FOCUS NOTE

OPEN BANKING IN THE CONTEXT OF FAST PAYMENTS

PROJECT FAST

FRICTIONLESS · AFFORDABLE · SAFE · TIMELY · TRANSACTIONS

AUGUST 2023

WORLD BANK GROUP

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

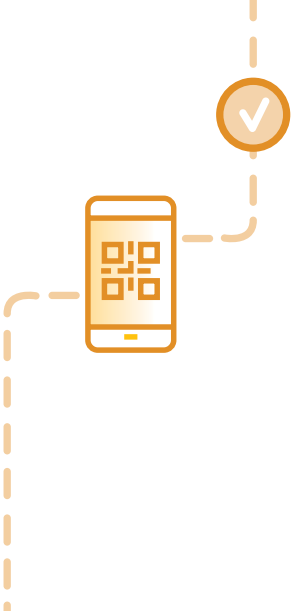
CONTENTS

1 SETTING THE CONTEXT

The World Bank has been monitoring closely the development of fast payment systems (FPS) by central banks and private players across the globe.[1] This comprehensive study of FPS implementations has resulted in a policy toolkit. The toolkit was designed to guide countries and regions on the likely alternatives and models that could assist them in their policy and implementation choices when they embark on their FPS journeys. Work on the FPS Toolkit was supported by the Bill & Melinda Gates Foundation under Project FASTT (Frictionless Affordable Safe Timely Transactions). The toolkit and other relevant resources under Project FASTT can be found at fastpayments.worldbank.org and consist of the following components:

1. The main report *Considerations and Lessons for the Development and Implementation of Fast Payment Systems*
2. Case studies of countries that have already implemented fast payments
3. A set of short focus notes on specific technical topics related to fast payments

This note is part of the third component of the toolkit and aims to provide input and guidance to policy makers on maximizing the potential synergies between open banking and fast payments.



2 BACKGROUND

Payment ecosystems have undergone a significant transformation over the last decade. The rate of payment digitalization has rapidly increased in response to technological advancements and the development of new payment products and services. Consumers and businesses can now access a wide range of convenient and customer-centric digital payment products and services. The entry of new players has led to increased collaboration between traditional banks and third-party service providers, enabling the adoption of new business models.

The development of open banking services alongside the adoption of fast payments has driven many of these changes. Fast payments and open banking services are natural complements, and their integration generates synergies that can enable the more rapid adoption of both. Although models for providing open banking services vary, fast payment systems (FPS) can provide the necessary infrastructure and governance framework to enable the secure transfer of data between banks and third-party service providers. For example, FPS can be used to offer payment initiation functionality, develop application programming interfaces (APIs) to connect with other systems, and implement security protocols to protect sensitive financial data shared in an open banking context.

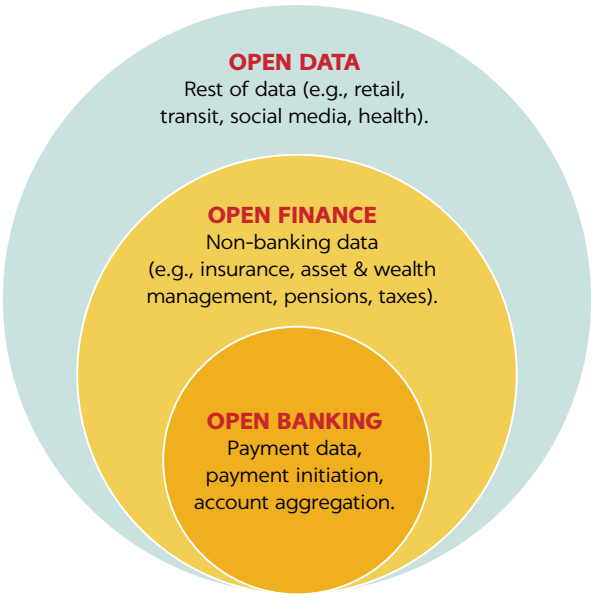
This report sheds light on the benefits that arise from leveraging FPS as a platform for the development of open banking services. It considers the various opportunities that arise in doing so and analyzes the implementation strategies taken in four different markets. It concludes with a set of best practices and recommendations for FPS operators and regulators as they consider how to maximize the synergies between open banking and fast payments.

2.1 THE DEVELOPMENT OF OPEN BANKING AMID TODAY'S DIGITAL PAYMENT LANDSCAPE

Open banking refers to the ability of third-party service providers to gain secure and permissioned access to users' account information. It allows users greater control over their banking data and enables third-party service providers to develop an array of new digital financial services. Both open banking and open finance can create an environment where traditional financial institutions are driven to improve their offerings and provide better, more innovative services to consumers and businesses. The resulting competition can lead to lower prices and increased accessibility and enable better choices for consumers. With access to more information, they can make more informed decisions, access a wider range of financial services, and benefit from new data-driven financial products and services. The concept of open data goes beyond open banking and open finance, encompassing data from other sectors, such as transit, social media, energy, telecommunications, health, and government records. The ultimate objective of open data is to provide consumers and firms with a holistic view of their data through a single platform.

In some markets, open banking regulations developed in response to the emergence of market-driven innovations

FIGURE 1 Distinguishing between Open Banking, Open Finance, and Open Data



Source: World Bank.

around payment initiation and account information services. In other markets, regulators sought to increase competition, innovation, and security in the financial sector, considering the growing demand for consumers to have greater control over their financial data. Concerns over data privacy and security amid rapid digitalization have also played an important role in the development of open banking regulations, as consumers have increasingly demanded greater agency over their financial data and the assurance that their data will be handled securely and transparently when shared.

Previously, data was obtained exclusively through methods such as screen scraping and reverse engineering, but industry standards and regulations now encourage or mandate the use of secure APIs for data sharing.[2] Some markets—including the European Union through the revised Payment Services Directive (PSD2) and Australia through the Consumer Data Right legislation—have mandated that banks share data and that third-party providers register with regulatory authorities.[3] Other markets do not have mandates, but regulators have provided the industry with recommendations and guidelines, including open API standards. For example, the Canadian government has issued guidelines for financial institutions on open banking, including recommendations for data security and privacy and guidance on API development.[4] Similarly, the Monetary Authority of Singapore has published guidelines for financial institutions on open banking, including recommendations for API standards and security, and requirements for customer consent for data sharing.

In today's open banking landscape, account information service providers (AISPs) and payment initiation service providers (PISPs) are the most common types of players. AISPs offer services such as balance inquiries, transaction history, and account aggregation. They act as intermediaries between customers and financial institutions, allowing customers to access information from their accounts such as account balances from several accounts, or their transactional history. PISPs initiate payments from customer bank accounts with the explicit consent of the account holder. Just as AISPs access customer data, PISPs can establish connections to bank APIs directly or utilize a single API hub provided by another service provider to connect with multiple banks. Payment initiation services are particularly compelling in a fast payment context and are therefore the focus of this report.

2.2 SYNERGIES BETWEEN OPEN BANKING AND FAST PAYMENTS

Both open banking and fast payments are designed to cater to increased consumer demand for instant and secure financial transactions. Leveraging fast payments in the context of open banking and vice versa can enhance the benefits of each by streamlining user experience, fostering interoperability, and minimizing the operational complexity required for data sharing between institutions. The synergies that arise in doing so can make it easier to achieve such policy goals as fast payment adoption, financial inclusion, and digitalization. These benefits are described in detail below.

More rapid fast payment adoption. Adoption of fast payments has tended to be low in markets where user experience is poor and system functionality limited, such as South Africa. Although the country's Real-Time Clearing was launched in 2006, its adoption has been limited until now partly due to factors such as low availability for users, absence of proxy payment services, and high pricing. Payment initiation is one of several potential tools that can help increase fast payment adoption in this instance.

The development of payment initiation services for fast payments can support migration away from cards for consumer-to-merchant transactions, which can benefit merchants in several ways. First, accepting account-to-account payments is often cheaper than accepting card payments. Moreover, the immediate availability of funds can provide merchants quicker access to liquidity and more flexible cash-flow management. In contrast, merchants often need to wait to access funds from card payments. The benefits of

immediate payments are particularly relevant in markets or sectors where merchants require funds daily to serve their liquidity needs.

Greater competition at the front end drives innovation and increases user choice. Payment initiation services simplify the payment process and reduce frictions at checkout, significantly enhancing user experience. This creates greater competition at the front end and allows consumers and businesses access to a wider range of innovative products and services. Service providers can develop solutions that are tailored much more to the specific needs of their customer. For businesses, these services could include advanced payment options, customized financial-management tools, and streamlined access to financial services.

Enhanced data portability prevents "lock-in" and enables customers to switch between service providers more easily. Weak competition in digital payments has been common in many markets historically, contributing to a lack of innovation and limited choice for users. When banks have access to more data about their customers (both consumers and businesses) than the other groups, customers are often unable to make fully informed decisions. Similarly, new players may be limited in their ability to enter the market and offer comparable products and services. The advent of open banking and inclusive fast payment ecosystems has helped alleviate this issue by disrupting traditional banking practices and facilitating the entry of new market players. At the same time, it forces service providers to improve user experience if they want to retain users.

New opportunities to strengthen the security of fast payments. The implementation of robust customer authentication for payment initiation can leverage existing fraud-prevention techniques and processes, simplifying the management of issues concerning fraud and unauthorized payments. Additionally, as sensitive customer data is not shared with the merchant if the payment is initiated via a PISP, the risk of fraud resulting from merchant data breaches is lower.

2.3 USE CASES FOR THIRD-PARTY PAYMENT INITIATION

The development of payment initiation services allows customers to initiate fast payments directly from their bank accounts to a recipient's account using a third-party platform or service. This provides customers with a more streamlined, simple, and efficient payment experience. Payment initiation services can be used to promote the adoption of fast payments for the following use cases:

Consumer-to-merchant transactions: For in-store point-of-sale transactions, payment initiation services can be integrated with third-party mobile applications to enable consumers to pay for goods and services instantly using their bank account instead of a card. As an example, third-party users can scan the merchant's QR code or input the merchant's proxy/alias to initiate a fast payment from the user's account (held at an account provider) to the merchant's account. In this example, the third party initiates a payment from the user's bank account to the merchant's account on the user's behalf. Similarly, for an e-commerce transaction, the user may utilize a third party to initiate a fast payment from the user's bank account to the merchant's bank account. In some cases, the merchant itself can act as a third party or partner with one to enable payment initiation. This allows customers to complete their transactions quickly and easily and may result in increased customer loyalty and revenue for merchants. It could also reduce the risk of cart abandonment for e-commerce transactions, as customers may be more likely to abandon a purchase if the payment process is too complex or time-consuming.

In Brazil, the Banco Central do Brasil (BCB) embedded payment initiation in Pix. Through this mechanism, merchants can manage Pix on their online platforms, eliminating the need for online shoppers to access their bank's app to complete a payment and reducing the complexity of the transaction flow. Customers can select the "Open Finance" option at checkout on digital platforms to make payments using this method. Once the selection is made, customers will be redirected to their financial institution, where they can enter their credentials and confirm the payment with ease. (Table 1 presents the online payment flow for Pix transactions with and without payment initiation.)

Bill payments and variable recurring payments: The market is still exploring potential use cases for open banking services for bill payments and other types of recurring payments. Variable recurring payments in the United Kingdom and PayTo in Australia have emerged as a new type of open banking service that allows customers to instruct third-party service providers to make payments from their bank account on their behalf in line with agreed limits.[5] These services, when used to initiate fast payments, could

TABLE 1 **Online Payment Flow for Pix Transactions with and without Payment Initiation**

Default Payment Flow: Consumer to Merchant	Open-Banking-Linked Payment Flow: Consumer to Merchant
1. Customer initiates a payment on the merchant's website.	1. Customer selects Pix as the payment method on the merchant's website.
2. Customer receives a key from the merchant or scans a QR code.	2. Customer is directed to a payment screen to check the information and confirm the payment with various authentication methods.
3. Customer opens a mobile/online banking app	3. Customer is directed back to the merchant's website and receives confirmation.
4. Customer chooses the Pix payment option and adds the key or merchant information.	
5. Customer confirms the information and completes the transaction with various authentication methods.	
6. Customer returns to the merchant's website to check whether the payment has been confirmed.	

Source: Banco Central do Brasil.

potentially offer more control, speed, and transparency to customers, compared to existing alternative, such as direct debits or card-on-file instructions.

Sweeping: Another potential use case is using payment initiation services to transfer money between different current accounts, making it easier for micro, small, and medium-sized enterprises to manage their liquidity. In combination with account aggregation services, this process can be streamlined and automated (CPMI 2021). The Competition and Markets Authority in the United Kingdom recently directed nine banks to implement an open banking API for variable recurring payments, to enable easier sweeping of funds from a customer's current account to another of their accounts. Other similar use cases could include moving funds from current or savings accounts to investment accounts or loan accounts.

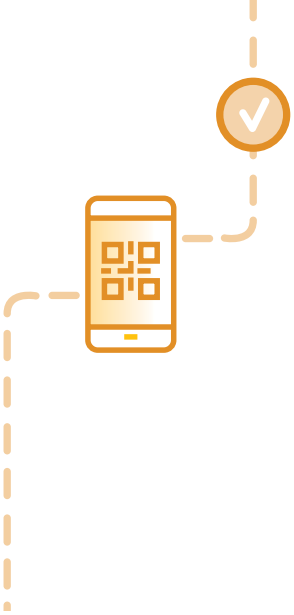
Funding mobile wallet and e-money accounts: Payment initiation services for fast payments could also be used to fund mobile wallet and e-money accounts held with a nonbank payment service provider (PSP)—that is, the third party. In this case, the nonbank PSP could act as a third party to initiate a payment from the user's bank account.

2.4 MODELS FOR THE DEVELOPMENT OF PAYMENT INITIATION SERVICES FOR FAST PAYMENTS

Promoting the development of third-party payment initiation services can be a complex endeavor and requires the integration of multiple business processes and technical aspects, such as customer authentication, APIs and QR codes, and data security and privacy, among others. In some markets, payment initiation by third parties has been explicitly addressed in open banking regulation or industry guidelines, while in others, this has not been the case. For example, in markets such as Mexico and India, open banking regulation does not explicitly cover payment initiation, while in Indonesia, for example, it does. In other markets, payment initiation was not considered as part of the initial scope for open banking, but industry regulators have expanded (or are seeking to expand) the scope to include payment initiation.

Regardless of the approach, FPS can also play an important role in providing shared technical infrastructure and governance for the development of payment initiation services. This does not replace a comprehensive governance framework for open banking, including API standards for payment initiation, authentication standards, and liability and dispute-resolution mechanisms, among others. When payment initiation is implemented in the context of a fast payment scheme, the scheme rules (as adapted) promote standardization and regulate relationships between the parties. Where FSP may provide a centralized API infrastructure, they can also help minimize costs of API development and implementation and reduce time to market of payment initiation services.

FPS operators can help expand user access and lower barriers to entry for potential new market entrants by enabling third-party initiation through their platforms. In the end, greater competition and the entry of new players are likely to lead to a more innovative and inclusive ecosystem that can better reach underserved or unbanked populations, granting them improved access to the advantages and opportunities offered by digital financial services.



3 DEVELOPING AN IMPLEMENTATION STRATEGY

Open banking implementation strategies have varied by market, reflecting the markets' unique priorities, challenges, and regulatory environments and resulting in diverse models that vary in scope, regulatory requirements, and the level of involvement of traditional banks and third-party service providers. Similarly, approaches to encourage the development of open banking services for fast payments may vary across countries and regions. In markets such as the European Union and United Kingdom, a relatively decentralized approach to providing payment initiation services has been implemented. In these examples, direct or brokered agreements link PISPs to account-holding institutions, which then access the relevant payment systems. However, in a market such as India, providing payment initiation services has been centralized through UPI. The FPS operator, the National Payments Corporation of India, provides technical access to third-party providers to offer payment initiation services assuming the providers' bank is a direct UPI participant and is willing to grant the third-party access to the system. Understanding the available implementation approaches and considerations can help stakeholders identify best practices and develop strategies for successful implementation.

3.1 API FRAMEWORKS

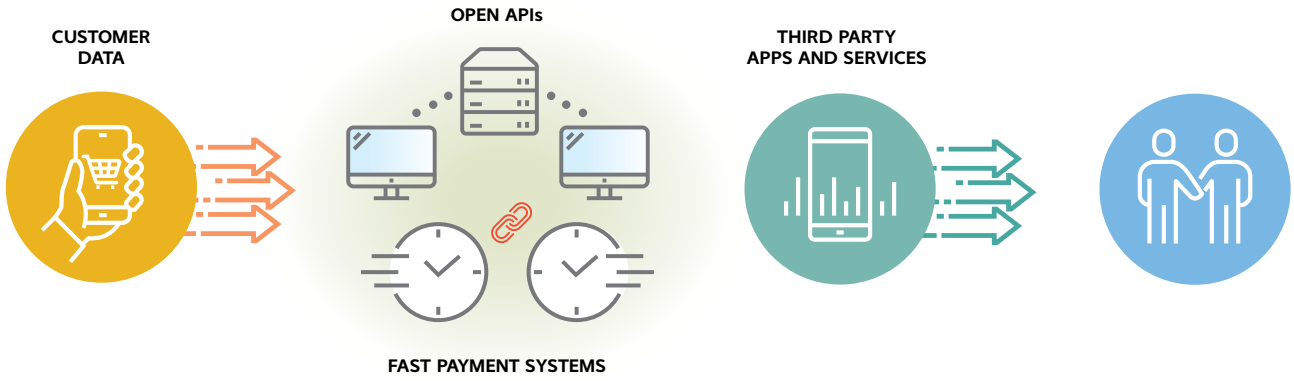
APIs are essential in open banking because they enable the secure and smooth exchange of data between different financial institutions and service providers. They facilitate the rapid transfer of data between different systems, enabling fast payment initiation and processing. In a fast payment context, APIs can also be used to create seamless payment experiences for customers and particularly businesses. APIs can be used for payment initiation and account verification to ensure that payments are being sent to the correct account, and APIs can provide real-time access to account information, enabling businesses and consumers to track their payment status and account balances in real time.[6] In some countries, such as Australia and Singapore, APIs for payments were part of a broader financial-services evolution to drive innovation across all aspects of banking. In other countries, such as Brazil and India, APIs for payments were specifically developed/mandated for use.

APIs can be used to facilitate communication between different players within the fast payment ecosystem, such as between the payer and the payer bank, the payer bank and third-party players, and the beneficiary bank and the merchant, among others. FPS operators are increasingly playing leading roles in creating standardized API frameworks or centralized hubs for third-party payment initiation.

Bilateral, Decentralized Approach: No Common API Standards

In countries where open banking is primarily market driven, banks and third-party service providers often rely on bilateral agreements and customized APIs to share data. These agreements outline the terms and conditions of data-sharing API access, usage, and security, as well as the responsibilities of both parties. In the absence of such agreements, access to bank accounts generally takes place through screen-scraping techniques, subject to no clear framework

FIGURE 2 **Encouraging the Development of Payment Initiation Services for Fast Payments**



Source: World Bank.

or external control on the third parties. This uncertainty, together with the exposure of personal log-in credentials, increases risks for consumers.

In some countries, regulators play an important role in ensuring that bilateral agreements are fair and balanced by setting clear rules and guidelines for data sharing. In Japan, regulators mandate that third parties establish individual bilateral agreements with banks, which provides greater protection for consumers and promotes fair competition. In Hong Kong, banks have the freedom to choose which third-party providers to collaborate with through bilateral agreements, providing more flexibility in terms of partnership arrangements. A bilateral, decentralized approach based on bilateral agreements requires clear and transparent guidelines to ensure that data sharing is conducted in a fair and secure manner. However, such agreements do not necessarily address market-fragmentation risks that arise from the lack of common standards across bank APIs.

Multilateral, Decentralized Approach: Standardized Frameworks

A common strategy taken by industry bodies, regulators, or other standard-setting organizations is to create a standardized API framework for open banking—a set of technical and business standards that enable different agents within the open banking ecosystem to communicate with each other seamlessly and securely. The development of a multilateral API framework can be led by the regulator or industry but often requires collaboration between the two spheres.

In North America, where open banking has generally been more market driven, the Financial Data Exchange has taken on the responsibility of creating a common API standard.[7] In New Zealand, a standardized API framework for payment initiation is governed by Payments New Zealand, which is an industry body that acts as the scheme operator for retail payments in the country.[8] In the euro area, the use of a single API standard for open banking was not defined by PSD2, which regulates open banking in the European Union. Rather, industry associations such as the Berlin Group have worked to define a voluntary common standard for account access.[9] In markets such as Brazil, the regulator has played a much more central role. For example, the BCB has mandated the use of its standardized APIs for payment initiation.

Standardized API frameworks can include a range of technical and business standards, such as data formats, protocols, authentication mechanisms, and security requirements. The usage of standardized API frameworks reduces the costs associated with building and maintaining proprietary or custom interfaces for data sharing. Technical standards for APIs in open banking include, among others, security protocols (such as OAuth), data formats (JSON), and communication protocols (REST). Business standards for APIs in open banking include standardization of data fields and services, such as account information, payments, and identity verification.

FPS operators can either play a role in developing an API framework for payment initiation or mandate the use of existing API frameworks created by the regulator or market. The benefits of this approach are that it creates a standardized way for third-party providers to connect via APIs to multiple banks. While this approach generally reduces the risk of market fragmentation, compared to the previous approach, it can still result in some fragmentation risks if use of the API framework is voluntary or if its use is mandatory but not rigorously enforced.

BOX 1 API DIRECTORIES

In some markets, an API directory is used to help third parties find and implement APIs that fit their business needs. The directories list APIs from multiple banks, but they do not provide a single point of access. The directories' main purpose is to provide a comprehensive list of APIs available from multiple banks, making it easier for PISPs to compare and choose APIs that meet their requirements. API directories may also provide additional information, such as technical specifications, usage limits, and pricing, to help third-party providers evaluate and select APIs. API directories consolidate existing APIs from multiple parties into one centralized source of information. However, they do not provide the same level of support and services as API hubs, as the primary focus is on providing a comprehensive list of APIs.

3.1.3 Multilateral, Centralized Approach: API Hubs

API hubs can be used in the context of open banking to give third-party providers access to APIs of financial institutions. API hubs are centralized platforms that offer a range of APIs from multiple financial or banking institutions in one place. These hubs provide a single point of access where third-party providers can find and access the APIs of multiple banks. They are designed to simplify access, making it easier for third-party providers to build and launch their products and services, and they are typically viewed as a tool to remove market-fragmentation risks.

API hubs typically provide additional services, such as documentation, testing tools, and support, to help third-party providers develop and test their applications. One approach is where FPS themselves handle data and transaction requests, ensuring efficient connectivity and standardized exchanges. Alternatively, independent hubs or platforms can be established, serving as centralized gateways for open banking interactions. These hubs simplify integration, foster collaboration, and enhance user experiences. Examples of API hubs developed and maintained by the FPS operator are in South Korea, where the Open Banking System enables multiple parties (including nonbank PSPs) to initiate payments and exchange information, and in Mexico, where Banxico, the central bank and operator of the country's FPS, is developing an API hub for payment initiation.

3.2 DATA INTEGRITY AND SECURITY

3.2.1 Data Quality

Data holders (for example, account providers and nonbank PSPs) must ensure that they maintain the accuracy, completeness, and timeliness of data shared with third parties, avoiding adverse effects on customer experience, reputation, and regulatory compliance. They also need to ensure that the APIs they provide are reliable, secure, and scalable enough to handle large volumes of data traffic, especially in a context where fast payments are gaining traction across the globe. Poor data within the API can lead to problems with reporting quality, searches, and analytics, creating problems for financial professionals or customer-facing employees who need to search for specific customer accounts and may find duplicate data for an individual. Duplicated records in online financial systems can cause discrepancies and take up unnecessary space, resulting in time and cost implications for a business. In other words, having incorrect data can potentially be damaging when making strategic decisions about products or other services, and it can mislead decision-makers and lead to poor strategic decisions.

In addition to ensuring the quality and integrity of data, data holders need to monitor the data flows to ensure that third-party providers are using the data only for authorized purposes and not misusing it. This may require data holders to have in place a robust data-governance framework that includes appropriate controls and policies to prevent breaches, ensure confidentiality, and minimize the risk of misuse. By implementing an effective data-governance framework, data holders can ensure that their data is secure and well managed and build customer trust in their services.

3.2.2 Data Security

APIs in open banking serve as a gateway to access sensitive customer data, including financial transaction history and personal information. Access to customer data should be granted upon explicit customer consent (that is, consent to access data to provide a specific service, as opposed to general consent to use data by the providers). Furthermore,

provisions must be in place so that AISPs do not retain indefinite access to sensitive information if the customer ceases to utilize their services.

The security of the API infrastructure must be robust enough to prevent unauthorized access or data breaches. In fact, poor data quality and security breaches can pose significant risks to open banking systems that use APIs. To avoid these risks, quality checks must be implemented to test data structures and ensure data integrity. In addition, to ensure API security—to protect the data during transit between the data holder and the third-party provider—the implementation of secure communication protocols, such as Transport Layer Security (TLS) encryption, may be needed. Data holders must also implement proper access-control mechanisms to regulate who can access and use their APIs. Access-control measures, such as API keys and OAuth 2.0 protocols, can help authenticate the identity of the third-party provider and ensure that it has the proper permissions to access the requested data. As an example, the NEXTGen PSD2 XS2A Framework (an industry standard for account access developed by the Berlin Group) specifies that a third-party service provider may access the account provider's interface only if the account provider can identify the institution through the provision of a certificate issued by a trusted certificate authority. Third parties must authenticate for a specific role, either as an AISP to retrieve customer information or as a PISP to initiate a payment on behalf of their user.[10] Moreover, data holders must also monitor API usage for any suspicious activity or potential breaches using advanced analytical tools and machine-learning algorithms to supervise anomalous behaviors and identify potential threats.

To manage the risks associated with customer data shared with third-party groups via an API, data quality assurance must be incorporated into the governance arrangements around data sharing. This may involve a validator or group of institutions being responsible for validating that all participants comply with the ecosystem's connection requirements and operational rules. Which entity takes on this role will depend on the design of the ecosystem and the characteristics of the market in which it is deployed. However, certain minimum technical requirements for third parties must be met to allow for the trust network to sustain itself. These requirements may include data encryption, secure storage, multifactor authentication, and regular security audits.

3.2.3 Data Privacy

As customer data is shared with third-party providers, data holders must take appropriate measures to implement robust security protocols, such as data encryption and access controls, to protect their customers' data from unauthorized access and use and safeguard sensitive information. Data holders must also obtain explicit customer consent before sharing their data with third-party providers, and customers must have control over how their data is shared and the ability to revoke access at any time. Also of relevance is the need to protect customer data and privacy. Data holders must therefore establish policies and procedures to handle customer complaints and inquiries related to privacy. They may provide clear and concise information to customers about how their data is being used and shared and provide channels for customers to voice their concerns and seek redress, if necessary.

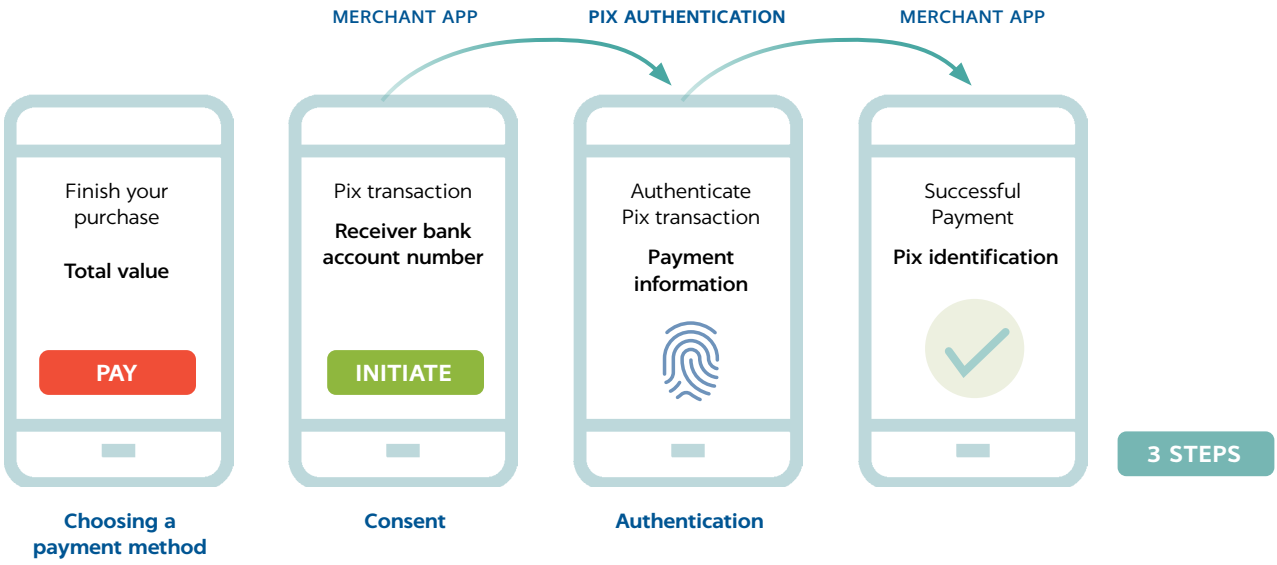
Data holders must also comply with relevant data-protection regulations, such as the General Data Protection Regulation in the European Union. The regulation places strict requirements on data holders and processors to ensure that they process personal data lawfully, fairly, and transparently. Data holders must obtain explicit consent from customers before sharing their data with third-party service providers and ensure compliance with other relevant data-protection regulations in each of the regions where they operate.

3.2.4 Customer Authentication

The robust authentication of users is particularly important to prevent unauthorized fraud in fast payments. A best practice is to require third-party providers to adhere to the same requirements for customer authentication as account providers—namely, multifactor or strong customer authentication, typically based on OpenAuth2, an industry-standard protocol for authorization.[11] In terms of the authentication flow, this can be implemented two ways: On the one hand, authentication can be based on a redirection flow, where the customer is transferred from a third-party app to the customer's account provider or bank and, once authentication and authorization of consent have been completed, back to the third-party app.[12] This type of flow tends to produce a positive experience, as it allows for a more seamless interaction in which authentication takes place on the same device and at the same time. (See figure 3.)

Alternatively, the customer's interactions with the account provider and third-party provider can be more segmented. While this may create some friction at the time of payment initiation, it allows for greater flexibility for the customer to authorize a consent request via different channels (that is, via SMS or authenticator apps) or even at a different time.[13]

FIGURE 3 Authentication Based on a Redirection Flow



Source: World Bank.

3.3 LEGAL AND GOVERNANCE CONSIDERATIONS

3.3.1 Licensing and Authorization

Given the role played by third-party providers of payment initiation services in transmitting and processing sensitive customer data, they should be required to obtain licenses or regulatory authorization to operate in the fast payment ecosystem. In the European Union under PSD2, for example, PSPs are subject to licensing requirements according to the type of payment services they provide. This helps to ensure that the providers meet the necessary standards for data security and customer privacy. In some markets, service providers must also comply with licensing requirements for their APIs and data-sharing agreements. In the United Kingdom, for example, third-party providers need to obtain explicit regulatory permission from the Financial Conduct Authority after demonstrating that they have a PSD2-compliant business model and appropriate data-privacy and security measures in place before being able to join the Open Banking Implementation Entity Directory.[14]

There should also exist a clear framework for authorizing third-party access (direct or indirect) to the technical infrastructure of the FPS. In Australia, for example, any organization that can meet the technical connectivity and security requirements of the New Payments Platform (NPP) and is legally authorized to operate in Australia and financially solvent can apply for direct access to the infrastructure.

3.3.2. Ensuring Reciprocity and Equal Access

In open banking, reciprocity[15] implies that third-party providers should have access to bank-held customer data equal to that of other financial institutions. It ensures that parties have equal access, promoting competition and innovation in the financial services industry. Reciprocity in data-sharing practices may also help to ensure that financial institutions and third parties comply with data-protection and privacy regulations. By requiring all parties to follow the same rules and regulations for data sharing, reciprocity promotes a level playing field and reduces the risk of data breaches or unauthorized access to sensitive customer data. In the context of fast payments, one benefit is that reciprocity can increase competition, leading to the development of more innovative services for fast payments.

3.3.3 Oversight

To ensure that information sharing in the open banking ecosystem operates smoothly and securely, oversight frameworks are necessary. Regulatory authorities must establish and monitor these frameworks to ensure that data holders and third parties comply with the necessary regulations and standards. This includes monitoring the flow of data, security protocols, customer privacy, and compliance with licensing requirements. For PISPs, for example, this means overseeing compliance with any regulations governing the provision of payment initiation services, such as providing customers with clear and transparent information about the

payment transaction, obtaining their explicit consent before initiating a payment, and ensuring the confidentiality and security of customer data.

Through oversight frameworks, regulators can monitor open banking developments closely and take action to address any potential risks or compliance issues. The goal should be to build trust between customers and service providers, ultimately benefiting the entire ecosystem. Regulators can also ensure that customer privacy is maintained by monitoring how data is shared and used. This is particularly important given the sensitive nature of financial information and the potential for misuse or unauthorized access. Additionally, oversight frameworks can help maintain a level playing field for all participants in the open banking and fast payment ecosystem. By ensuring that all parties adhere to the same regulations and standards, competition can be fair and innovation can thrive, benefiting customers by providing more options and better services.

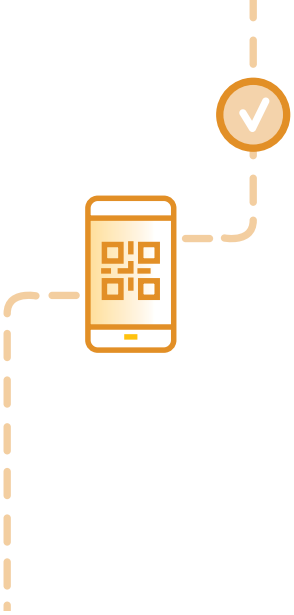
Each market needs to determine the most appropriate oversight approach for its ecosystem. In some countries, the competition-protection authority oversees the implementation and supervision of the country's open banking framework. In others, central banks and financial regulators play this role.

3.3.4 Dispute Resolution and Liability

With the increasing use of APIs to share customer data among different entities, it is important to establish clear policies and procedures for resolving any disputes that may arise. Two aspects of dispute resolution and liability must be considered: those related to disputes between data holders and third-party providers, and those related to consumer protection (that is, disputes and liability between end users and their account providers and/or third parties).

Regarding the latter, it is useful to look at PSD2 in the European Union, which lays out the liability conditions for fraudulent payments initiated via payment initiation services. It states that if a payment transaction is unauthorized, non-executed, defective, or executed late, the user must receive an immediate refund from the provider that services the user's account. If the PISP is found liable, it must compensate the bank promptly. It is the PISP's responsibility to demonstrate that the payment order was received by the bank in compliance with PSD2 regulations and that the transaction was recorded accurately, authenticated, and unaffected by technical issues or other deficiencies within its control.

When looking at dispute resolution and liability between data holders and third-party providers, the United Kingdom's Open Banking Standard provides an example of a dispute-management system to address requests, inquiries, complaints, or disputes between account-servicing providers and third-party providers. In contrast, in countries where the government has not had a leading role, such as the United States, the liability regime for open banking is established through bilateral agreements between banks and third-party providers. These agreements may outline appropriate insurance or own resources and dispute-resolution procedures. In this context, regulators must establish rules and guidelines to ensure that banks and open banking providers comply with industry standards and best practices. By ensuring that all parties in the open banking ecosystem are working together and adhering to regulations, trust and confidence in the system can be promoted—essential for the growth and success of open banking–linked fast payments.



4 CASE STUDIES

There are already several examples of markets where open banking services for fast payments are developing. This section provides insight into the degree of involvement of the FPS, the specific implementation and API strategy, and the overall governance and oversight approach. Table 2 summarizes key aspects of the approaches taken by four markets: Australia, Brazil, India, and Mexico. The approaches are covered in detail in the following subsections.

4.1 AUSTRALIA

Background on Australia's Open Banking Approach

The Consumer Data Right is the key piece of legislation in Australia that gives customers the power to choose with whom they share their data and serves as the foundation of the country's open banking framework. Since the law was passed in 2018, consumers have been able to access and share their banking data with third-party providers of their choice, enabling consumers to compare and switch between products and services more easily. The Consumer Data Right was introduced initially in the banking, energy, and telecommunications sectors and will gradually be implemented across other sectors of the economy.[16]

Beginning in 2019, the Australian government began to implement the Consumer Data Right in gradual phases, beginning with the banking sector. A clear timeline was established to ensure compliance with the regulatory requirements. Major banks were required to make data available on credit and debit cards, deposits, and transaction accounts by the middle of July of that year. (Remaining banks had one extra year.) One year later, data sharing was extended to multiple products. Remaining banks will be required to implement open banking with a 12-month delay on the timelines, compared to the major banks.

TABLE 2 Comparison among Country Profiles

	Key Motivation for Open Banking in General	Type of Open Banking Regime	Model for Provision of Payment Initiation Services	Type of API Framework for Payment Initiation
Australia (NPP)	Promoting competition and innovation	Regulator driven	Centralized through the NPP	Decentralized, multilateral API framework; use of the framework is voluntary
Brazil (Pix)	Financial inclusion	Regulator driven	Centralized through Pix	Multilateral, decentralized API framework; use is mandatory
India (UPI)	Financial inclusion, digitalization	Hybrid	Centralized through UPI	Multilateral, centralized API framework; use is voluntary but strongly encouraged
Mexico (SPEI)	Financial inclusion	Regulator driven	In development; likely to be centralized through SPEI	In development; may involve a centralized API hub

Source: World Bank.

NPP Australia's Strategy for the Development of Payment Initiation Services

NPP Australia, which operates the NPP, introduced the NPP API framework in 2018 to guide the design of APIs for the NPP. The framework provides a recommended technical approach and mandatory data elements, eliminating the need for participants and third-party service providers to create customized APIs and aiming to achieve interoperability among providers.

While the NPP API framework is not mandatory, providers are encouraged to use it to design APIs. The first version includes three sample APIs that enable authorized third parties to perform tasks such as looking up a PayID in the addressing service, sending a payment initiation request, and confirming payment completion. The second version expands the sample APIs to include such functions as cancelling a payment, requesting the return of a payment, providing notification of a payment, and delivering notification of the return of a payment. The API framework will continue to expand over time, with NPP Australia and SWIFT collaborating to establish an API sandbox to encourage its use (RBA 2019).

PayTo, a service designed to offer a secure and user-friendly method for households and businesses to authorize third-party entities to initiate payments via NPP from their accounts, was launched in 2022. NPP Australia has aligned the certification and accreditation requirements for PISPs with the Consumer Data Right accreditation model of the Australian Competition and Consumer Commission.[17] PayTo is governed by an overarching rules framework established by NPP Australia. In 2023, about 50 organizations were live with the PayTo service, including several third parties offering PayTo payment initiation services (Weber 2023). NPP Australia neither hosts an NPP API service nor offers NPP APIs for third-party use on the platform. Participating financial institutions can choose to make their proprietary NPP APIs available for use by third parties (PayTo 2021). Third parties can access the NPP Australia Developer Portal, where they can build and test their NPP-based prototypes and solutions, using the NPP API framework.

Payment Initiation Flow

Payment initiation through NPP has been possible since the launch of the PayTo service. Customers have the freedom to initiate NPP-based payments through the app of any bank or nonbank, irrespective of which financial institution holds their account. Described below and shown in figure 4 is the transaction flow between two people (a sender and a receiver) through a third-party provider using NPP:

1. The sender selects the amount of the payment in a third-party provider's app.
2. The third-party provider uses a direct participant (the originator bank) to send payment information to PayTo.
3. PayTo sends the request to the beneficiary bank to confirm the details.
4. The beneficiary bank checks its internal database to confirm that the receiver's info is correct.
5. PayTo hands over the authorization to the sender's bank to verify the sender's info. (PayID must be verifiable.)
6. The sender's bank sends this information over NPP to the receiver's bank to credit the receiver's account.
7. The receiver's bank credits the account and sends confirmation to NPP.
8. PayTo notifies both banks.
9. The sender and receiver are notified.

Governance and Oversight Framework

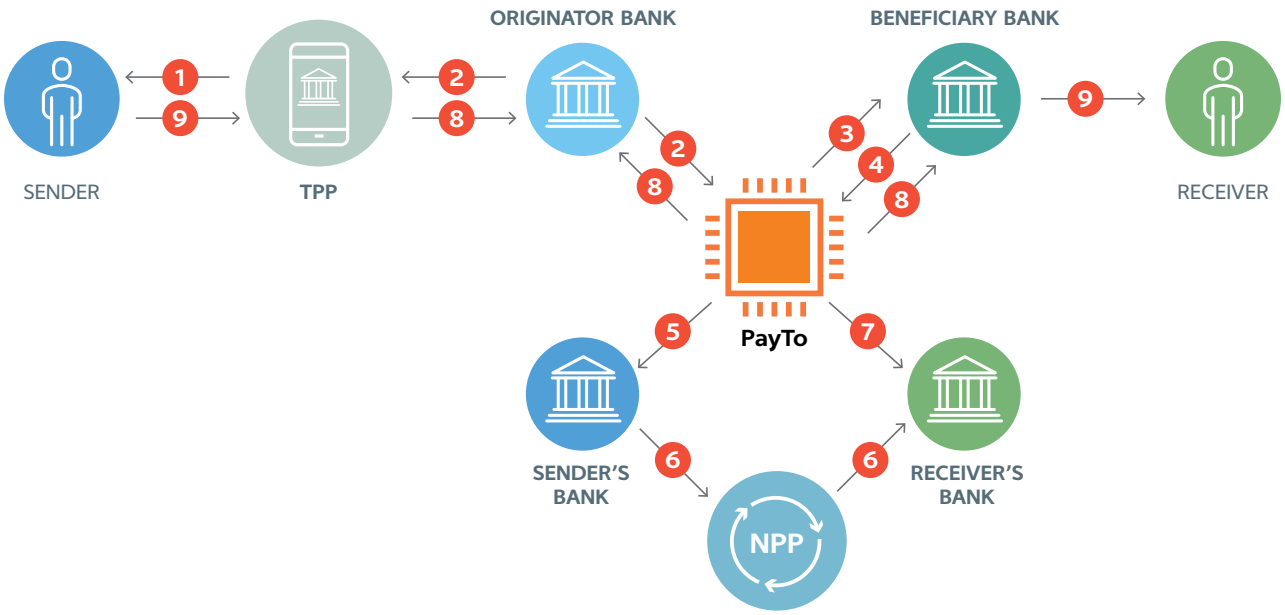
The Australian Competition and Consumer Commission plays a supervisory role over the country's open banking ecosystem and is responsible for its implementation, including whether it is meeting its aim of increasing competition and fostering innovation in the banking sector. NPP Australia oversees the NPP framework and is responsible for encouraging NPP participants, third-party providers, and software developers to build further upon its API framework when developing API solutions for NPP transactions.

4.2 BRAZIL

Background on Brazil's Open Banking Approach

At the beginning of 2019, the BCB and National Monetary Council introduced a regulatory proposal for the implementation of the Open Finance Initiative, establishing foundational principles for open banking and facilitating the evolution of the landscape. The aim was not only to promote innovation and the emergence of new business models for financial service providers, encouraging customer-centricity, but also to increase competition and decrease information asymmetry in the financial system by allowing third parties to access customer data held by established institutions. The BCB intended to increase financial inclusion among Brazilian customers and businesses that had previously been unable to access financial services and to enhance the efficiency of the country's financial and payment systems.[18] The Open Finance Initiative, along with Brazil's fast payment system Pix, are the

FIGURE 4 **Third-Party Payment Initiation in NPP**



Source: Jimmy (2021).

cornerstones of the BCB's plan to transform the country's financial system and to modernize its payment landscape (BIS 2022). The implementation of open banking is mandatory for the larger banks and voluntary for other institutions.

BCB's Strategy for Encouraging the Development of Payment Initiation Services

Brazil has taken a gradual approach to open banking generally, and regulation has been rolled out in four phases.[19] Phase 3 was a key step in terms of integrating Pix into the data-sharing ecosystem. It enabled third-party providers to initiate payments, with any licensed merchant or PSP allowed to initiate Pix transactions within their own platform, keeping customers from having to leave the merchant's website to make a purchase digitally.

The BCB's strategy for open banking involves the creation of a standardized set of APIs—in phases—that all participating financial institutions can use to share customer data securely and efficiently. Phase 1 included the standardization of APIs for sharing open data on available products and access channels. Phase 2 involved the rollout of nine standardized APIs in the field of registration and transactional data sharing: consents, resources, customers (for individuals and legal entities), credit card accounts, accounts, and four credit operations (Open Finance Brazil 2022). The standardization of payment-initiation APIs was covered in phase 3. Phase 4 embraced APIs to share data on investment, insurance, and foreign-exchange operations. The BCB developed the Pix API for payment initiation.

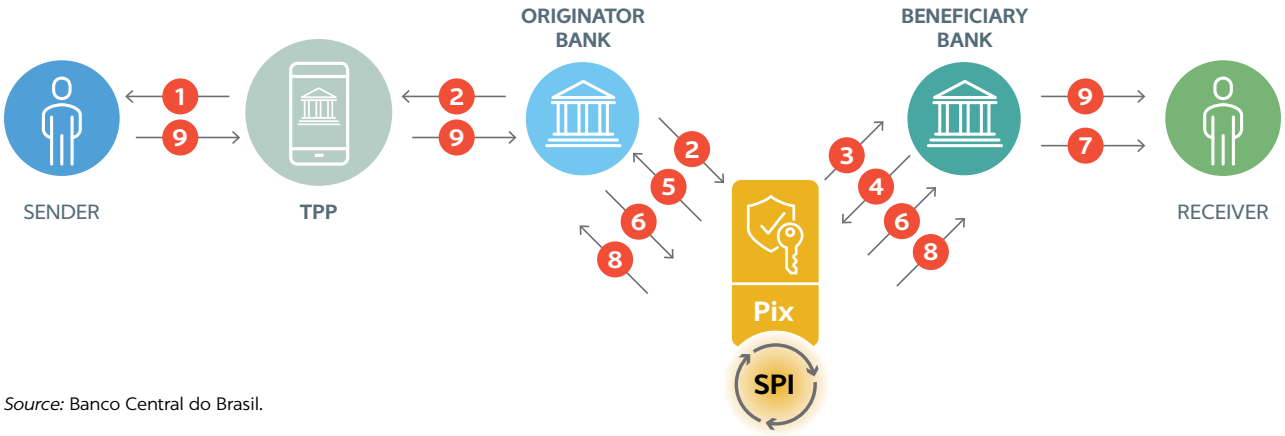
As of now, open banking–linked Pix transactions are e-commerce and person-to-person payments, but other use cases, such as recurring, forward-dated, and bill payments, are being introduced as part of the continued phased implementation (Open Finance Brazil 2022). As of February 2023, after two years of implementation, the initiative in Brazil had completed more than two billion successful API calls, counted 17.3 million active consents, and had more than 800 participating institutions.

Payment Initiation Flow in Pix

Pix operates via a centralized structure that involves messaging communication between direct and indirect participants as well as the BCB. The BCB is responsible for providing the settlement system, which is called the Instant Payments System (SPI).[20] Described below and shown in figure 5 is the detailed transaction flow between two people (a sender and a receiver) through a third-party provider using Pix:

1. The sender opens the Pix payment section in a third-party provider's app.
2. The third-party provider uses a direct participant (the originator bank) to send payment information to SPI.
3. SPI sends the request to the beneficiary bank to confirm the details.
4. The beneficiary bank checks its internal database to confirm that the receiver's Pix address exists and is linked to a bank account.

FIGURE 5 Third-Party Payment Initiation in Pix



Source: Banco Central do Brasil.

5. SPI hands over the authorization to the sender's bank to verify the sender's info.
6. The sender's bank sends this information over SPI to the receiver's bank to credit the receiver's account.
7. The receiver's bank credits the account.
8. SPI notifies both banks.
9. The originator bank and beneficiary bank notify the sender and receiver, respectively.

Governance and Oversight Framework

The BCB has established a clear governance structure for open banking and finance. A deliberative council composed of several representatives from financial associations and an independent councillor oversees the definition of the technical and operational standards for Brazil's open banking. The council is responsible for leading and overseeing the implementation of the open finance environment and supporting the evolving model. Through this structure, participating institutions can develop the framework to achieve the objectives of the initiative. Relevant industry associations, participating institutions, and independent professionals are all represented. The BCB does not vote but has veto power and can regulate issues that governance fails to regulate. This represents the BCB's self-regulatory approach, although all proposed changes to the framework must be approved by the central bank.[21]

4.3 INDIA

Background on the "India Stack"

The inception of API infrastructure in India can be traced back to 2009, when the country introduced the Unique Identification Authority and the concept of unique ID numbers, known as Aadhaar. The first API was released in 2010, followed by a series of other APIs that were progressively added to the "India Stack" platform. The creation of UPI years later also involved the development of a standardized set of API specifications. The messaging format in UPI allows for a high degree of flexibility in supporting a wide range of APIs. The adoption of APIs among participants and third-party providers has been encouraging (World Bank 2021). While not mandatory, new players were encouraged to utilize the public infrastructure based on these standards.

Development of Payment Initiation through UPI

With the continued growth of digital payments—the success of UPI—and the adoption of open API standards, the Reserve Bank of India has expressed its commitment to continue promoting open banking in the country and its aim to facilitate its growth. UPI enables third-party-initiated payments through a centralized API framework, which has been used to drive the digitization of payments and movement of money with phenomenal success. Customers have the freedom to initiate UPI-based payments through the app of any bank or nonbank, irrespective of which financial institution holds their account. Enabling convenient digital payments that are accessible to a large section of the population has led to the development of alternative business models that have been leveraged to facilitate financial inclusion. One of the key factors for the large-scale adoption of UPI has been the participation of third-party payment providers. These providers were essentially nonbank fintech companies that leveraged these open technologies and built business models that were not reliant on revenue generated from the processing of payments, but on revenue generated from the cross-selling and upselling of financial services. These companies are not direct partici-

pants in UPI but can access it indirectly through a bank that is a direct participant, with commercial terms being negotiated independently. Although banks are not required to provide access, the wide participation of banks has generally enhanced access to UPI.

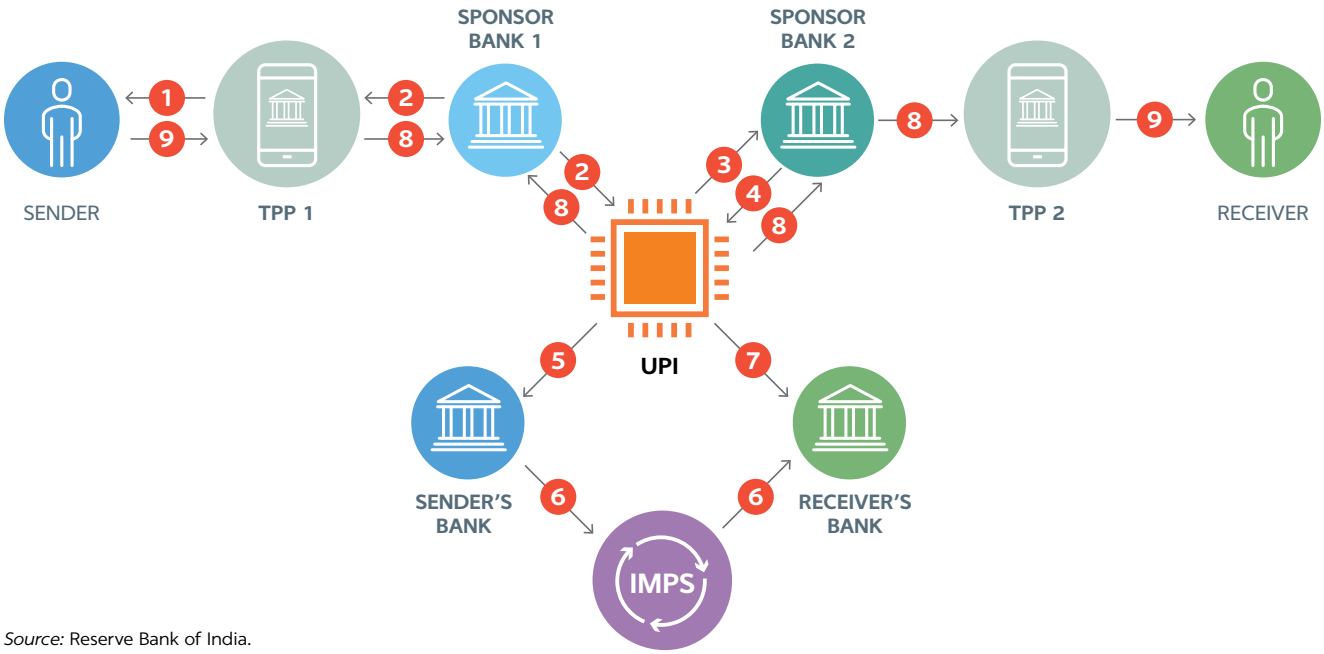
The UPI API, developed by the National Payments Corporation of India, provides a standardized and interoperable platform for seamless and instant mobile payments. This approach is like the "India Stack" approach of open APIs that have transformed the way citizens interact with public services, enabling secure and convenient access to various government schemes and documents. UPI was developed by the industry with close collaboration of the regulator. The National Payments Corporation has implemented a multilateral, centralized API framework based on a directory model. Although the use of UPI is voluntary, it is strongly encouraged, to foster widespread adoption. Through this framework, the National Payments Corporation authorizes third-party PSPs to access UPI through technical means and ensures the maintenance and governance of payment-initiation APIs. This framework enables seamless and secure transactions while facilitating the integration of various digital payment services into the UPI ecosystem.

Payment Initiation Flow in UPI

Payment initiation through UPI, the Indian fast payment system, is allowed. Customers have the freedom to initiate UPI-based payments through the app of any bank or nonbank, irrespective of which financial institution holds their account. Even fintech companies that are not direct participants in UPI can access it indirectly through a participant, with commercial terms being negotiated independently. Although banks are not required to provide access, the wide participation of banks guarantees some form of access to UPI. Described below and shown in figure 6 is the transaction flow between two people (a sender and a receiver) through a PSP using UPI:

1. The sender opens the UPI payment section in a service provider's app. The sender chooses the receiver from his or her phone's address book and enters the amount.
2. The third-party service provider uses its sponsor bank to send this information to UPI.
3. The UPI directory knows that the receiver's phone number is linked to third-party provider 2 through its sponsor bank, so it sends the request to sponsor bank 2 to confirm the details.
4. Sponsor bank 2 checks its internal database to confirm that the receiver's UPI address exists and is linked to a bank account. It returns to UPI the bank account and the bank identifier called the Indian Financial System Code (IFSC).
5. UPI hands over the authorization to the sender's bank to verify the sender's PIN and debit the sender's account.
6. The sender's bank sends this information over UPI to the receiver's bank to credit the receiver's account.

FIGURE 6 Third-Party Payment Initiation in UPI



Source: Reserve Bank of India.

7. The receiver's bank credits the account and sends confirmation to UPI.
8. UPI notifies both parties.
9. The sender's app and receiver's app send out push notifications to the sender and receiver, respectively.

Governance and Oversight Framework

The governance of open banking in India is under the purview of the Reserve Bank of India, which has been actively promoting the adoption of open standards and the UPI APIs.

4.4 MEXICO

Background on Open Banking in Mexico

Mexico was one of the pioneer countries in Latin America to introduce financial data-sharing regulation, paving the way for both open banking and open finance. Mexico's 2018 Fintech Law set the intention for institutions to share different types of data (publicly open, aggregated, and transactional data). The Fintech Law mandates standardization of APIs for data sharing, and the technical specifications are outlined in secondary regulations. There are no special obligations or accreditation requirements for fintechs or financial institutions to share or receive data over APIs if they comply with the API technical and security standards. However, key open banking issues, such as payment initiation, were not considered in the original Fintech Law. In the new regulatory framework that is being developed (Banxico 2021), Banxico has mentioned the creation of a new key actor for payment initiation, the payment service providers (*proveedores de servicios de transferencia* in Spanish).

Mexico's API Framework for Payment Initiation Is Still Evolving

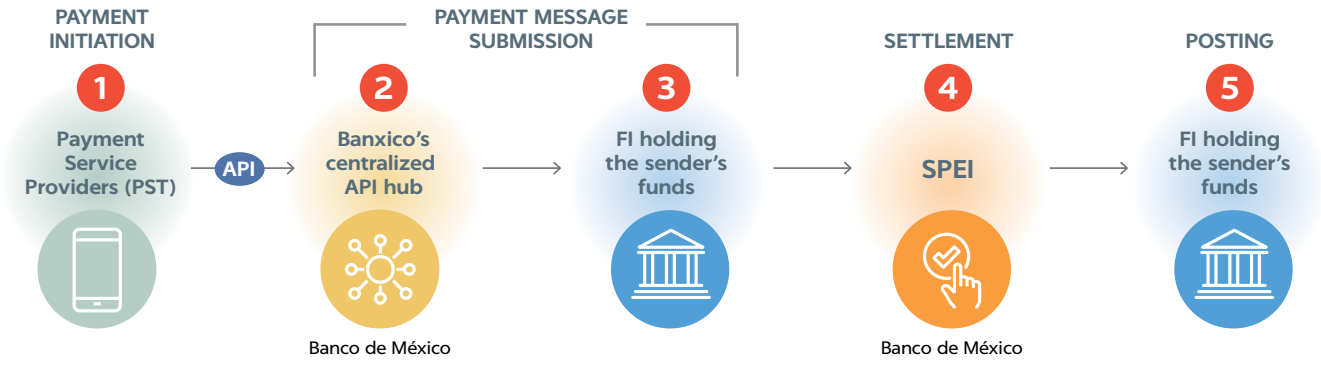
In terms of implementation, the country has been lagging others in Latin America, such as Brazil. The financial regulator, the CNBV, the Mexican National Banking and Securities Commission, has yet to publish secondary provisions covering transactional data. Responsible for issuing specific guidelines for data providers and requesters, the CNBV has issued only guidelines for aggregated data. Therefore, Banxico, the operator of SPEI, the country's fast payment system, has decided to move forward with plans for a regulatory framework and a platform for third-party payment initiation in SPEI.

Banxico has also shared some details, mentioning that it may create a centralized API hub that will facilitate payment initiation through third-party apps and SPEI participants via a single connection to an API. Third parties will connect to said platform, which will transmit the payment initiation request to the end user's account service provider (for example, a bank), so that the bank can submit the payment to SPEI.[22] In addition, payment initiation will be permitted only after end-user identity verification (through a new identification system called SAVI).

Payment Initiation Flow in SPEI

Allowing payment initiation in Mexico's fast payment system has several implications for the country. First, there is a huge potential for SPEI to be used in consumer-to-business e-commerce transactions and other use cases. Second, SPEI could expand further adoption of low-value account-to-account payments if conditions allow for open banking payments to take off. Third, it is likely that more actors will be involved in the account-to-account payment space. Described below and shown in figure 7 is

FIGURE 7 Third-Party Payment Initiation in SPEI



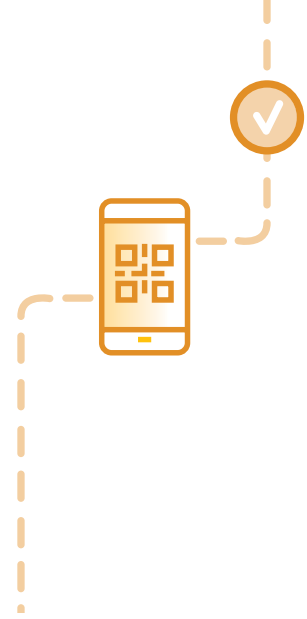
Source: Banxico.

the possible flow of payment initiation in the Mexican fast payment system:

1. The user initiates a transaction through a payment service provider by inputting the amount, funding account, and receiving account (beneficiary). The payment service provider requires the end user's consent to initiate payments from the user's bank account and to authenticate the user.
2. Once the user is authenticated, the payment instruction is delivered to the sending financial institution.
3. The financial institution submits the payment message to SPEI.
4. SPEI settles the transaction.
5. The receiving financial institution makes funds available to the beneficiary. Confirmation messages are sent to all actors in the value chain.

Governance and Oversight Framework

The governance and oversight frameworks are still in development.



5 CONCLUSION

As reflected in the case studies above, FPS operators are taking various approaches to support the development of open banking services for fast payments. While their precise role is likely to vary with the specific market context, including the role of the regulator in promoting open banking generally and the stage of open banking implementation, several best practices for FPS operators emerge.

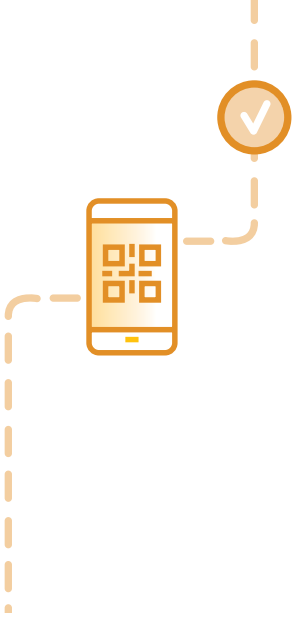
FPS operators can play a central role in the development of multilateral API frameworks for open banking services. Bilateral API frameworks can result in a lack of common standards and are highly decentralized by nature, resulting in greater market-fragmentation risks that could hamper adoption. Although the development of multilateral API frameworks often requires greater effort, given the need to engage the industry and coordinate across multiple parties, multilateral frameworks support standardization and interoperability. This reduces operational complexity, simplifying implementation costs and reducing the risk of market fragmentation. Multilateral frameworks also help to promote a more consistent user experience, supporting a wider range of services/service providers for customers while improving security for users. As core players in the ecosystem, FPS operators can play a central role in helping to define the right standards for APIs and effectively engage the industry.

Determining the right approach for developing and maintaining standardized API frameworks should be considered uniquely for each market. Standardized API frameworks can be developed by the private sector, regulator, or some combination thereof. Mandating adoption of API standards for payment initiation and other open banking services can help ensure that all involved parties are operating on a level playing field. However, it is important to consider the potential impact this may have, as it may be infeasible for all participants to comply. In some instances, overly narrow standards may inadvertently hamper innovation. While mandates can certainly act as an enabler, it is also important to allow market forces to act as drivers to encourage innovation, flexibility, and change. Moreover, in cases where the use of certain API standards is mandated, it is important to set up a reliable enforcement framework to monitor compliance.

For markets that opt to centralize open banking services through an FPS, ensuring the openness of the ecosystem is crucial. Third-party initiation services centralized through the FPS system benefit from existing network effects, which can lead to synergies that boost adoption of both fast payments and open banking services. However, this approach may also require expanded scheme access to include a wider range of third parties to promote competition necessary to drive innovation. FPS and regulators may need to develop clear frameworks for authorizing third parties' technical access to FPS infrastructure. Relevant considerations for doing so include the type of access (direct or indirect) available, whether entities such as PISPs must comply with the same requirements as any other system participant, and, in the case of offering indirect access, the specific licensing process and business models through which access can be granted.

Strong authentication mechanisms and effective dispute-resolution mechanisms are essential for preventing fraud and maintaining trust in the FPS and open banking ecosystems. Given the entrance of third-party providers and the use of APIs, it is essential to prioritize the implementation of robust security measures. This is necessary to safeguard customer data adequately, prevent fraudulent activities, and mitigate against cyber risks. Data holders must ensure the adoption of advanced security technologies, including encryption and multifactor authentication, to prevent unauthorized access and protect customer data. Compliance with regulatory standards is also crucial, playing a pivotal role in ensuring the safety and security of customer data in open banking transactions. It is equally important to strike a balance where the implementation of these security measures does not hinder the user experience or introduce unnecessary friction for customers. Doing so ensures that open banking services remain user-friendly, convenient, and accessible while maintaining robust security standards to protect sensitive information.

Clear and transparent communication made available on multiple channels is necessary for generating user awareness of new products and services. Doing this will keep customers informed about the benefits and risks of using open banking and fast payment services—particularly in markets with a strong preference for cards. In this context, businesses can benefit from operational and transaction costs and gain a competitive advantage. This cost efficiency is particularly advantageous for small merchants, who can enjoy the affordability of accepting fast payments, compared to traditional card payments. FPS operators should keep customers informed about the benefits and risks of using open banking services for fast payments. This can include implementing clear and transparent communication channels to provide customers with information on how their data is being used, what risks they may face, and what steps they can take to protect themselves.



6 ACKNOWLEDGMENTS

Organization	Contributor
Lipis Advisors	Lipis Advisors
World Bank	Harish Natarajan
	Holti Banka
	Nilima Ramteke
	Maria Teresa Chimienti
	Thomas Piveteau
	Andrea Monteleone

NOTES

1. According to the Committee on Payments and Market Infrastructures, a fast payment can be defined as a payment in which the "transmission of the payment message and the availability of 'final' funds to the payee occur in real time or near real time on as near to a 24-hour and seven-day (24/7) basis as possible."
2. These methods are still prevalent in some markets, such as the United States.
3. Fintech Legal Center (2022); Australian Banking Association, "Open Banking" (web page), https://www.ausbanking.org.au/priorities/open-banking/.
4. Government of Canada, "Open Banking" (web page), https://www.canada.ca/en/financial-consumer-agency/services/banking/open-banking.html.
5. Open Banking Limited, "Variable Recurring Payments" (web page), https://www.openbanking.org.uk/variable-recurring-payments-vrps/; PayTo, https://payto.com.au/.
6. APIs are often seen as a catalyst for just-in-time treasury management. Historically, the management of cash balances has been carried out on an end-of-day basis. With the combination of open banking APIs and fast payments, businesses can maintain a cash balance without any surplus at any given moment throughout the day. As a result, they can optimize their cash buffer while increasing the amount of funds retained in their investment accounts. This enhanced cash-management capability leads to more efficient cash planning and usage on a real-time basis.
7. The National Payments Corporation of India governs UPI's API. See NPCI (2016).
8. API Centre, "Payment Initiation API Standard" (web page), https://www.apicentre.paymentsnz.co.nz/standards/available-standards/payment-initiation-api-standard/.
9. More specifically, the "NextGenPSD2 XS2A." See Berlin Group (n.d.).
10. See NextGen PSD2 operational guidelines (Berlin Group 2018).
11. OAuth 2.0, https://oauth.net/2/.
12. API Centre, "Authentication Flows" (web page), https://www.apicentre.paymentsnz.co.nz/standards/available-standards/authentication-flows/.
13. API Centre, "Authentication Flows" (web page), https://www.apicentre.paymentsnz.co.nz/standards/available-standards/authentication-flows/.
14. Open Banking Limited, "The Open Banking Standard" (web page), https://standards.openbanking.org.uk/.
15. In this context, reciprocity is understood as third parties having fair access to their customers' information that is equal to the access enjoyed by banks.
16. Australian Government, the Treasury, "Review into Open Banking in Australia—Final Report" (web page), https://treasury.gov.au/consultation/c2018-t247313.
17. Australian Government, Office of the Australian Information Commissioner, "Consumer Data Right Participants" (web page), https://www.oaic.gov.au/consumer-data-right/consumer-data-right-legislation,-regulation-and-definitions/consumer-data-right-participants.
18. Banco Central do Brasil, "Open Finance" (web page), https://www.bcb.gov.br/en/financialstability/open_finance.
19. Phase 1 covered information about service channels and products and services. Phase 2 covered the sharing of consumer data. Phase 3 established the rules for payment initiation and credit proposals. Phase 4 (in progress in 2023) expands upon the previous rules to other types of data, products, and services, such as foreign-exchange operations, investments, pensions, and insurance. (See Banco Central do Brasil, "Open Finance," https://www.bcb.gov.br/en/financialstability/open_finance.)
20. Banco Central do Brasil, "Pix" (web page), https://www.bcb.gov.br/en/financialstability/pix_en.
21. Open Finance Brazil, "Governança" (web page), https://openfinancebrasil.org.br/governanca/.
22. As of April 2023, the regulatory framework had yet to be announced. It is unknown whether institutions outside of the traditional financial system will be able to participate.


WORLD BANK GROUP