, there is no universally 'correct' model with each country's approach shaped by its legal system, financial infrastructure, policy goals and consumer protection priorities.

Open banking is an evolving global phenomenon that promotes innovation, competition and customer-centricity in financial services. At its core, open banking enables consumers to authorise secure access to their banking data by third-party providers (TPPs), unlocking new services like personal finance tools, alternative lending and payment initiation.

Despite shared objectives, countries have adopted markedly different approaches to open banking regulation, ranging from market-led frameworks with minimal regulatory intervention to comprehensive government-mandated regimes.

Examples of open banking regulatory models

Market-Driven
(Non-Regulatory) Environments

Hybrid
Collaborative Models

Fully Regulated
Mandated Environments

Regulatory approaches

The key factors that determine the regulatory approach for a given jurisdiction include, but are not limited to: governmental policy goals, legal traditions, consumer protection priorities, financial market maturity and most importantly - stakeholder readiness.

Regulatory Approaches

Access to data and information is a key enabler for financial inclusion. Konsentus supports central banks, regulatory authorities and NGOs in creating and operating accessible and standardised market infrastructures.

No One-Size-Fits-All

Open banking has no universal blueprint. From the regulated open banking environments to the market-led models, each jurisdiction has crafted its own path based on its unique context. The diversity of approaches highlights the need for flexibility, stakeholder collaboration and continuous evolution.

There is no definitive 'right' or 'wrong' way to implement open banking. The success of an open banking initiative and ecosystem depends on:

- Alignment with national objectives and government policy
- Integrating with existing infrastructure
- Implementation strategy (phased vs. full-scale)
- Extent of Regulatory Reach/Regulatory Oversight (banks, fintechs, etc.)
- Participation model (voluntary vs. mandatory)

The approach taken may evolve, as demonstrated in India where they have moved from voluntary to structured, and the U.S. which has adopted formal rules (i.e Dodd-Frank 1033 Act) in place of a market-driven approach.

Open banking has no universal blueprint. From the regulated environment of the EU to the market-led model of Singapore and Japan, each jurisdiction has crafted its own path based on its unique market environment. The diversity of approaches highlights the need for flexibility, stakeholder collaboration and continuous review. Ultimately, the goal remains the same: to empower consumers, promote competition and foster innovation in financial services.

The Need for Open Banking Trust Frameworks

In a highly inter-connected environment, trust between participants is paramount. A Trust Framework defines the legal, technical, operational and governance foundations that allow disparate entities such as banks, fintechs, regulators and consumers to interact securely and reliably.

Without a coherent Trust Framework, inconsistencies in security, identity management, onboarding processes and data handling can lead to fragmentation, security vulnerabilities a decline in adoption and loss of consumer confidence. A well-defined framework mitigates these risks by establishing common expectations and requirements for all ecosystem participants.

Adopting International Standards and Rulebooks

A core component of any Trust Framework is the adoption of international standards and rulebooks. These define the roles, responsibilities and behaviours of participants, creating a predictable and interoperable environment.

Standards

Open standards such as ISO 20022, OAuth 2.0, OpenID Connect and FAPI (Financial-grade API) ensure interoperability and secure data exchange across borders

Rulebooks

These codify obligations for data sharing, customer consent, liability models, dispute resolution and service level agreements (SLAs)

Using globally accepted standards reduces technical fragmentation, accelerates ecosystem maturity and enables cross-border collaboration. Rulebooks provide a unified guide for operations and compliance, promoting fairness and predictability.

Directory Services

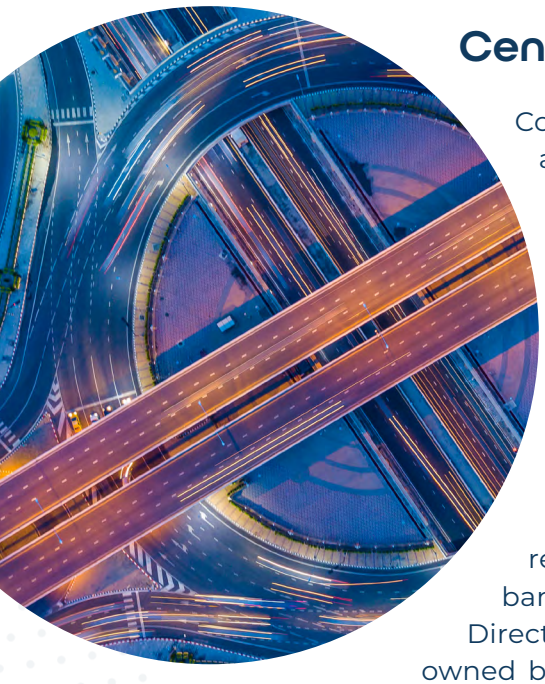
In environments where regulatory oversight of open banking third-party providers (TPPs) is absent, Directory Services become essential to establish a level of transparency, trust, security, surety and operational efficiency. Directory Services help create a structured, accessible way to manage and authenticate participants within the open banking ecosystem. By implementing such services in a distributed manner, the ecosystem can maintain flexibility, scalability and reliability.

Directory Services are the cornerstone of the Trust Framework in the open banking ecosystem. They provide a verified register of all authorised participants, including banks, TPPs and regulatory entities.

Directory Services act as a central or distributed repository that holds information about entities (e.g., banks, TPPs, consumers, etc.) participating in the open banking ecosystem. The core purpose of these services is to enable seamless and secure connections between entities within open banking while ensuring compliance with technical and regulatory requirements. Key functions of Directory Services include:

- Participant Registration and Authentication
- Directory Listing and Discoverability
- Certification and Compliance Verification
- TPP Access Control and Permissions
- Real-time Updates and Monitoring

Directory Services support automated trust establishment and streamline technical integrations by serving as a single source of truth for participant metadata and digital certificates.



Central vs Distributed Directory Services

Countries such as the United Kingdom, Australia and Brazil have all implemented central Directory Services to support the implementation, development and growth of their open banking ecosystems giving the financial supervisor oversight of all legally regulated ecosystem participants.

In other countries, where financial supervisory oversight does not extend to third-party service providers, they have adopted a distributed approach to Directory Services (e.g. Chile & USA). In this scenario, the Competent Authority regulates the activities and accreditation of the Credit Institutions (i.e. banks), but the responsibility for ensuring third-party providers comply with the relevant regulatory requirements is passed to the Data Providers (i.e. banks) and/or nominated service providers. In this model construct, Directory Services are spread across multiple, federated systems, each owned by different stakeholders (e.g., banks, services providers etc.). These systems would maintain their own records but cooperate to create a unified directory accessible to all participants, giving each participant control over their own information while still enabling them to interact securely with other entities.

Centralised vs Distributed Directory Services

Feature	Centralised Directory	Distributed Directory
Governance	Simple, top-down	Complex, multi-party
Security	Strong but vulnerable	Resilient and decentralized
Scalability	Limited	High
Innovation	Slower	Faster, decentralized
Transparency	Controlled	Transparent by design
Compliance & Auditing	Easier	Complex, peer-based
Risk of Outage or Failure	High	Low

Both approaches to Directory Services are valid, with the model a market adopts primarily driven by the breadth of entities under the Financial Regulator's legal oversight.

Administration of Directory Services in a Distributed Ecosystem

Administering a distributed Directory Service requires effective governance mechanisms and agreed-upon standards for data sharing and updates. The key components of administration include:

a) Decentralised Governance

Without regulatory oversight, it is crucial to establish a decentralised governance framework. A trusted industry body or consortium could manage the governance, ensuring that participants adhere to agreed-upon standards and policies. This body would:

- Set the rules for data entry, validation and updating records within the directory.
- Ensure that any new entities joining the ecosystem are authenticated and meet security standards.
- Facilitate dispute resolution and encourage compliance with the framework.

b) Authentication and Authorisation

Directory Services must be able to authenticate participants, ensuring that they are legitimate and authorised to interact in the ecosystem. This can be achieved through a combination of:

- Public Key Infrastructure (PKI): Ensures cryptographic trust and secure communication.
- OAuth 2.0 and OpenID Connect: Enable authorised access to Directory Services through token-based authentication.

c) Real-Time Updates and Monitoring

Distributed directories must be updated in real time to reflect new participants, changes in credentials, or updates in compliance status which requires:

- Event-driven mechanisms: When an entity updates its information (e.g., new certification), the update is broadcast to the network.
- Monitoring and auditing tools: To ensure integrity, the system needs to include auditing mechanisms to track changes and ensure compliance.

d) Interoperability and Standardisation

For a distributed directory service to function seamlessly, it must be compatible across various platforms and technologies. Standardisation of data formats, security protocols and governance rules are critical. Common standards such as REST APIs for directory access, JSON Web Tokens (JWT) for identity management and ISO/IEC 27001 for security compliance could be adopted.

The Advantages of Distributed Directory Services

The benefits of adopting a distributed Directory Services architecture within a given jurisdiction include:

Enhanced Trust	With a decentralised and transparent system, participants can trust the authenticity of the directory and its information
Security and Privacy	The use of encryption, cryptographic signatures, and decentralised validation protocols ensure the protection of sensitive data
Scalability	As the ecosystem grows, the directory system can scale without relying on a central authority, ensuring responsiveness to demand
Reduced Single Point of Failure	The distributed nature of the system ensures that even if one node fails, the directory service continues to operate smoothly

Conclusion

The development of a trusted and secure open banking or open finance ecosystem requires more than just API access, it demands a cohesive and comprehensive Trust Framework. By adopting international standards, implementing rulebooks, establishing central Directory Services and investing in technical conformance testing and tooling, ecosystems can ensure safety, scalability and efficiency. Trust Frameworks not only reduce risk but also accelerate innovation by providing a consistent and secure foundation for all participants.

Trust Frameworks are underpinned by Directory Services, which can be deployed in a variety of ways, typically shaped by government policy and the extent of regulatory oversight within a given jurisdiction. These Directory Services should be designed and implemented in alignment with the country's regulatory governance structure, ensuring they support the principles of transparency, trust, security and surety. When deployed effectively, they provide a foundation for confidence among consumers and businesses, reinforcing the integrity and resilience of the open banking ecosystem.

As trust continues to evolve and expand, the countries and regions that make it a priority will be better positioned to deliver consumer-centric financial services, driving economic growth and building resilient digital economies.

About us

Konsentus provides specialist advisory services and technology solutions to support the national implementation of open finance ecosystems. Subject matter experts, Konsentus advisors have a proven track record in navigating complex, multi-stakeholder ecosystems and understanding individual regulatory and market requirements.

Konsentus' award-winning technology powers national open finance infrastructures. Modular and scalable by design, our solutions are tailored to individual market requirements, enabling ecosystem participants to seamlessly identify each other and interact within a safe and trusted environment.

Konsentus is ISO 27001 certified.

Keep up to date:

To find out more, get in touch at:
info@konsentus.com

www.konsentus.com