FIGI
FINANCIAL INCLUSION
GLOBAL INITIATIVE

Technical Note on Open Banking

Comparative Study on Regulatory Approaches

WORLD BANK GROUP

ACKNOWLEDGEMENTS

This document has been prepared by Luis Maldonado (Consultant) under the guidance of Fredesvinda Montes (Senior Financial Sector Specialist) in the context of the Financial Inclusion Global Initiative for the authorities in Mexico, including the Secretariat of Finance and Public Credit *(Secretaría de Hacienda y Crédito Público, SHCP), t*he National Banking and Security Commission *(Comisión Nacional Bancaria y de Valores, CNBV),* and the Bank of Mexico *(Banco de México).* We are grateful to the Reserve Bank of India, Financial Conduct Authority of the United Kingdom, Fintech Association of Spain, Monetary Authority of Singapore, Hong Kong Monetary Authority, Bank of Canada, and Spanish Association of Banks for their valuable contributions toward the finalization of this document.

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE

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

DISCLAIMER

The Financial Inclusion Global Initiative led in partnership by the World Bank Group (WBG), International Telecommunication Union (ITU), and the Committee on Payments and Market Infrastructures (CPMI), with the support of Bill & Melinda Gates Foundation (BMGF). The FIGI program funds national implementations in three countries (China, Egypt, and Mexico), supporting topical working groups to tackle 3 sets of outstanding challenges in closing the global financial inclusion gap, and hosting 3 annual symposia to gather the engaged public on topics relevant to the grant and share intermediary learnings from its efforts.

This report forms part of a broader project under the Financial Inclusion Global Initiative Mexico country implementation. The work is a product of the staff of the World Bank with external contributions prepared for the Financial Inclusion Global Initiative. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including The World Bank, its Board of Executive Directors, or the governments they represent, or the views of the Committee for Payments and Market Infrastructure, International Telecommunications Union, or the Bill & Melinda Gates Foundation.

The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Table of Contents

Tables

Figures

Abbreviations and Acronyms

AFIN	ASEAN Financial Innovation Network
API	application programming interface
CDR	Consumer Data Right
CMA	Competition and Markets Authority
EBA	European Banking Authority
GDPR	General Data Protection Regulation
HKMA	Hong Kong Monetary Authority
MAS	Monetary Authority of Singapore
OBIE	Open Banking Implementation Entity
PSD2	Revised Payment Services Directive
RBI	Reserve Bank of India
RTS	Regulatory Technical Standards
SCA	strong customer authentication
TPP	third-party provider

Executive Summary*

Open banking has emerged strongly in the past few years as a system to give customers the right to share with parties they trust the information that banks have about them in a secure manner and also as a way to open up processes and services in banking. The main objectives pursued by regulatory frameworks that define open banking are generally encouraging innovation and fostering competition, resulting in new products and services at competitive prices to the benefit of consumers.

With that in mind, and with the United Kingdom as a first mover, different regulatory approaches have been developed. Some of them are regulatory driven, while in other cases, with a hands-off approach, they have been led by industry. In between, we also find collaborative models in which both the public sector and private-party players are instrumental to the definition and adoption of open banking.

Regulatory approaches also differ in the scope of data that is to be shared, the definition of the financial institutions that have to publish their application programming interfaces and share data, the mandatory or voluntary nature of the framework, the definition of the type of license that third-party providers need to operate, and the definition or not of concrete standards, among other things.

While there is no single right approach, there are common challenges that countries considering regulation certainly need to bear in mind in terms of the definition and interoperability of technical standards, security, governance, and consent and authentication mechanisms.

With different strategies and intensity, some banks are starting to be active in the development and opening of their application programming interface frameworks. On the other hand, different business models and players have emerged to connect banks with fintech companies through a middleware of application programming interfaces, especially in Europe, the United States, and some Asian countries.

Although open-banking regulatory frameworks have been operating for less than two years at most, early lessons can be drawn from the first movers and the debates that are taking place between regulators and market participants.

1. Introduction and Background

The Financial Inclusion Global Initiative (FIGI) is implemented in partnership by the World Bank Group, Committee on Payments and Market Infrastructure, and International Telecommunications Union and is funded by the Bill and Melinda Gates Foundation to support and accelerate the implementation of country-led reforms to meet national financial-inclusion targets and, ultimately, the global Universal Financial Access 2020 goal.

FIGI funds national implementations in three countries (China, Egypt, and Mexico) and supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) electronic payment acceptance, (2) digital ID for financial services, and (3) security. FIGI also hosts three annual symposia on relevant topics to gather national authorities, the private sector, and the public and to share emerging insights from the working groups and country programs.

The Mexico FIGI Program aims to expand access to transaction accounts and broader financial services by more empowered users. This objective will be achieved by (i) enhancing the design of payment and financial products, including through the innovation of technology and business models to meet the needs of underserved individuals and micro, small, and medium-sized enterprises, (ii) fostering the sustainable expansion of physical access points, in parallel with leveraging technology for remote access, and (iii) empowering users through increased transparency and the use of transactional and other relevant data. The Mexico FIGI Program includes six different components: (i) access points, (ii) digital ID, (iii) fintech regulation, (iv) financial consumer protection, (v) financial literacy, and (vi) large-volume payments.

Article 76 of the Fintech Law determines that financial institutions, money transmitters, credit information companies, clearing houses, regulated fintech companies, and companies authorized to operate with new models will be required to establish application programming interfaces (APIs) that allow interconnectivity between these institutions. The Fintech Law also requires the development of secondary regulations by the National Banking and Security Commission (*Comisión Nacional Bancaria y de Valores, CNBV)* for banks and financial institutions, including the new Financial Technology Institutions, and by Banco de México for payment systems, central counterparties, and credit-reporting systems. The Fintech Law states that entities required to create APIs shall share three types of data: (i) open financials, which are nonconfidential data including information on services offered and access points; (ii) aggregate data, which are those related to the statistical information of its operations; and (iii) transactional data, which are those related to the use

of financial products and services by a consumer. The General Dispositions issued by the National Banking and Security Commission and Banco de México establish the common technical standards that ensure the interoperability of APIs, including their design, development, and maintenance standards. The secondary regulations also establish the security mechanisms to access, send, and obtain data and information and outline the information considered critical for the good functioning of the applications requiring access to APIs. Finally, the General Dispositions outline the process to obtain consumers' consent to access their transactional data. As per the Fintech Law, to permit transactional data to be shared and accessed, the consumer shall grant authorization, and the data shall be used only for the uses expressly authorized by the consumer. The consumer can also withdraw this authorization at any time.

In this context, Mexican authorities are interested in understanding the approaches pursued in other markets and fintech ecosystems to inform and develop their own policies and regulation effectively.

2. Context for Open Banking

The increasing interaction and use of bank-held customer-permissioned data by third parties has led different countries to take regulatory actions on different aspects of open banking.[1] Data sharing has taken place though different techniques, such as screen scraping and reverse engineering, as standard market practices. However, regulations are generally encouraging the use of APIs, considering the use a more secure and reliable practice.

Some jurisdictions have taken a prescriptive approach, requiring banks to share customer-permissioned data and requiring third parties that want to access such data to register with particular regulatory or supervisory authorities. Other jurisdictions have taken a facilitative approach, issuing guidance and recommended standards and releasing open API standards and technical specifications. Remaining jurisdictions follow a market-driven approach, having no explicit rules or guidance that requires or prohibits banks from sharing customer-permissioned data with third parties.

The frameworks created vary across countries in terms of stage of development, approach, and scope. Indeed, most regulations are in the early stages of development, and many were issued or came into effect in 2018 or later. It is therefore still very early to draw substantial lessons. In any case, the countries that are developing their regulatory frameworks are looking at learnings from the early players.

Finally, while some topics have not been incorporated into any regulation yet and hence are beyond the scope of the technical note, they are on the agenda for discussion in many countries. The role of bigtech firms in the data economy, the extension of data sharing to other sectors of the economy (referred to as "smart data"), or potential efforts toward international interoperability are examples of issues that will very likely have the attention of regulators in the near future.

3. Objective of the Technical Note, Scope, and Methodology

Mexico issued its Fintech Law in 2018 with the purpose of regulating financial services provided by financial technology institutions that are offered or performed by innovative means. This law is based on the principles of financial inclusion and innovation, the promotion of competition, consumer protection, the preservation of financial stability, the prevention of illegal operations, and technological neutrality. A general approach to the open-banking framework in Mexico is contained in the article 76 of the Fintech Law.

To give context to the Mexican authorities as they develop their secondary regulation around consumer data-driven open banking, this technical note reviews open-banking regulations and practices in those countries that are more advanced in that respect. To understand the different elements to consider when developing a regulation, the following aspects of API infrastructure are analyzed: governance, technical requirements, security measures, outsourcing models, interoperability, and access to third parties. Also, a review of the players providing API infrastructure has been included. Aspects referring to consumer rights around the use of their data and regulations affecting the use of their data have also been considered. Additionally, those initiatives that include authentication of consumers have been taken into account. Finally, incentives to adopt APIs have been reviewed. A comparison of how different countries have approached these elements, as well as lessons learned from early implementation, could serve as a guide for future regulatory efforts.

Countries analyzed for this technical note include Australia, Brazil, Canada, the European Union, Hong Kong, India, Japan, Mexico, New Zealand, Singapore, the United Kingdom, and the United States.

Part of the analysis in this note is based on a desk review of (a) relevant regulations in the abovementioned countries; (b) materials on open banking by the World Bank and other international financial institutions; (c) literature on open banking by international market analysts and other reliable sources; and (d) reports and consultations made public by different countries.

The desk review was complemented with information gathered through in-person and phone interviews with authorities, market participants, lawyers, and other experts from the countries included in the scope of this technical note.

4. Challenges and Opportunities of Open Banking

A new wave of disruption has been progressively introduced in the retail banking industry in the past few years. Open banking can securely provide other financial institutions and third-party providers (TPPs) with seamless access to customer data through APIs and enable banks and non-banks to provide integrated modular services sourced from different specialist firms. This consent-based access to data and the potential communication that it allows open great opportunities for innovation to banks, fintech companies, and other players. This access to data is not exempt of risks; to reap the full benefits of open banking, they must be accounted for.

From the standpoint of banks, they have traditionally been in control of the data about their customers, and within a closed architecture, this allows them to make use of that data and gives them the initiative on the design and development of products. Opening to third parties requires API developments that enable other players to have access to their customers' data and to play a role in the production and delivery of financial and auxiliary services, moving banks to some extent from their comfort zone and opening up to competition. The need to develop and maintain an API infrastructure, the time and cost involved, the potential loss of revenue, more complex distribution of liabilities between banks and third parties, and cybersecurity are among the challenges that banks are facing. At the same time, implementation of open finance allows banks to develop new business models with potential new revenue streams and, to the extent banks also connect with other banks or players, have deeper insight into their customers.

As far as fintech companies are concerned, open banking creates an environment that encourages the development of the ecosystem. Access to consumer data and collaborative business models with banks enable great opportunities for innovation. Building the necessary security and compliance elements that an adequate treatment of customers data require is an important challenge for fintech companies.

Consumers, for their part, are probably the biggest winners from a move toward open banking. While some concerns may arise about privacy and data security, access to a wider range of services, improved user experience, lower prices that increased competition entails, and the potential for wider financial inclusion are important gains. Those gains could be enhanced with "dynamic efficiency" as the process around data exchange consolidate.

Concerning regulators, they can find in APIs a more stable framework of data sharing, with enhanced security. Also, the development of solutions could potentially contribute to more efficient surveillance and compliance of banks. Open banking could play a role in the areas of

regtech and suptech, capturing information directly from financial institutions through APIs and, hence, significantly automating the supervision. At the same time, this could allow financial institutions to meet their compliance obligations in a more efficient manner. One interesting example in this direction is AuRep, an innovative regulatory reporting system that has been implemented by the Austrian central bank and the country´s banks to capture data directly from financial institutions.

Regulators are also facing important challenges in an open-banking framework, such as the need to have new technical capabilities to analyze APIs, the need to resolve conflicts between banks and fintech companies, and coordination among regulators.

Finally, all the players involved on the potential extension are challenged by data sharing to other sectors of the economy and the role that bigtechs might be playing in the data economy.

TABLE 1: Challenges and Opportunities of Open Banking

	Banks	Fintech Companies	Consumer	Regulators
Opportunities	New business models New revenue streams Deep customer insight More user-centric solutions	Enables ecosystem development New business models Collaborative business models with banks Scale faster	Wider range/choice of services Improved user experience Lower prices Financial inclusion	More stable exchange of information Enhanced security Potential for suptech solutions
Challenges	Need to develop API infrastructure (cost and time) Competition and revenue loss New distribution of liability Business model risk Customer disintermediation Cybersecurity	Security Compliance	Privacy Data security	Need to have technical capabilities to analyze APIs Need to resolve conflicts between banks and TPPs Coordination among regulators

Source: Author's summary

5. Legal Framework of Open Banking and APIs in Selected Countries

Open banking offers great opportunities for incumbents, new service providers, and consumers. At the same time, banks and financial institutions are big targets for criminals, and the loss or misuse of financial data can cause real damage and distress to individuals. The risk of data loss, privacy breaches, fraud, and other cybersecurity attacks is real and increasing. Therefore, banks and financial service providers face new legal responsibilities to prevent the unauthorized or unlawful processing of data and to prevent loss, destruction, or damage. In such a context, there might be a need to balance legal and regulatory provisions related to information sharing and enabling access by different institutions with legal provisions related to data protection. Since rules are enacted by different authorities, potential conflicts of law might exist. In addition, one of the objectives of enabling open banking is to provide consumers more control over their account information and the possibility to decide with whom they would like to share such data. In such a context, consumer consent to allow third parties to access information through APIs has become a key issue in the formulation of the legal and regulatory framework of open banking.

Safeguarding competition, strengthening market contestability, and protecting the integrity of legal frameworks in the face of innovations from payment initiation and account services/aggregation are the main reason why the European legislator has decided to intervene and why national authorities are implementing and enforcing these rules. On the one hand, large financial institutions (or groups thereof) held too much control over the industry and the array of payment and other services that users could combine with their core banking services. On the other hand, big techs are entering the financial market and are outside of the regulatory perimeter. Avoiding regulatory arbitrage has become a key priority for financial-sector regulatory authorities.

Data sharing is one of the key aspects of open banking, and safeguarding such data is also important. In this context, the adoption of measures to secure not only data but also networks, software, applications, hardware, and facilities is a relevant element of the design of open finance ecosystems. This security includes not only banks and institutions accessing data through APIs but also institutions that provide outsourcing services to banks and other institutions accessing their data, including providers of cloud-computing services.

Sharing data through the screen-scraping technique—where a TPP or financial data aggregation service accesses bank accounts on the consumer's behalf using their credentials—raised consumers' as well as lawmakers' and banks' concerns, as there was no possibility to limit the time or scope of data accessed by the third party. Open banking therefore requires a new approach to authentication and access to permissioned data.

The adequate assignment of accountability for financial losses in the event of erroneous data sharing is also a relevant legal aspect that is typically covered under contractual arrangements that might not be enforced in a rapid manner.

Finally, one additional important point is the adoption of alternative dispute-resolution mechanisms, established either by banks or by the third parties through processes and procedures and contractual arrangements between banks and third parties.

Although early precedents are also in other constituencies, the United Kingdom was the first country to regulate open banking; the Open Banking Standards went live in January 2018. Since then, the number of countries defining their open-banking regulatory frameworks has been increasing.

The first attempt to create an open-banking framework in the United Kingdom was the Midata Initiative, which was launched in 2011 by the Department for Business, Innovation and Skills with the objective to give consumers greater access to their transaction data in a portable electronic format. Banks voluntarily supported the initiative by providing downloadable account-transaction data in a standardized file format. Customers needed to download these files, save them to a disk, and then upload them. Providers, in turn, would analyze the data and make recommendations based on them. Midata was rolled out in 2015 but emerged with serious problems, in particular a very poor user experience. The project was not as satisfactory as had been envisaged and did not reach wide adoption. However, it served well as a learning experience for the framework to be designed later.

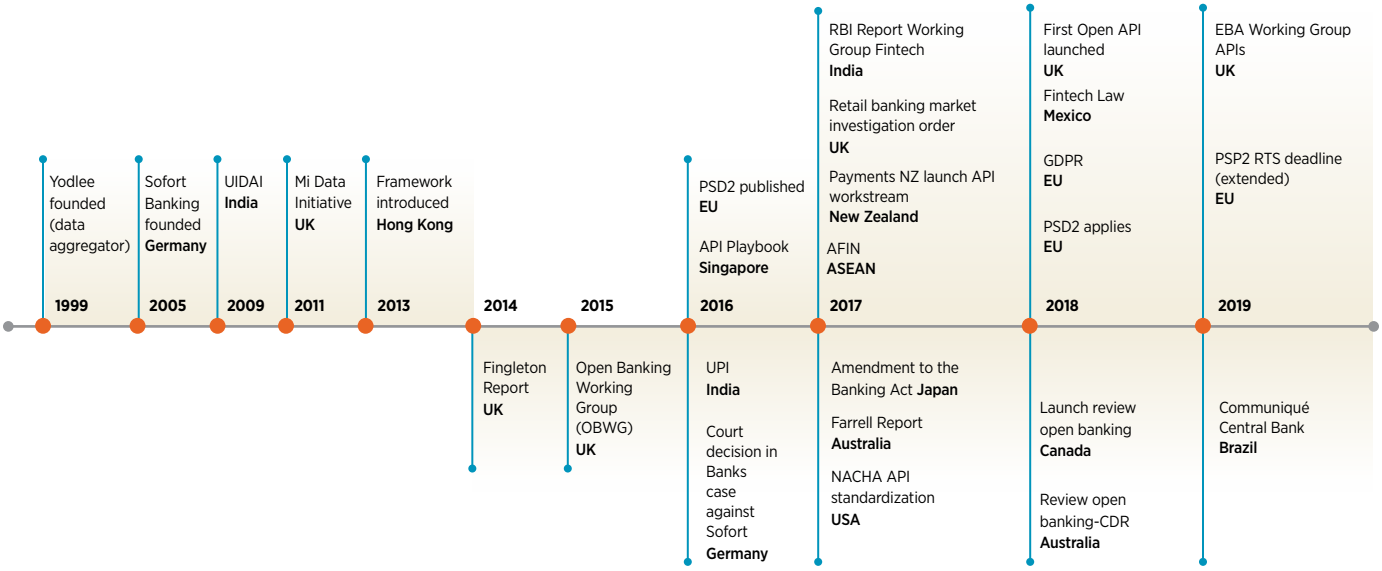
Envisaging the important benefits that open banking could unlock, the Treasury and the Cabinet Office commissioned a report[2] in 2014 to assess the opportunities that a model of open banking with data on bank transactions shared with APIs could entail for banks in the United Kingdom. The authors concluded that a greater access to data would improve competition, and they made a strong case for the use of common standards to enable interoperability between banks and providers.

As a next step toward establishing open banking in the United Kingdom, the Treasury in 2015 created the Open Banking Working Group, with representatives from the banks, open-data groups, consumers, and TPPs, to determine the practical definition of data sharing. In 2016, the working group published a framework for banking data sharing and guidelines on how to implement it.[3] The group recommended standardized APIs to be shared.

In parallel to those developments in the United Kingdom, important pieces of regulation emerged at a European level affecting how open banking and data sharing were unfolding in the United Kingdom—namely, the revised Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR). These will be analyzed later.

The Competition and Markets Authority (CMA) conducted an investigation of the retail banking market in 2017 that resulted in the issuance of a mandatory order[4] concluding that competition was insuffient in the United Kingdom, leading to high prices and insufficient incentives to innovate, to the detriment of final consumers. Among the remedies that merged from this result, the nine largest banks (referred to as the CMA9)[5] were obliged to make

FIGURE 1: Open-Banking Timeline



Source: Author's summary based on public information

customer data from their current personal and business accounts available to authorized third parties through APIs. The CMA also established an implementation entity to write the standards, build the supporting infrastructure, and coordinate and drive the implementation. The design of open banking was delegated to an individual (the Trustee), who would head up a body, the Open Banking Implementation Entity (OBIE), that would work with stakeholders across the sector to deliver open banking and at the same time have powers delegated to compel banks to comply. Open banking went live in January 2018, with the launch of the first account-information API. Once the implementation phase is complete,[6] the role of the OBIE will transition into a monitoring role to ensure that banks continue to meet their obligations.

Among the early learnings from the United Kingdom's experience, analyzed in a report commissioned by the OBIE,[7] the importance of enhancing the user experience, the need to improve payment capabilities, the need also to improve consent protection for customers, the possibility to expand open banking into open finance, and the introduction of premium APIs that go beyond the mandatory ones could be highlighted.

While the United Kingdom's experience has opened the way and been taken into account by other countries, different models and regulatory approaches to open banking have emerged.

In Europe, PSD2[8] came into force on January 12, 2016, and for most of the provisions, member states had until January 13, 2018, to implement them into national laws. The most impactful parts of PSD2 related to open banking are the introduction of new payment-initiation and account-information services operated by TPPs that are granted access to bank data though APIs, and the provisions on strong customer authentication (SCA) for online payments. The PSD2 security measures related to TPP account access and to SCA were further detailed in the European Banking Authority Regulatory Technical Standards (RTS),[9] which were foreseen to enter into force on September 14, 2019. Finally, due to the complexity in the implementation, the European Banking Authority (EBA) has allowed national authorities to postpone for a year the introduction of the RTS for online payments.

At a European level, no common APIs standard have been adopted. Different set of standards have been proposed by bodies representing coalitions of European banks (for example, STET[10] and the Berlin Group[11]).

In January 2019, the EBA established a working group on APIs under PSD2. The working group is tasked with facilitating industry preparedness for the Regulatory Standard on Strong Customer Authentication and Common and Secure Communication and to support the development of high-performing and customer-focused APIs under PSD2.

Europe´s GDPR[12] marked a significant milestone in data protection and had a global impact. GDPR is the primary law regulating how all companies protect the personal data of citizens of the European Union. It provides several new rights relating to personal data for citizens of the European Union, including a right to access, a right to be forgotten, a right to restrict processing, a right to data portability, and a right to revoke consent. GDPR requires explicit consent and that customers are made fully aware of how their personal data will be used and by whom. Finally, GDPR also imposes legal duties on organizations to protect customer data and to ensure its accuracy and completeness.

The European Data Protection Board is working on guidelines on the relationship and compatibility between relevant provisions of GDPR and PSD2. The first version of this guidelines is expected for the first quarter of 2020.

In Japan, the Amendment to the Banking Act in 2017,[13] which came into force in June 2018, introduced a registration system for TPPs and set the framework for collaboration between banks and TPPs, including both payment-initiation and account-information service providers. The amendment encourages banks to open up their APIs. Financial institutions have the discretion to opt in to open banking but must comply with specific rules if they do. Banks must endeavor to establish a system for carrying out interconnection through APIs within two years from the enforcement of the amended Banking Act. In 2018, banks had already presented their plans to realize open APIs. The fact that TPPs need an authorization, and especially that they are required to sign an individual agreement with each of the banks to which they want to connect, are making the process burdensome and adoption slow.

The Monetary Authority of Singapore (MAS) has been very active promoting open banking with a comprehensive, nonmandatory regulation and governance framework. The MAS has led by example by opening its own data for APIs and establishing scalable data practices and a payments infrastructure that underpins innovation in the area. Singapore has taken a collaborative stance with the industry. In 2016, with the Association of Banks in Singapore, it published an API playbook[14] that encourages banks to participate in open banking. The playbook presents a high-level guideline for API design aimed at stakeholders intending to use APIs, including providers, consumers, fintech companies, and the developer community. It includes a description of the full sequence of steps toward a complete strategy to open banking: prioritize and select APIs, implantation guidelines, data standard, security standards, and governance mechanisms. Four categories of APIs are included: product, servicing, marketing, reporting and payments. Finally, the MAS has also established an API register, to list open APIs available

in the Singaporean financial industry. In total, the playbook sets out a comprehensive framework, listing more than 400 recommended APIs and over 5,600 processes for their development.

At a regional level, the MAS, with the Association of Southeast Asian Nations (ASEAN) Bankers Association and the International Finance Corporation, has participated in the creation of ASEAN Financial Innovation Network (AFIN), established in 2018 as a not-for-profit market institution. AFIN´s objective is to create a scalable, market-driven, open architecture platform that can help expand access to responsible financial services innovation in the digital economy to smaller banks and markets across Asia. AFIN operates the API Exchange (APIX)[15] platform, the world's first cross-border, open-architecture API marketplace and sandbox platform for collaboration between fintech companies and financial institutions. The marketplace expedites discovery and collaborative undertakings between fintech companies and financial institutions.

As a result, several banks have launched their own initiatives and API platforms in Singapore (DBS, OCBC Bank, Citi, and Standard Chartered, among others), making Singapore one of the most dynamic markets in the development of an API ecosystem.

Australia has approached open banking from the wider perspective of consumer data rights.

In 2017, the Treasury Department commissioned the Review into Open Banking in Australia, chaired by Scott Farrell,[16] to recommend the most appropriate model for open banking in Australia. Since then, the government has decided to legislate a Consumer Data Right (CDR)[17] to empower customers to choose to share their data with trusted recipients only for the purposes that they have authorized. The right will be implemented initially in the banking (open banking), energy, and telecommunications sectors and then rolled out economy wide on a sector-by-sector basis.

On May 9, 2018, the Australian government agreed to the recommendations of the review, both for the framework of the overarching CDR and for the application of the right to open banking, with a phased implementation from July 2019. The government decided to phase in open banking with all major banks making data available on credit and debit cards and deposit and transaction accounts by July 1, 2019, and mortgages by February 1, 2020. Data on all products recommended by the review will be available by July 1, 2020. All remaining banks will be required to implement open banking with a 12-month delay on timelines compared to the major banks.

The Australian Competition and Consumer Commission has a supervisory role in the process and has been empowered to adjust timeframes if necessary. In September 2019, the commission released draft guidelines on the CDR accreditation process and supplementary guidelines on the insurance and information-security requirements of accreditation.

Also following a public consultation, the Hong Kong Monetary Authority (HKMA) published its Open API Framework for the Hong Kong Banking Sector[18] in July 2018, laying out its approach to open banking. The formulation of the Open API Framework is one of the seven initiatives announced by the HKMA in September 2017 to prepare Hong Kong to move into a new era of smart banking.

The framework takes a risk-based principle and a four-phase approach to implement various Open API functions (product information, customer acquisition, account information, and transactions) and recommends prevailing international technical and security standards to ensure fast and safe adoption. It also lays out detailed expectations on how banks should onboard and maintain relationship with TPPs in a manner that ensures consumer protection.

Hong Kong has defined a collaborative approach where the HKMA will monitor progress of Open API implementation and further consider the need for new regulatory measures. However, it has permitted flexibility to banks in implementing Open API as part of their strategies. It has allowed the industry to set its own standards without making them mandatory. Having reviewed implementation challenges after a year, the HKMA signaled its intent to play a more proactive role in the definition of standards and security for the higher-risk phases 3 and 4 of API implementation for account information and debit initiation.

Concerning the US market, the regulator has taken a hands-off approach, issuing nonbinding guidelines and letting open-banking practices be industry driven. We can find a general driver for open banking in Section 1033 of the Dodd-Frank Act,[19] which states that US citizens can allow access to their financial data. Also, the Consumer Financial Protection Bureau issued a document in 2017 containing consumer nonbinding principles for data-sharing protection[20] that encourage the use of APIs for data sharing.

More recently, in July 2018, the US Treasury issued a report[21] containing general recommendations on the use of consumer financial data and encouraging regulators to take the necessary steps to avoid regulatory uncertainty and create a context for secure and efficient access to data.

With a widely established practice of screen scraping, the United States' bank payments association, the National Automated Clearing House Association, launched in 2017 a group to work on API standardization, mainly in three areas: fraud and risk reduction, data sharing, and payment access.[22] Also, in late 2018 the Financial Data Exchange[23]

was launched with the goal of unifying the leading financial institutions in the United States, together with fintech and others, around a common API standard and technical framework for data sharing across the industry.

In New Zealand, the development of open-banking standards is also being led by the payment association, PaymentsNZ. It launched an API workstream as a central part of its Payments Direction strategic initiative since 2017; the main driver for that initiative is encouraging innovation in the payment sector in the country. In March 2018, the first pilot of APIs for payment initiation and account information was launched. This pilot is now closed, and the first versions of payment-initiation and account-information APIs are available in the newly created API Centre. In June 2019, PaymentsNZ released a set of standards on account information and payment initiation.[24]

India entered into open banking in the area of payments. The National Payments Corporation of India, an umbrella organization for operating retail payments and settlement systems in India, as an initiative of the Reserve Bank of India (RBI) and Indian Banks' Association under the provisions of the Payment and Settlement Systems Act, launched the Unified Payments Interface in 2016. The interface facilitates interbank transactions through an API framework together with a digital identity solution. It is partly built within the unique identification platform in India (Aadhaar).

The history of API infrastructure dates back to 2009, when India launched the Unique Identification Authority and created the Unique Identification Numbers (UIDs), named as Aadhaar. The first API was launched in 2010, and several APIs were progressively added within the platform India Stack: Payment Bridge and Aadhaar Enabled Payment System, eKYC, eSign, and DigiLockers. In 2019, India Stack has collected 1.06 billion Aadhaar numbers, linked 339 million bank accounts, and done 150 million electronic know-your-customer actions.[25]

The RBI has remained active, encouraging the adoption of open banking. In 2017, the RBI published a report of the Working Group on Fintech and Digital Banking,[26] providing recommendations for an environment for developing fintech innovations and testing of APIs. Also, the RBI established directions for a Non-Banking Financial Company-Account Aggregator,[27] describing a framework for the registration and operation of an account aggregator in India.

More recently, Canada embarked on a journey toward open banking with the announcement in the 2018 budget of the government's intent to undertake a review of the merits of open banking.[28] To guide the review, the minister of finance appointed an advisory committee on open banking. The following three core financial-sector policy objectives were clearly stated to be guiding the review: efficiency, utility, and stability. The consultation sought to understand how stakeholders perceived the potential benefits of open banking and, also, how Canadians felt that risks related to consumer protection, privacy, cybersecurity, and financial stability should be managed.

While the government completes the review, different stakeholders are contributing to the debate. In June 2019, the Standing Senate Committee on Banking Trade and Commerce issued a report with recommendations on how the deployment of open banking should take place in Canada.[29] The recommendations include (i) the designation of the Financial Consumer Agency of Canada as the interim oversight body for screen scraping and open-banking activities, with a mandate to conduct research and public education and to respond to complaints; (ii) the provision of immediate funding to consumer-protection groups to help them conduct and publicize research on the benefits and risks of screen scraping and open-banking activities; and (iii) to facilitate the development of a principles-based, industry-led open-banking framework. Over the longer term, it is also recommended modernizing the Personal Information Protection and Electronic Documents Act, to align it with global privacy standards and to designate the privacy commissioner of Canada and the Canadian commissioner of competition as the co-regulatory and enforcement authorities for open-data frameworks.

In Mexico, the Fintech Law[30] came into force in March 2018. This the first law in the world to regulate in a comprehensive manner all the aspects affecting digital innovation in the financial sector, new business models, and new players, including the creation of a sandbox. The main guiding principles of this regulation are financial inclusion and innovation, which differ from the focus on competition stated by some other regulations mentioned in this section. Open banking is mandated in article 76, describing the institutions that must publish their APIs and the type of data to which they need to give access. The details of these elements of the strategy, together with the other dispositions of the Fintech Law, are being developed by the Mexican authorities.

Finally, Brazil has also declared its intent to regulate open banking. In a communiqué published in April 2019,[31] the Central Bank of Brazil disclosed the fundamental requirements for the implementation of open banking in Brazil. Specifically, the communiqué provides for the scope of the Brazilian open-banking model, the definition of the customer personal and transactional data to be shared, and its phased implementation approach, expected to be completed for the second half of 2020.

Self-regulation initiatives are expected, and the Central Bank of Brazil may coordinate these initial self-regulatory efforts. In December 2019, as a first step to start the regulatory process, the central bank submitted the drafts for public consultation.

TABLE 2: Regulatory Approaches to Open Banking

Regulatory-Driven Model	Collaborative Model	Industry-Led Model
United Kingdom	Singapore	United States
European Union	Hong Kong	New Zealand
Australia	Japan	
Brazil		
Mexico		
Canada		
India		

Source: Author's summary

6. Analysis of Selected Topics

6.1 DATA EXCHANGE THROUGH APPLICATION PROGRAMMING INTERFACES

Data exchange between financial institutions and service providers has become increasingly common, as it promises to facilitate industry-wide innovation and increased business agility and competition while allowing consumers further choices. However, the types of data to be exchanged, the mandatory versus voluntary nature of the exchange, and the types of participants in the exchange might vary from one context to another.

6.1.1 Types of Data

The scope of open banking varies with the kind of data and functions made available via APIs. Some frameworks apply only to specific types of data, such as payment processing data, and provide third parties with both "read" and "write" access to data and payment initiation, while other frameworks provide "read-only" rights for data aggregation purposes. Concerning type of data shared, the following five categories could be considered:

- Product and service data: Non-confidential data provided by financial institutions—for example, data about their products or services offered or offices and ATM locations.
- Customer-provided data: Information provided directly by customers to their banks. Customer ownership is most obvious in this type of data.
- Transactional data: Data generated as a result of a direct interaction with the financial institutions. This data is usually available in internet or mobile banking statements. Products included can go from the most basic current account to a wide range.
- Customer insights: Data that results from an effort made to gain insights about a customer. Credit scoring or know-your-customer data would be examples of this type of data.
- Aggregate data sets: Non-individualized data that results when the bank uses multiple customer´s data to produce collective or average data across a group or subset of customers.

6.1.2 Types of Participants

Participants in the open-banking ecosystem are both banks and financial institutions, and third parties accessing the data. Among the latter, payment initiators and account information aggregators have emerged as the two main actors.

TABLE 3: Types of Data Exchanged in Selected Countries

	UK	EU	Singapore	Japan	Hong Kong	Australia	New Zealand	India	USA	Brazil	Mexico
Payment initiation	✔	✔	✔	✔	✔		✔	✔	✔	✔	
Current account information	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Product information	✔		✔		✔	✔		✔	✔	✔	✔
Credit scoring			✔			✔			✔		
Verification—ID					✔	✔		✔			
Information about ATMS and offices	✔				✔					✔	✔

Source: Author's summary based on public information and interviews with authorities and market participants

Concerning the institutions that are subject to opening their data, different approaches are observed, depending on how wide the definition of financial institutions affected by open banking is.

Developing an API framework, the definition of processes, compliance requirements, and staff training or hiring impose some initial costs that have been considered in some instances to include only players of a certain size. This is the case, for example, of Open Banking in the United Kingdom, where initially opening mandated largest banks to give access to current personal and business accounts customer´s data to authorized third parties through APIs (the CMA9).

Brazil has announced a progressive approach, where, at first, only the institutions that are part of prudential conglomerates will be obliged to participate. Subsequently, this obligation may be extended to other institutions, at the discretion of the Central Bank of Brazil. The final scope of the model envisaged for Brazil should include financial institutions, payment institutions, and other institutions licensed by the Central Bank of Brazil.

In most countries, banks are the addressee of regulations or guidelines about open banking. This is the case in the European Union, Hong Kong, Japan, New Zealand, Singapore, and the United States. In some of those cases, such as in Hong Kong, New Zealand, or the United States, only major banks are affected, at least at an initial stage.

Finally, in some instances, a broader set of institutions are subject to the opening of their APIs.

In the case of India, the concept of financial information provider includes the bank, banking company, non-banking financial company, asset-management company, depository, depository participant, insurance company, insurance repository, pension fund, and any other entity that the RBI may identify.

In Mexico, the Fintech Law has included as obliged to establish standardized APIs financial institutions, money transmitters, credit information companies, clearinghouses, financial technology institutions, and companies authorized to operate under new models.

In some cases, the opening of APIs for the financial institutions described in the regulations is established as mandatory, while in other cases, countries have drafted the regulation more in the shape of nonbinding guidelines or other prescriptions that make them voluntary.

Concerning the parties who can have access to the data, ensuring that only entities that adhere to the appropriate security and privacy standards and have the customer´s authorization becomes key to guaranteeing a secure open-banking framework. With that in mind, some constituencies have established licensing or authorization requirements for TPPs. That is the case of Australia, the European Union, India, Japan, Mexico, New Zealand, and the United Kingdom. In the case of Japan, regulation has gone a step further, also requiring an individual bilateral agreement between the TPP and the bank. Finally, Hong Kong gives banks the freedom to choose which TPP to collaborate with using bilateral agreements.

In the case of Europe, to increase transparency, the EBA established a central register that contains information about payment and electronic money institutions authorized or registered within the European Union.[32] TPPs, both account information service providers and payment initiation service providers, are required to have an electronic ID to prove that they are a licensed player. This ID is then read by the bank before granting their access.

In Singapore, the authorities have established a Financial Industry API Register, updated semiannually, which tracks APIs by functional category as they are launched. These open APIs provided by financial institutions have been broadly classified as either transactional (that is, containing sensitive client data, user/partner authentication required) or informational (that is, containing nonsensitive data, no/minimal authentication required).

TABLE 4: Types of Participants and Nature of the Framework in Selected Countries

	UK	EU
UK	Banks	Mandatory for MA9
EU	Banks	Mandatory
Singapore	Banks	Voluntary
Japan	Banks	Voluntary
Hong Kong	Banks	Voluntary
Australia	Banks and other sectors	Mandatory
New Zealand	Banks	Voluntary
India	Financial information provider	Voluntary
USA	Banks	Voluntary
Brazil	Financial institutions	Mandatory
Mexico	Financial institutions and others	Mandatory

Source: Author's summary based on public information and interviews with authorities and market participants

Finally, one particular principle that the CDR has introduced in Australia is reciprocity. All accredited recipients (fintech companies and other) must transfer data at their customers' request in a format equivalent to how they received it.

6.2 API INFRASTRUCTURE

6.2.1 Governance

One important aspect around open banking is how to operationalize the open-banking framework, including the potential creation of governance entities, and their roles, responsibilities, and activities. To ensure an adequate governance of the open-banking framework, certain aspects need to be defined, such as the appropriate mechanisms to determine engagement of participants to ensure that obligations are met, or how issues that materialize between participants are resolved.

Authorities involved in open banking can include the banking supervisor, an API or technical standards competition authority, the consumer-protection authority, the data privacy authority, and an alternative dispute mechanism.

In some cases, such as in the European Union, Hong Kong, India, and Singapore, the bank supervisor is the one in charge of overseeing the open-banking framework. In other cases, such as Australia, it is the competition authority that is responsible for the implementation of the open-banking framework to increase competition in the banking sector and to foster innovation.

In the case of the United Kingdom, to manage API standards in a way that enables a transparent and open governance framework that supports accessibility, usability, and innovation, an independent body was created. Recognizing that the CMA could not specify the technical standards in the primary regulation, the design of open banking was delegated to the "Trustee" who would head up a body, the OBIE, that would work with stakeholders across the industry to deliver open banking. Funding for the OBIE comes from the largest banks (the CMA9), while the CMA, the Financial Conduct Authority, and Her Majesty´s Treasury provide governance oversight. The OBIE is the custodian of the Open Banking Standards for APIs and owns and maintains the Directory of Open Banking Participants (also referred to as the Open Banking Directory), which provides a "whitelist" of participants able to operate in the open banking ecosystem. Once the implementation phase is completed, the role of the OBIE will transition into a monitoring role to ensure that service levels and obligations are met.

Considering the API architecture and framework within a bank or financial institution, there is the need on their part to define an internal governance that includes the following phases: ideation of APIs; prototyping and production; publishing; consumption (including partner onboarding, security, and so on); and retirement (notification of changes and migration). Singapore has been the country that has issued the most detailed description of guidelines about this API life-cycle governance. Also, in the case of Singapore, recommendations around the API risk governance have been detailed.

In the case of Hong Kong, which leaves the strategy of adoption of open API to banks, the HKMA mandates that those that chose to move forward should ensure that a commensurate level of protections and suitable TPP governance arrangements are in place with appropriate, clear contracts to define responsibility, liability, control, and customer protections. A detailed description of the preferred governance framework, based on bilateral arrangements with a common baseline, for the different phases of API adoption is described by the HKMA in their Open API framework.[33] Processes range from simple TPP registration process with basic consumer-protection measures to onboarding checks, ongoing monitoring, and bilateral contractual relationships.

Also, once open APIs have been implemented by banks, the HKMA contemplates the creation of a body to review the relevance of the architecture, security, and

data standards on an ongoing basis. The body may also take on other industry-wide tasks, such as coordination and consumer education, where needed. In the longer term, if harmonization of open API functions is desired by the industry, the body can also take on this task to work with the industry to achieve interoperability.

In the case of Australia, to govern the data standards, the Australian Competition and Consumer Commission has established the creation of a data standards chair and an advisory committee.

There are instances where industry-led workstreams are defining the governance of APIs. This is the case of payment associations in the United States (National Automated Clearing House Association) and New Zealand (PaymentsNZ).

Concerning liability frameworks, many countries have existing or planned laws for regulations addressing customer liability with respect to data access by third parties. For example, PSD2 requires authorized third parties to have professional indemnity insurance, or a comparable guarantee, against specified liabilities, such as unauthorized transactions or non-execution and defective or late execution of payment transactions. In other cases, customer liability may be addressed by national personal data-protection laws, general banking laws covering customer protection against fraudulent transactions, consumer-protection laws, and civil, commercial, and criminal codes. In some countries, customer liability is included in the bilateral contracts or agreements between the bank and TPP.

Finally, several countries have existing or planned complaint-handling or alternative dispute-resolution mechanisms that cover open-banking issues.

Among jurisdictions with existing or planned complaint-handling or alternative dispute-resolution mechanisms, in the European Union, PSD2 requires payment service providers, including authorized third parties, to put in place adequate and effective complaint-resolution procedures. In Hong Kong, terms addressing the complaint-handling mechanisms are expected to be included in contracts with third parties, as customers should not be responsible for any direct loss suffered as a result of unauthorized transactions conducted unless the customer acts fraudulently or with gross negligence. In Japan, the Association for Electronic Payment Services, a private body, is responsible for handling customer complaints related to open banking. In Singapore, the Personal Data Protection Commission facilitates the complaint between the customer and the provider. India has an ombudsman scheme for digital transactions.

For jurisdictions that do not have regulatory guidance requiring complaint- or dispute-handling mechanisms, customers often initially take their complaints and disputes to their bank.

6.2.2 Technical Requirements

While regulation in some countries has defined standardized technical standards, in other cases, a flexible approach has been adopted. In some instances, the industry has been the one establishing nonbinding standards.

In the case of Australia, Mexico, and the United Kingdom,[34] the standards have been mandated by regulation. Both Australia and the United Kingdom have introduced guidelines on standards even in customer experience. Hong Kong, based on international practice and the feedback during the consultation exercise, recommended internationally accepted architecture and security standards. In Singapore, a joint effort between the MAS and the Association of Banks resulted in the publication of an API playbook containing detailed recommended standards for APIs. In New Zealand and the United States, it has been the industry that has led the publication of nonbinding standards. In India, the RBI envisages developing API standards with the technical support of the Reserve Information Technology.

Concerning Europe, while PSD2 has not defined prescriptions on technical standards, some market initiatives have emerged (such as the German Group, STET, and the Polish API). Secondary regulation in the European Union has defined regulatory technical standards for SCA and common and secure open standards of communication (RTS).[35]

In Brazil, the expectation is that the participating industries will agree themselves on technology standards, operational procedures, safety standards and certificates, and the implementation of interfaces. However, to ensure

TABLE 5: Technical Standardization in Selected Countries

	UK	EU	Singapore	Japan	Hong Kong	Australia
Technical standards	Regulatory	No standards, partial industry adoption	Collaboration MAS/ Banking association	No standards	Recommended	Regulatory

	New Zealand	India	USA	Brazil	Mexico
Technical standards	Industry	Regulatory	Industry	Expectation of industry self-regulation	Regulatory

Source: Author's summary based on public information and interviews with authorities and market participants

compliance with the regulation, as well as the achievement of the proposed objectives for the model, the Central Bank of Brazil may coordinate the initial self-regulatory efforts, approve decisions and revisions, and exercise the veto power, imposing restrictions or regulating nonagreed aspects.

In Mexico, the Fintech Law dictates that the Supervisory Commission and the central bank could determine the technical standards for the interoperability of APIs, their governance, security, and consent mechanisms.

6.2.3 Security Measures

Different potential operational and cybersecurity issues have been identified related to the use of APIs, including data breaches, misuse, falsification, denial-of-service attacks, and un-encrypted login. Mechanisms used by some banks to mitigate these risks include stricter access privileges, authorized end-to-end encryption, authentication mechanisms, and vulnerability testing, among others.

Robust security foundations are crucial to realizing the benefits of data transfer that open banking promises without compromising the soundness of the system. A right balance needs to be struck to ensure that security standards do not act as a barrier to entry for new players. This general principle has resulted in different degrees of regulation, from mandatory standards to recommended guidelines on security measures.

In the United Kingdom, the OBIE has released highly detailed and prescriptive technical security standards[36] in the areas of customer authentication, API specification, encryption, management of data, and controls.

The European Union has also mandated specific requirements in PSD2 with regards to payments in aspects such as managing operational risks, including system performance monitoring, contingency measures for unplanned unavailability or a system breakdown, incident management, and reporting. The European Regulation 2018/389 develops the requirements to be complied with by payment providers to apply the procedure of SCA, protect the confidentiality and the integrity of the payments service user´s personalized security credentials, and establish common and secure open standards for communication between the different parties involved in open banking.

In Singapore, the API playbook contains detailed guidelines on information security standards in domains such as authentication, encryption, authorization, hosting security, secure coding, vulnerability assessment, and robust fail-over mechanisms. MAS recommendations clarify that the level of security standards for each API depends on the business criticality of the data being exchanged, permissible access levels, including role-based access, and availability requirements across the identified information security domains.

Banks in Australia are also subject to prudential standards and guidance on data security issued by the Australian Prudential Regulation Authority[37] and to the Privacy Act's requirement to secure personal information. Those standards set out the authority's expectations for regulated financial institutions to consider and address risks such as fraud due to theft of data, business disruption due to data corruption or unavailability, delivery failure due to inaccurate data, breach of regulatory obligations resulting from unauthorized disclosure, and controls to ensure adequate data quality and data security, particularly in arrangements involving third parties.

In India, the main characteristics, and the definition, of security elements of APIs will be defined in guidelines that are being drafted. The main features are likely to be technology agnostic, reliable, scalable, simple, minimalist and evolutionary in nature, customer-centric, driven by consent, and asynchronous by design. The specifications would promote interoperability and layered innovation and transparency and accountability through data, including data privacy and security concerns. The account aggregator will be data blind, and the data will move in encrypted form, so that account aggregators cannot store data on their servers.

Finally, in Hong Kong, the Open API Framework recommends the architecture and security standards. The HKMA will also define a more detailed set of standards in 2020 for Phase III and IV open APIs to facilitate secure and efficient implementation across the industry. While certain technical standards have been prescribed, they cannot be considered as the only standards that cover all security requirements. Banks should always refer to sound industry practices and relevant regulatory and internal requirements and apply holistic controls on information and cybersecurity based on a risk- and principle-based approach to protect banks' systems as well as bank and consumer data.

6.2.4 APIs Developed In-House by Banks or Outsourced APIs Providers

On a practical matter, banks have followed different approaches to open banking, resulting in different levels of openness for their APIs. Depending on their API strategy and internal capacities, banks either have decided to develop and publish their own APIs or have connected to external platforms.

While each model has its merits and challenges, standardized APIs (either regulatory or industry driven) tend to create a more balanced competitive context than closed APIs, which give a higher level of power and control to large banks and fewer opportunities to compete to smaller banks. And they also impose more costs on fintech companies wanting to partner with several financial institutions.

We can find examples of banks having launched their open APIs framework in different countries. Some of the banks leading globally the development and publishing of their APIs are DBS in Singapore—with the largest API developer portal, with more than 155 APIs available—OCBC, Unionbank in Philippines, Citi, and BBVA. The two main origins of front-runner banks are either advanced Asian countries—namely, Singapore—or banks in the European Union adhering to PSD2. (More than 250 banks operating in the European Union have launched developer portals and APIs.) According to market analysis, 65 percent of banks' implementation in Europe adheres to the Berlin Group standards.

On the other hand, a large number of banks deploy their offering through so-called API hubs, which provide a single interface to access all banks using their solution.

The following two models of API hubs are in the market:

1. **Compliance model:** This model incorporates a layer to bank APIs that guarantees compliance with the regulation, hence mitigating compliance risk. They have been developed specially in Europe to ensure compliance with PSD2. Examples are Redsys (Spain), CBI (Italy), Stet (France), and Nets (Nordic countries).
2. **Technical TPPs or aggregators:** They develop their own APIs, which enable interconnection between banks and fintech companies. Examples are BEC, Luxhub, SIBS, Eurobits, and Figo (Europe); Plaid and Yodlee (United States); or Saltedge (Europe and United States).

Some of these platforms work as marketplaces, allowing the connection between banks and fintech companies through APIs, and have appeared on the market with a regional approach and, in some cases, with public or multilateral support. The AFIN APIX platform,[38] working in the countries of the Association of Southeast Asian Nations and with some partnerships outside the region, such as Abu Dhabi Global Markets, is one example of a multicountry marketplace platform. Another example is Finconecta,[39] operating with the platform 4wrd, which provides an API framework for connecting banks with fintech companies in some African countries, the Middle East, Europe, and Latin America, in partnership with the Inter-American Development Bank in that region.

Several banks, especially in the European Union, have also started to act themselves as third parties; many large banks now offer account-aggregation services (for instance, Railsbank, Solaris, and BBVA). This trend is likely to consolidate in other markets introducing open-banking regulation.

Concerning the business models around APIs and the possibility of charging third parties for the use of APIs, jurisdictions that regulate the obligation of APIs to be published generally do not allow banks to charge for them. For those APIs that are not mandatory, the so-called premium APIs, regulations generally leave freedom for banks to decide on a business model for charging. So far, there are not many instances where banks are charging for APIs.

6.2.5 Interoperability

Interoperability could be defined as the ability of a system or a product to work with other systems or products without increased cost or effort. In the context of open banking, interoperability entails that legal and operational terms facilitate switching between banks. Regarding fintech companies and third parties, interoperability provides banks with the reciprocal stability of being able to change providers or work with several of them without increasing fixed costs. When standardization has not been imposed or has not yet been completely implemented, interoperability becomes a key driver for ecosystem development, and especially for customer adoption. It is also key for enabling a competitive environment that encourages small and medium players to develop their APIs on a level playing field with large banks.

Indeed, one of the recommendations of the Fintech Bali Agenda[40] is to reinforce competition and a commitment to open, free, and contestable markets to ensure a level playing field and to promote innovation, consumer choice, and access to high-quality financial services. The successful and large-scale adoption of technology would be facilitated by an enabling policy framework regardless of the market participant, underlying technology, or method by which the service is provided. It encourages policy makers to address the risks of market concentration and to foster standardization, interoperability, and fair and transparent access to key infrastructures.

Also, different reviews of digital competition across Europe, such as the Furman Review[41] and the European Commission's digital competition report,[42] concluded that data and protocol interoperability could drive increased competition in digital markets.

Hence, interoperability has been broadly incorporated as an objective for countries to achieve while promoting and encouraging the adoption of API standards. Industry practice also becomes key to achieving interoperability.

In the case of the United Kingdom, interoperability has been forced by regulation but also pushed by banks, especially large ones. Authorities estimate that 80–90 percent of account providers currently operate under the open-banking standards.

Hong Kong is also moving toward interoperability. Since the launch of the first phase of open banking in January 2019, the APIs launched by banks have largely followed the recommended technical standards in the Open-API Framework.

India has interoperability as a clear aim as it moves in advance of its draft API standards.

In Europe, the EBA has determined in the RTS that, to ensure the interoperability of different technological communication solutions, the interface should use standards of communication that are developed by international or European standardization organizations. Thus, without defining a concrete standard, it calls for the interoperability of the system.

In Singapore, collaboration with the banking association in the development of the API handbook has been instrumental to promote the interoperability of the API framework.

In some cases, such as in the United States and New Zealand, efforts toward interoperability have been led by industry associations.

Finally, Australia has understood interoperability in a wider way, in the sense that what has been designed for the banking sector will also be able to work in other sectors of the economy (for instance, in energy and telecommunications).

6.2.6 Access to Third Parties

Access by third parties to customer data has occurred in the absence of APIs with the use of the widespread practices of screen scrapping or reverse engineering, still prevalent in several markets.

In screen scraping, the customer provides a third party with his or her log-in credentials (for example, a username and password) for the online banking platform. This third party then uses the details to log in to the website of the customer's bank and extract data on behalf of the customer.

The practice of reverse engineering decompiles the code of the mobile banking applications to figure out which information is exchanged between the application and a bank's servers (through the nonpublic API) and subsequently build a "reverse-engineered" version of the mobile application that is capable of directly exploiting the communication from and to the bank's servers. It requires a second enrollment of a mobile application upon receipt of the customer's authentication credentials and the subsequent use of these credentials, or even the creation of a proprietary set of authentication credentials (to the third party). This technique is often favored by data aggregators over screen scraping because it is much more scalable and robust, as its performance is not influenced by changes that banks make to their customer interface.

Interestingly, one of the latest countries to launch a consultation process, Canada, is paying a lot of attention to the analysis of the advantages and disadvantages of open banking versus screen scraping, as part of their consultation and the reaction to it on the part of the Standing Senate Committee on Banking, Trade and Commerce.[43]

Some of the concerns associated with screen scraping and reverse engineering have to do with security and customer protection, stability, and the lack of revoking rights on the part of the customer. Hence, screen scraping and reverse engineering are perceived as slower, less stable, and less secure processes. Also, they allow less control on the part of the bank over who accesses customer data and which data are retrieved. Generally, banks prefer a system of APIs where they are in full control of the data accessed by TPPs. However, the cost and time needed to build and maintain public APIs could represent a challenge, particularly for smaller banks.

On the other hand, while fintech companies are aware of some of the drawbacks entailed with accessing data through screen scraping and reverse engineering, they generally also have concerns about limitations on access only through APIs, which give permission only to certain data, with more limited flexibility on the type and number of queries and, in some cases, with some lags on the update to the latest information.

In some areas, these different approaches have led to tension about whether the regulator should choose to prohibit screen scraping once APIs are mandatory. Most jurisdictions do not prohibit the practices of screen scraping and reverse engineering.

The case of the European Union is particularly illustrative of this heated debate. The RTS introduced the concept of a "dedicated interface" (API). This enabled account servicing payment service providers, those who provide and maintain a payment account for a payer, to develop their own APIs and impose them on TPPs.

Indeed, the latest version of the RTS saw a last-minute change in December 2018 incorporating a contingency mechanism to use screen scraping (also known as the "fall-back mechanism") in case the dedicated API interface is unavailable or not working properly. In that vein, the EBA Guidelines from the Contingency Mechanism under Article 33(6) of the RTS[44] establish that, if the interface does not respond to five requests within 30 seconds, it is considered unavailable, mandating banks to publish metrics on their service levels.

Banks can benefit from an exemption if their dedicated interface fulfills a number of conditions centered around how robust, available, and well supported the solution is. To gain the exemption, the dedicated interface also has to meet certain design and testing standards and has to have been widely used for at least three months. There are a number of challenges with the exemption process, especially given that these assessments include fairly technical analysis of each interface. Several regulators in the European Union are open about the fact that they

do not have the technical expertise required to perform these assessments, so they are encouraging banks to use standardized conformance tools available in the industry. Many have also mandated self-assessments and audit steps as part of the exemption process.

TPPs make several claims about the system established in Europe. They allege that it creates an imbalance. Each account servicing payment service provider has, at most, one API to implement—namely, its own. Whereas TPPs must implement a large number of APIs, depending on their current service and market coverage. Also, they underline the challenge that TPPs have in testing these APIs for bugs and other problems without compensation. Finally, the APIs were opened up for testing on March 14, 2019. Initial evaluations from some of the largest TPPs in Europe found that testing environments (sandboxes) were available for only about half the account servicing payment service providers.

6.3 CONSENT MECHANISMS

Data openness is an essential element of open-banking regimes. One key aspect to deal with is the protection of customer rights. This has resulted in the need for an explicit consent on the part of customer, which in some cases is contained in other regulatory pieces that deal horizontally with customer data rights that could introduce more strict measures to the open-banking framework.

In Europe, in accordance with data-protection rules under both PSD2 and GDPR, account holders can exercise control over the transmission of their personal data. Hence, no data processing can take place without the explicit informed consent of the consumer.

Under PSD2, providers (that is, banks, account information service providers, payment initiation service providers, and so on) can access and process only the data needed for the provision of the services subscribed to or requested by the consumer. PSD2 regulates the provision of new payment services that require access to the payment service user´s data. For instance, this could mean initiating a payment from the customer's account or aggregating the information about one or multiple payment accounts held with one or more payment service providers for personal finance management. When a consumer seeks to benefit from these new payment services, she or he will have to request such services from the relevant provider explicitly. Payment service providers must inform their customers about how their data will be processed.

Payment service providers will also have to comply with other customers' rights recognized in GPDR, such as the right of access, the revocation of consent, or the right to be forgotten. All payment service providers (banks, payment institutions, or new providers) must comply with the data-protection rules when they process personal data for payment services.

Australia, under the principle of giving customers control of their data, has determined that customers should be able to give specific instructions on what data is shared, with whom that data is shared, and for what purpose it is shared, as well as the duration the sharing arrangement. The CDR requires banks to implement effective and efficient consent-management policies and processes and establish dashboards. Banks must demonstrate clear governance around collecting and managing customer consent and authorizations before data is shared. Also, the CDR contemplates that a consumer who has given consent to use particular CDR data may withdraw the consent at any time by communicating the withdrawal to the accredited person in writing

In Singapore, open-banking practices also need to be fully compliant with the regulation that protects the use of individual personal data, the Personal Data Protection Act,[45] where it is mandated that organizations must obtain previous consent to collect, use, or disclose personal data, and where an individual has the right to withdraw this consent at any time.

The Open API Framework in Hong Kong expects banks and TPPs to implement appropriate measures for addressing requirements related to customer data protection and the protection of personal data, including applicable laws and guidance on the protection of personal data. These include the Personal Data (Privacy) Ordinance in Hong Kong,[46] as well as the regulations and codes promulgated by the Privacy Commissioner for Personal Data under the said ordinance. Specifically, this regulation requires consent from the data subject and mandates that data subjects must be informed whether supplying data is obligatory or voluntary, the purpose of using their data, and the classes of person to whom their data may be transferred. A data subject can withdraw his/her consent previously given.

In India, the consent architecture established in the RBI Master Directions[47] determines that no financial information of the customer shall be retrieved, shared, or transferred by the account aggregator without the explicit consent of the customer. The consent of the customer should be obtained in a standardized way and contain, among other details, the identity of the customer and optional contact information, the purpose of collecting such information, and the consent expiration date. Account aggregators should also provide their customers with a functionality to revoke consent.

Brazil has also declared that the sharing of a customer's personal and transactional data, as well as the execution of payment services, should be subject to the customer's prior consent. Procedures to obtain such consent should aim to promote a simple, efficient, and safe customer experience.

Finally, Mexico requires in the Fintech Law that personal transactional data could be shared only with prior explicit consent from the customer. Only data that has been authorized may be used, and the owner of the data (the customer) has the right to revoke consent.

6.4 AUTHENTICATION OF CONSUMERS

The transmission of data, and especially remote electronic payment transactions, are subject to a high risk of fraud. Hence, some constituencies have deemed the introduction of additional requirements for SCA to be necessary. Also, fraud methods are constantly changing; thus, the requirements of SCA should allow for the innovation of technical solutions addressing the emergence of new threats to security.

In this vein, PSD2 introduces in Europe strict security requirements for the initiation and processing of electronic payments. PSD2 and the development regulation (the RTS) oblige payment service providers to apply SCA when payment service users

- Access their payment accounts online, whether directly or through an account information service provider;
- Initiate an electronic payment transaction, or
- Carry out any action through a remote channel that may imply a risk of payment fraud or other abuses.

SCA is an authentication process that validates the identity of the user of a payment service or of the payment transaction. More specifically, SCA indicates whether the use of a payment instrument is authorized.

It requires payment service providers to provide two of the following three items to verify identity:

- Something you know (a password, response to a security question, or PIN)
- Something you have (two-factor authentication via mobile phone, hardware token, or smart card)
- Something you are (a fingerprint scan or facial recognition)

SCA isn't applied to some transactions that are considered low risk, including balance checks, low-value transactions (less than €30 for a single transaction), and the number or amount of transactions relative to the last time SCA was performed. Also, for remote transaction between €30 and €500, it is accepted not to use SCA if the levels of fraud are proved to be under certain thresholds.

The requirements of SCA across the European Union are aimed at reducing the risk of fraud for online payments and online banking and protect the confidentiality of the user's financial data, including personal data. However, given the complexity of adoption, the EBA has given flexibility to national authorities to postpone the adoption of RTS for non-present card transaction up to 15 months from September 2019.

SCA in Europe could result in different user experience levels depending on how the authentication flow is implemented by banks. TPPs are required to have an electronic ID, which serves to certify that it is a licensed player. The bank must not create obstacles to the process, but, in the absence of a contract, once the bank has read the electronic ID, it has the option to require the SCA to take place on its website and then send the customer back to the TPP.

Other countries, such as Hong Kong, have so far opted to introduce only recommendation in their Open API Framework about security-protection requirements and technologies related to the authentication of customers. It is expected that in 2020, the HKMA will also define a more detailed set of standards, which may include more security elements, including more sophisticated technology and authentication infrastructure.

In the case of Singapore, their API playbook has defined the recommended authentication standards through tokenized protocols (OAuth 2.0 and Open ID Connect). In other cases, such as Australia, different authentication methods are being tested as part of the implementation of the regime.

Broadly speaking, there are two options for enabling customer authentication: bank-specific (models such as the one described above, where banks need to comply with certain rules) or market-specific schemes (such as eID solutions). We can find examples of eID solution in some Nordic countries, in India (UID), and in New Zealand (Digital Identy NZ).

In the case of India, Aadhaar Auth API allows banks and other financial institutions to verify the identity of the customer instantly, as required by RBI regulations.

6.5 INCENTIVES TO ADOPT OPEN BANKING

Although regulators and market participants recognize the importance of the financial industry taking a leading role in the adoption of open banking, countries are adopting particular measures to kick-start the adoption of a framework.

First, most regulations have taken place after a prior open consultation process and intense dialogue with the industry.

Second, in some cases, standards have been defined in a collaborative manner with the banking industry. One of the clearest examples of such a practice has been the joint publication of API standards by the MAS and the banking association in Singapore.

Having a single point of reference (known as a repository or dashboard) of all open APIs offered by banks is also a measure that some countries, such as Hong Kong, have taken to facilitate ease of access by TPPs. During discussions, some banks suggested that it would be desirable for the Data Studio of the Hong Kong Science and Technology Parks to take up this dashboard role. Hence, the HKMA recommended that all open APIs should be listed under the Data Studio. The listing of open APIs under the Data Studio will not preclude banks from using other repositories. The industry or individual banks are free to list their open APIs in multiple repositories.

Additionally, other practices—such as partnering with interested parties on the promotion of open banking, organizing educational events and competitions on the use of open APIs among the industry, or hosting seminars and workshops for banks and technology companies to share use-case ideas or experience gained elsewhere—are ideas mentioned by different regulators as potential formulas to encourage the adoption of open banking.

An enabling environment in which regulators set standards of a technical or legal nature can provide a baseline that reduces risks for banks and other users, encouraging the use of APIs.

Finally, some market drivers—such as new business models in e-commerce or other areas of digital business that require real-time intercompany processes or real-time payments—are incentivizing the use of APIs.

7. Conclusions and Future Agenda of Open Banking

As described in this document, open banking is to great extent about ecosystem creation and the smart use of data to deliver new products to customers and to encourage competition. There is no single model or solution to achieve these objectives. The models analyzed in this note differ in their approach and scope, in the strictness of the standards or principles defined, and in the definition of the responsible governing bodies, among other things.

Most regulations analyzed under this note came into effect in 2018, so it might be too early to draw substantial lessons, but the following trends are observed:

- In Europe, more TPPs than payment initiators have been authorized as aggregators, signalling higher challenges in the business model and accessing process in the case of the latter.
- Some concrete technical definitions on PSD2 are acting as a bottleneck for the development of TPPs. For instance, requiring the customer to provide consent every 90 days results in a very high rate of dropoff. Also, the fact that PSD2 does not accept variable recurrent payments impedes the inclusion of a wide assortment of use cases. Finally, PSD2 is not contemplating the possibility of a refund on direct payments, giving much less flexibility than traditional payment schemes.
- TPPs claim that the APIs published by banks do not have the quality they require and are not being used, and de facto screen scraping is still prevalent. TPPs claim that there is no real incentive for banks to publish good, free, open APIs.
- As a corollary to the former, some market players argue that it would have been desirable to regulate based more in principles and less in details that in the end require interpretation, and hence are subject to controversy.

Early regulatory efforts have been concentrated on defining standardized API frameworks, creating governance bodies and rules, enhancing security, developing infrastructure, and establishing authentication methods. Among the next items on regulators' agenda in the area of open banking are issues such as the future scope of open banking, competition with other industries, especially with big tech players, and international interoperability.

In that respect, market participants and regulators are starting to talk about the evolution of the scope of open banking toward open finance and smart data. Open finance refers to the capacity of consumers to access their

data via a suite of finance products, including mortgages, savings, insurance, pensions, and so on. On the other hand, smart data suggests the idea of customers accessing their data in nonfinancial services sectors, such as energy, water, mobile, and data from bigtechs. Although the only country to regulate the extension of open banking to other sectors so far is Australia, discussions around it are taking place at different levels in other areas. The idea of reciprocity when giving access to data is a principle that banks are starting to claim as a necessary step toward a level playing field. The Smart Data Review in the United Kingdom and the report of the Canadian Senate Committee on Open Banking also go in the direction of extending access to data to other sectors beyond banking.

Concerning bigtechs, their increasing interest and positioning as financial service providers, especially through banking-as-a-service models, has raised questions about the impact of their access to data from financial institutions. Some banks are starting to claim the idea of reciprocity in the access to customer data to guarantee a level playing field. On the other hand, regulatory authorities are analyzing the implications for financial stability and consumer protection, and also the division of responsibilities between bigtechs and their partnering banks.

Finally, one last element on the agenda of open banking that could contribute to the development of global markets is international interoperability, still at very early stages of discussion. The fact that there is no globally adopted API standard, and that TPPs may need to use different API standards to communicate with banks in different jurisdictions, could lead to potential challenges, such as inefficiencies for third parties or fragmentation of the digital financial ecosystem.

References

ABS (Association of Banks in Singapore) and MAS (Monetary Authority of Singapore). 2019. *Finance-as-a-Service: API Playbook. ABS and MAS, 2019.*

ACCC (Australian Competition and Consumer Commission). 2019. Competition and Consumer (Consumer Data) Rules 2019. Exposure Draft, March 2019.

Accenture. 2018a. "The Brave New World of Open Banking."

Accenture. 2018b. *Making Open Banking a Platform for Industry Transformation: An Australian Perspective.*

Accenture. 2019a. *It's Now Open Banking: Do You Know What Your Commercial Clients from It?*

Accenture. 2019b. *Open Banking in Canada: Opportunity Knocks.*

Accenture. 2019c. *Unlocking Value with Consumer Data Rights Rules.*

Accenture, Avanade, and Microsoft. 2019. *PSD2 and Open Banking: Using Regulation to Kick-Start the Transformation of Banking.*

AEFI (Asociación Española Fintech e Insurtech). 2017. "¿Quién gana la batalla con la nueva directiva PSD2?" December 14, 2017.

Application Programming Interface Evaluation Group. 2018. "Terms of Reference," API EG 002-18, February 28, 2018.

APRA (Australian Prudential Regulation Authority). 2019. *Prudential Practice Guide: Draft CPG 234 Information Security. March 2019.*

Australian Government. 2017. *Review into Open Banking: Giving Customers Choice, Convenience and Confidence. December 2017.*

Badour, Ana, and Arie van Wijngaarden. 2019. "UK Open Banking Implementation Entity Report Released." McCarthy Tetrault, July 26, 2019.

Badour, Ana, Shauvik Shah, and Tyler Hawley. 2018. *Open Banking Update: Canada 2020 Issues Open Banking Report. August 1, 2018.*

Banco Central Do Brasil. 2019. Communiqué 33,455/2019, April 2019.

BBVA. 2019. "Estados Unidos encara el open banking." October 2019.

BCBS (Basel Committee on Banking Supervision). 2019. *Report on Open Banking and Application Programming Interfaces.* Bank for International Settlements, November 2019.

Bhat, Deepa. 2018. "Screen Scraping vs. API—10 Questions to Understand the Differences." *Medium,* October 11, 2018.

Brodsky, Laura, and Liz Oakes. 2017. "Data Sharing and Open Banking." McKinsey & Company, September 5, 2017.

Capgemini and BNP Paribas. 2018. *World Payments Report 2018.*

Capgemini and Efma. 2019. *World Fintech Report 2019.*

CFPB (Consumer Financial Protection Bureau). 2017. "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation." October 18, 2017.

Chaib, Ismail. 2018. "How to Regulate Open Banking." Open Bank Project, November 2018.

Chandran, Sasidharan. 2017. "Open Banking: Implications and Risks." *Financier Worldwide,* July 2017.

CMA (Competition and Markets Authority). 2017. "Guidance: The Retail Banking Market Investigation Order 2017." Gov.UK, February 2, 2017.

Congreso General de los Estados Unidos Mexicanos. 2018. Ley para Regular las Instituciones de Tecnología Financiera. Nueva Ley DOF 09-03-2018.

Cortet, Mounaim. 2018. "Mastering Open Banking: How the 'Masters in Openness' Create Value." Innopay, January 7, 2018.

Creehan, Sean, and Paul Tierno. 2019. "The Slow Introduction of Open Banking and APIs in Japan." *Pacific Exchanges Podcast,* May 2, 2019.

Datahen. 2018. "Data Harvesting War: Scraping vs Using API." *Datahen Blog,* December 14, 2018.

Deloitte. 2018. "Open Banking around the World: Towards a Cross-Industry Data Sharing Ecosystem."

Deloitte. 2019. *Open Banking: A Seismic Shift.*

Department of Finance Canada. 2019. *A Review into the Merits of Open Banking.* Department of Finance Canada/Ministère des Finances Canada, January 2019.

EBA (European Banking Association). "EBA Open Banking Working Group" (website).

EBA (European Banking Authority). 2017. "Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)." EBA/RTS/2017/02, February 23, 2017.

EBA (European Banking Authority). 2018. "Guidelines on the Conditions to Benefit from an Exemption from the Contingency Mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC)". EBA/GL/2018/07, December 4, 2018.

EBA (European Banking Authority). 2019a. "EBA Clarifications to Issues I to III Raised by Participants of the EBA Working Group on APIs under PSD2." March 11, 2019.

EBA (European Banking Authority). 2019b. "EBA Responses to Issues IV to VII Raised by Participants of the EBA Working Group on APIs under PSD2." April 1, 2019.

EBA (European Banking Authority). 2019c. "EBA Responses to Issues VIII to XIII Raised by Participants of the EBA Working Group on APIs under PSD2." April 26, 2019.

EBA (European Banking Authority). 2019d. "EBA Responses to Issues XIV to XX Raised by Participants of the EBA Working Group on APIs under PSD2." July 26, 2019.

EBA (European Banking Authority). 2019e. "EBA Responses to Issues XXI to XXVI Raised by Participants of the EBA Working Group on APIs under PSD2." August 14, 2019.

EBA (European Banking Authority). 2019f. "Opinion of the European Banking Authority on the Elements of Strong Customer Authentication under PSD2." EBA-Op-2019-06, June 21, 2019.

EBA Working Group on Electronic Alternative Payments. 2019. *Understanding the Business Relevance of Open APIs and Open Banking for Banks.* EBA, May 2016.

Endeavor México. 2018. *Termómetro fintech: Los retos de la regulación*.

Eroglu, Hakan. 2019. "The Asia-Pacific Way of Open Banking Regulation." Finextra, June 20, 2019.

Estévez Luaña, Rita. 2019. "Open banking: una nueva oportunidad en la era del 'data.'" CincoDías, September 10, 2019.

European Parliament and Council of European Union. 2015. Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and Repealing Directive 2007/64/EC.

European Parliament and Council of European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

European Parliament and Council of European Union. 2017a. Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 Supplementing Directive (EU) 2015/2366 with Regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication.

European Parliament and Council of European Union. 2017b. Revised Rules for Payment Services in the EU: Summary of Directive (EU) 2015/2366 on EU-wide Payment Services. European Union, March 2017.

EY Americas. 2019. "Why Building Consumer Trust Is Key to Brazil's Open Banking Success." EY, August 14, 2019.

Financial Data Exchange. n.d. *The Global Industry Standard for Consumer Access to Financial Data.*

Freebairn, Pip. 2018. *Response to the Farrell Report into Open Banking: Submission to Australian Treasury. Australian Banking Association,* March 23, 2018.

Gehrke, Nobert. 2019. "Open Banking & Open APIs in Japan." *Medium,* March 28, 2019.

Gilder, Andrew. 2018. "How Open Banking in Singapore May Pivot or Remain Organic." EY, December 17, 2018.

Gobierno de España. 2018. Real Decreto-ley 19/2018 de servicios de pago y otras medidas urgentes en materia financiera. November 2018.

GoCardless. 2017. "Screen Scraping 101: Who, What, Where, When?" *Medium,* July 19, 2017.

Harrison, Megan. 2018. *Open Banking vs. Screen Scraping: What's the Difference?* Infographic. Openwrks, July 5, 2018.

HKMA (Hong Kong Monetary Authority). 2018. *Open API Framework for the Hong Kong Banking Sector.* July 2018.

IDC. 2018. *Who's Ready for OPEN?* Infographic, March 7, 2018.

JBA (Japanese Bankers Association). 2017. *Report of Review Committee on Open APIs: Promoting Open Innovation.* July 13, 2017.

Kanehisa, Naoki, and Kenichi Tanizaki. 2018. "Open Banking in Japan." *Payments & Fintech Lawyer,* July 2018.

KPMG. 2017. *Embracing PSD2 and the Era of Open Banking: Comply, Compete, Innovate.* June 2017.

KPMG. 2018. *Fintech in India—Powering a Digital Economy.* September 2018.

KPMG. 2019. *Open Banking Opens Opportunities for Greater Customer Value: Reshaping the Banking Experience.* May 2019.

Krupena, Silvija. 2019. "Has the Ship Sailed for PSD2 Fallback Exemptions?" RedCompass Labs, March 28, 2019.

Lancos, Peter, and Jonathan Naismith. 2019. "Open Banking Security Risks May Open Pandora's Box." Innovate Finance, May 14, 2019.

Light, Jeremy. 2017. "PSD2: Scoping Out the Impacts of the RTS." Accenture, July 2017.

López Morales, Tomás. 2017. "Tu banco está celoso: no quiere más 'screen scraping.'" *El Pais, December 16, 2017.*

MAS (Monetary Authority of Singapore). n.d. "Application Programming Interfaces (APIs)," https://www.mas.gov.sg/development/fintech/technologies---apis.

Mastercard and Ipsos. 2019. *The State of Pay 2019–2020.* September 2019.

Mathorpe, Roland. 2018. "What Is Open Banking and PSD2? WIRED Explains." *Wired,* April 17, 2018.

McDowell, Brett. 2019. "Open Banking: Why a New Approach to Authentication Is Key to Its Success." The Paypers, March 7, 2019.

McKinsey & Company. 2019. *The Last Pit Stop? Time for Bold Late-Cycle Moves: McKinsey Global Banking Annual Review 2019.* October 2019.

Medici. 2018. *Open Banking Report 2018.* September 2018.

Miyamoto, Koichi, and Hajime Taura. 2017. "Amendments to Legislation on Electronic Payment Intermediate Service Providers." *Anderson Mōri & Tomotsune Financial Services & Transactions Group Newsletter,* June 2017.

Mnuchin, Steven T., and Craig S. Phillips. 2018. *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation.* US Department of the Treasury, July 2018.

Moyer, Kristin. 2016. "BankThink Screen Scraping vs. APIs Is a Sideshow. Here's the Real Battle." *American Banker,* June 15, 2016.

ODI (Open Data Institute) and Fingleton Associates. 2014. *Data Sharing and Open Data for Banks: A Report for HM Treasury and Cabinet Office.* September 2014.

ODI (Open Data Institute) and Fingleton Associates. 2019. *Open Banking, Preparing for Lift Off: Purpose, Progress & Potential.* July 2019.

Online Business Technologies. 2018. *PSD2 and Open Banking: Summary of the Most Important Lessons Learned from the PSD2 Workshop of June 22, 2018.*

Open Banking (web site), https://www.openbanking.org.uk/about-us/.

Open Banking. "Welcome to the Open Banking Standard" (web page), https://standards.openbanking.org.uk/.

Open Banking. n.d. *Background to Open Banking,* https://www.openbanking.org.uk/wp-content/uploads/What-Is-Open-Banking-Guide.pdf.

Open Banking. 2018a. *Open Banking: Guidelines for Open Data Participants.* July 2018.

Open Banking. 2018b. *Participant Guide: Information Security Operations—A Guide to Implementing Effective Information Security Controls.* January 2018.

Open Banking Working Group. 2017. *Open Banking: Advancing Customer-centricity—Analysis and Overview.* EBA, March 2017.

Pallardó, Arturo. 2016. "PSD2: Screen Scraping vs APIs?" Kantox, December 19, 2016.

Pavoni, Silvia. 2019. "What Impact Will Open Banking Have on Brazil?" The Banker, July 2, 2019.

PaymentsNZ. 2019. 2019 *Environmental Scan Report: Developments in the Global Payments Landscape.* August 2019.

Peyton, Antony. 2019. "New Zealand Heads to Open Banking." Fintech Futures, March 4, 2019.

Policy Lab. 2018. *Open Banking: Report on Findings and Resolutions.* Canada 2020, July 5, 2018.

PwC. 2018a. *The Imminent Arrival of the Age of Open Banking: A Shift to the Platform Business Model in Banking.*

PwC. 2018b. *Opening the Bank for a New Era of Growth.* June 2018.

PwC and ODI (Open Data Institute). 2018. *The Future of Banking Is Open: How to Seize the Open Banking Opportunity.*

PYMNTS. 2019. "How APIs Safeguard Bank-FinTech Collaboration." Pymnts.com, May 6, 2019.

RBI (Reserve Bank of India). 2017. *Report of the Working Group on FinTech and Digital Banking.* November 2017.

Read-Parish, Kelly. 2019. "Open Banking vs. Screen Scraping: Looking Ahead in 2019." Finextra, January 4, 2019.

Rothwell, Graham. 2018a. "The Brave New World of Open Banking in APAC: Japan." *Accenture Banking Blog,* October 16, 2018.

Rothwell, Graham. 2018b. "The Brave New World of Open Banking in APAC: Singapore." *Accenture Banking Blog,* September 27, 2018.

Standing Senate Committee on Banking, Trade and Commerce. 2019. *Open Banking: What It Means for You.* Senate of Canada, June 2019.

Stoyanov, Radoy. 2019. "10 Things You (May) Have Forgotten in Your PSD2 Project." BULPROS, April 2019.

The Paypers. 2019. *Open Banking Report 2019: Insights into the Global Open Banking Landscape.*

Thomas, Hamish. 2020. "Open Banking Opportunity Index: Where Open Banking Is Set to Thrive." EY, August 31, 2020.

Thomas, Hamish, and Anita Kimber. 2019. "How Regulation Is Unlocking the Potential of Open Banking in the UK." EY, March 28, 2019.

Tibshraeny, Jenée. 2019. "Payments NZ Releases Standards Detailing How Banks and Fintechs That Engage in Open Banking Have to Protect Consumers' Data." Interest.co.nz, March 4, 2019.

Tink. 2019. "Why 2019 Is the Year of Open Banking." *Tink Blog,* April 2, 2019.

TMI Associates. 2019. "Banking Regulation in Japan." March 2019.

Umezawa, Taku. 2016. "FinTech Developments in Japan and Reform of the Banking Act." NO&T *Japan Legal Update,* no. 6 (August 2016).

WB (World Bank). 2019a. "Open Banking and APIs Survey for Authorities of Hong Kong," October 2019.

WB (World Bank). 2019b. "Open Banking and APIs Survey for Authorities of India," October 2019.

WB (World Bank). 2019c. "Open Banking and APIs Survey for Authorities of the United Kingdom," October 2019.

Which?. 2021. "Open Banking vs Screen Scraping, What Are My Rights?" *Which?,* March 4, 2021.

Whyte, Lindsay. 2019. "Why Is the UK Leading the World on Open Banking?" Medium, January 18, 2019.

Wood, Chris. 2019. "How Does Open Banking Apply to US Banks?" Nordic Apis, April 2, 2019.

Zachadiaris, Markos, and Pinar Ozcan. 2017. "The API Economy and Digital Transformation in Financial Services: The Case of Open Banking". *SWIFT Institute Working Paper No. 2016-001, June 15, 2017.*

Zunzunegui, Fernando. 2018. "La digitalización de los servicios de pago (Open Banking)," Working Paper No. 1. Revista de Derecho del Mercado Financiero, October 11, 2018.

Endnotes

1. There are different definitions of open banking. The Bank for International Settlements, for example, defines open banking as the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, including, for example, those that provide real-time payments, greater financial transparency options for account holders, marketing, and cross-selling opportunities.
2. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/382273/141202_API_Report_FINAL.PDF
3. https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%202%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf
4. https://www.gov.uk/cma-cases/review-of-banking-for-small-and-medium-sized-businesses-smes-in-the-uk
5. The CMA9 includes Lloyds Bank, Nationwide, RBS, Danske Bank, Barclays, HSBC, Bank of Ireland, Allied Irish Bank, and Santander.
6. The initial phase of implementation of Open Banking began in early 2018 and ran until September 2019.
7. https://www.openbanking.org.uk/wp-content/uploads/open-banking-report-150719.pdf
8. https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
9. https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf
10. https://www.stet.eu/en/psd2/
11. https://www.berlin-group.org/psd2-access-to-bank-accounts
12. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
13. https://www.fsa.go.jp/common/diet/193/index.html
14. https://abs.org.sg/docs/library/abs-api-playbook.pdf
15. https://apixplatform.com/landing
16. https://treasury.gov.au/sites/default/files/2019-03/Review-into-Open-Banking-_For-web-1.pdf
17. https://treasury.gov.au/consumer-data-right
18. https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf
19. https://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm
20. https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf
21. https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf
22. https://www.nacha.org/news/nachas-api-standardization-industry-group-names-first-five-apis-develop-support-payments
23. https://cdn.shopify.com/s/files/1/0038/4987/9625/t/4/assets/8.23_FDX_WhitePaper_Final.pdf?2846
24. https://paymentsdirection.atlassian.net/wiki/spaces/PaymentsNZAPIStandards/overview
25. https://indiastack.org/about/
26. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF
27. https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10598
28. https://www.fin.gc.ca/activty/consult/2019/ob-bo/pdf/obbo-report-rapport-eng.pdf
29. https://sencanada.ca/content/sen/committee/421/BANC/reports/BANC_SS-11_Report_Final_E.pdf
30. http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf
31. https://www.bcb.gov.br/content/config/Documents/BCB_Open_Banking_Communique-April-2019.pdf
32. The comprehensive list of registered TPPs is available at https://euclid.eba.europa.eu/register/pir/search.
33. https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2018/20180718e5a2.pdf
34. https://www.openbanking.org.uk/wp-content/uploads/Guidelines-for-Open-Data-Participants.pdf

35. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389&from=EN
36. https://www.openbanking.org.uk/wp-content/uploads/Participant-Guide-Information-Security-Operations.pdf
37. https://www.apra.gov.au/sites/default/files/draft_prudential_practice_guide_cpg_234_information_security_march_2019.pdf
38. https://apixplatform.com/landing
39. https://finconecta.com
40. https://www.imf.org/en/Publications/Policy-Papers/Issues/2018/10/11/pp101118-bali-fintech-agenda
41. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf
42. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf
43. https://sencanada.ca/content/sen/committee/421/BANC/reports/BANC_SS-11_Report_Final_E.pdf
44. https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from-contingency-measures-under-article-33-6-of-regulation-eu-2018/389-rts-on-sca-csc-
45. https://sso.agc.gov.sg/Act/PDPA2012
46. https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html
47. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10598&Mode=0

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP