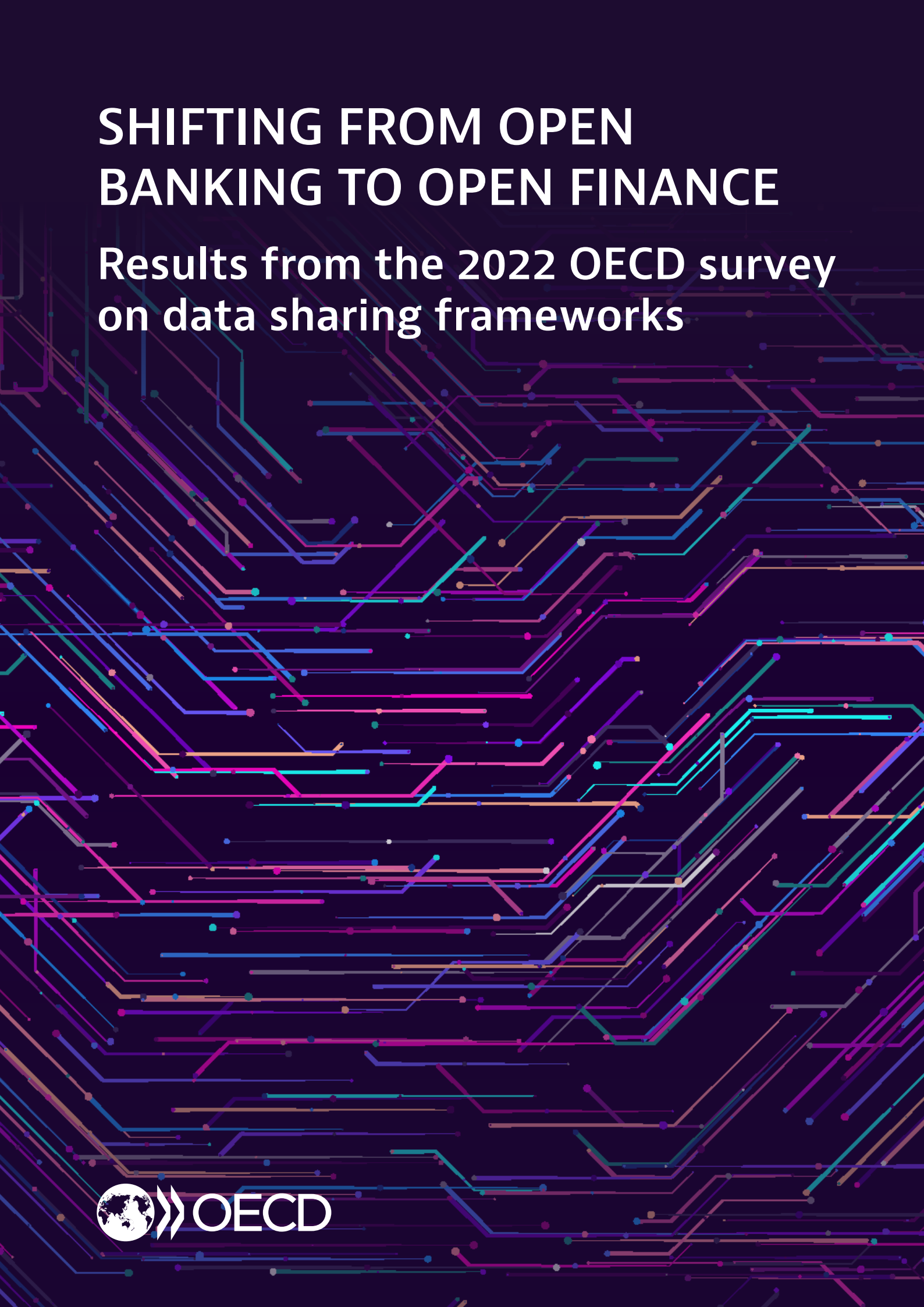
SHIFTING FROM OPEN BANKING TO OPEN FINANCE

Results from the 2022 OECD survey on data sharing frameworks



OECD

Please cite as: OECD (2023), *Shifting from Open Banking to Open Finance: Results from the 2022 OECD survey on data sharing frameworks*, OECD Business and Finance Policy Papers, OECD Publishing, Paris, https://doi.org/10.1787/9f881c0c-en.

Data sharing arrangements are evolving from Open Banking to Open Finance. This next stage of the evolution builds upon existing frameworks to expand data access and data source sharing beyond payment/transaction data, while also including other areas of financial activity (e.g. insurance). This paper analyses the different types of data sharing frameworks currently available in OECD and non-OECD member countries. It examines the specific rules and conditions of such frameworks around data access and sharing, consumer safeguards, and operational and technical specifications. It also discusses learnings from existing frameworks on the impact that such arrangements have had on customers and financial markets.

Foreword

This report analyses the different types of data sharing frameworks that have been established in OECD and non-OECD countries. It examines the specific rules and conditions of such frameworks around data access and sharing, consumer safeguards, operational and technical specifications. It also discusses learnings from existing frameworks on the impact that such arrangements have had on customers and financial markets.

The report has been drafted by *Iota Kaousar Nassr* and *Hyojeong Kim* under the supervision of *Robert Patalano* from the Division of Financial Markets of the OECD Directorate for Financial and Enterprise Affairs. Liv Gudmundson provided editorial and communication support.

The report supports the work of the OECD Committee on Financial Markets and is a product of its Expert Group on Finance and Digitalisation, both chaired by *Aerdt Houben*. It was first discussed by the Expert Group on 5 October 2022 and then approved by written procedure by the Committee in November 2022. The report was declassified on 9 December 2022.

The author gratefully acknowledges valuable input and constructive feedback provided by the following individuals and organisations: *Peter Johnson, Claire McKay and Jocelyn Co-oper*, Department of the Treasury of Australia; *Angelika Schlögel, Timo Frömmel and Dominic Winkler*, Federal Ministry of Finance, Austria; *Abraham Tachjian and Read Guernsey*, Finance Canada; *Gonzalo Arriaza, Tomás Pintor, Constanza Mella,* Ministerio de Hacienda, Chile; *Francisco Javier Duque Sandoval*, Superintendencia Financiera, Colombia; *Andrea Maria Oconitrillo Rojas* CONASSIF, Costa Rica; *Alex Ivančo and Lenka Franče Rejzková*, Ministry of Finance of the Czech Republic; *Kristen Leppik and Marit Maidla*, Ministry of Finance, Estonia; *Tatu Räsänen* Bank of Finland*; Beranger Butruille*, Banque de France and *Arthur Frappereau*, Direction Générale du Trésor, France; *André Witt*, Deutsche Bundesbank and *Finn Strickert*, Bundesministerium der Finanzen, Germany; *Péter Sajtos* and *Magyar Nemzeti*, Bank Hungary; *Mai Santamaria*, *Mark Curran and Jefferson Vieira*, Department of Finance, Ireland; *Daniel Hahiashvili*, Bank of Israel; *Ilaria Supino* and *Giuseppe Ferrero*, Banca D'Italia; *Ryosuke Ushida*, Financial Services Agency, Japan; *Ieva Bite* and *Dina Buse*, Ministry of Finance of the Republic of Latvia; *Eleftheria Kostika*, Bank of Greece; *Nora Marija Laurinaitytė*, Bank of Lithuania; *Karen O'Sullivan*, Commission de Surveillance du Secteur Financier Luxembourg; *Luis Urrutia*, Banco de Mexico; *Coen ter Wal, Marc van der Maarel, Gibran Watfe*, De Nederlandsche Bank; *Adam Głogowski*, National Bank of Poland; *Bae Sooam*, Financial Services Commission, Republic of Korea; Adam Nádaský, National Bank of the Slovak Republic; *Borut Poljšak*, Bank of Slovenia; *Luz Seoane*, Ministry of Economic Affairs and Digital Transformation, Spain; *Benjamin Müller, Nicolas Brügger,* Swiss State Secretariat of International Finance; *Necmettin Mete Sakallioğlu, Mehmet Zahid Samancıoğlu*, Ministry of Treasury and Finance of Türkiye; *Patrick Keenan and Fayyaz Muneer*, HM Treasury, UK; *Dan McGonegle*, Federal Reserve System, US and *Peter Grills* and *Evan Enns*, US Treasury; *Alisdair McDade, João André Calvino, Marques Pereira*, Central Bank of Brazil; *Ada Kwok*, Hong Kong Monetary Authority; *Dino Lazaridis*, Financial Sector Conduct Authority South Africa.

Table of contents

FIGURES

Executive summary

Open Finance could be described as the next stage in the evolution of Open Banking-type of data sharing arrangements. Building on existing frameworks, it expands data access and sharing to data sources beyond payment/transaction data, while it also includes other areas of financial activity (e.g. insurance). This draft report analyses the different types of data sharing frameworks that have been established in OECD and non-OECD countries.[1] It examines the specific rules and conditions of such frameworks around data access and sharing, consumer safeguards, operational and technical specifications. It also discusses learnings from existing frameworks on the impact that such arrangements have had on customers and financial markets.

The concept of Open Banking is generally well understood as the practice of sharing banking data via standardised and secure interfaces at the request of clients. In most cases, it allows for the secure sharing of a customer's financial information with third party service providers, with customer consent. It generally – although not necessarily – also includes the ability of third-party service providers to initiate payments on behalf of a customer, with explicit customer's consent. Data sharing frameworks can vary significantly depending on the entities obliged to make data shareable; the type of customers entitled to share data; how data is shared between the parties; and the entities with which data can be shared. In addition, the timing of the data sharing (real time vs. deferred) and the standardisation of transmission mechanisms (e.g. APIs) make a huge difference between both frameworks in terms of the usability of data.

Most OECD countries have established specific frameworks for Open Banking or other similar arrangements for access to financial account/payment data. EU member countries have transposed PSD2 into national law, setting the basic requirements for allowing access to accounts. Other countries are in the process of setting up their frameworks (e.g. Canada, Chile). The US and Switzerland as OECD countries with a primarily market-led approach to open finance. When it comes to extending the framework to Open Finance and Open Data more broadly, Australia has explicitly extended its framework to the energy and telecommunications sectors, is expanding to the non-bank lending sector and assessing other financial sectors. In Brazil, other areas covered under Open Finance include insurance, open pension funds, investment and foreign exchange which demanded co-operation among other regulatory and industry entities. In Israel, sharing of information includes securities and deposits.

Open Finance arrangements have multiple objectives with common themes around fostering innovation, encouraging competition and customer empowerment and choice found across the OECD countries' frameworks. Innovation can be promoted through the development of new, innovative products and services in the banking and payments sector, and even beyond. The promotion of innovation can have a knock-on positive effect on competition conditions in financial services in particular. Customer experience

[1] The report is based on 34 responses to the OECD Survey by 31 OECD countries: Australia, Austria, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, Poland, the Slovak Republic, Slovenia, Korea, Spain, Switzerland, Türkiye, UK, US, as well as by three non-OECD member countries Brazil, Hong Kong (China) and South Africa.

can be enhanced by allowing for the possible provision of more efficient and less costly services. Client empowerment is indeed being sought, as financial services customers possess control of their data and decide on which data they provide under such data access and sharing arrangements.

The establishment of the Open Banking and other data sharing frameworks has contributed to the emergence of various active use-cases in a variety of areas within the financial services space. These are found primarily in the payment space, with payment account information services, payment initiation services, and aggregation services by new intermediaries. Other services based on innovative business models emerging on the basis of such frameworks include credit scoring applications, debt management tools, wealth management applications, alternative payment services, product comparison, account verification and balance checks by third parties and other such as cloud account management for small businesses.

OECD countries have reported evidence that data sharing frameworks produce positive impacts to customers and financial services, fostering innovation, increasing competition, lowering costs, and delivering better customer experiences. Such frameworks encourage third party providers, such as FinTech start-ups, to offer existing services in a different way, or to provide new services to customers on the basis of data access. The impact of Open Banking and other data sharing frameworks on the FinTech industry can be observed both in regard to growth and diversity of companies active in several OECD countries. This has a knock-on effect on competition in the market for financial services, which has indeed been reported since the implementation of data sharing frameworks in several OECD economies.

Open Finance is expected by OECD countries to stimulate competition by de-monopolising data and improving information availability, while also encouraging the emergence of cheaper and better financial products for consumers. Indeed, lower prices have been observed in several OECD countries for specific financial services (e.g. lower fees). Importantly, some countries reported that significant proportions of customers claim that such platforms are helping them keep to budgets, reduce unnecessary expenditure, shop around and minimise fees and charges. Open Finance could further contribute to the creation of new business models, to the servicing of previously underserved parts of the population, and to the offering of better customer experience. Another possible impact for the FinTech market involves greater and closer co-operation between banks and FinTechs, as seen in Japan and the EU, or the emergence of new participants (e.g. account information service providers or aggregators). Nevertheless, many OECD members expect that the impact remains to be seen in the future.

The results of the OECD Survey showcase the gradual evolution of open banking-related frameworks towards an expanded set of data types and other sectors of the financial (and non-financial) market, in what is being described as Open Finance. While this evolution is taking place at different paces, common themes appear between different OECD and non-OECD countries approaches and experiences, and common challenges remain to be addressed. Building on the results of the OECD Survey, further analysis may be warranted on how access to financial customer data can be ensured in a responsible and safe manner; how liability should be attributed and what other consumer safeguards need to be in place (e.g. around consent); but also whether and how there is a need to support the development of technical infrastructure that will promote data interoperability, without undermining the technology neutral approach to regulation that most OECD economies endorse.

1 Frameworks for Open Finance

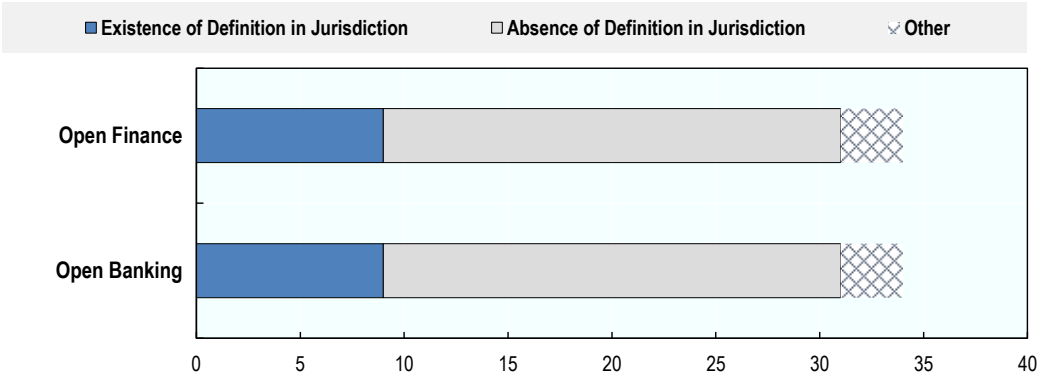
1.1. Data sharing frameworks in OECD member countries

Open Finance can be described as an extension or evolution of Open Banking, and as such, it is worthwhile to start by examining the frameworks in place for Open Banking. There is no legal definition of Open Banking in most OECD countries (Figure 1.1), however, the concept is generally well understood as the practice of sharing banking data via standardised and secure interfaces at the request of clients. In the UK, it is defined as the framework which allows for the secure sharing of a customer's financial information with third party service providers (Account Information Service Providers or "AISP"), with customer consent. As part of that description, it also includes the ability of third-party service providers to initiate payments on behalf of a customer, with that explicit customer's consent (Payment Initiation Services "PIS").

In the EU context, Open Banking primarily refers to payment account-related data (EU PSD2 regulation), in accordance with the rules set down in the Directive (EU) 2015/2366 on payment services (PSD2) and the Commission Delegated Regulation (EU) 2018/389. The goal of PSD2 was to open up the EU payment market to more competition, by allowing third party providers ("TPPs") to have access to payment accounts held at account servicing payment service providers ("ASPSPs", most commonly banks, previously holding the monopoly on payment account data and payment services).

Countries with an explicitly defined Open Banking framework include Australia, Brazil, Colombia, Israel, Korea and Türkiye. In Israel, the Financial Information Service Act, enacted in November 2021, prescribes that information sources (mainly banks) have to share their data with TPPs. A directive of the Banking Supervisor details the standards and other relevant regulation on the matter (Regulation 368). In Türkiye, Open Banking services are defined in the Regulation on Information Systems and Electronic Banking Services of Banks as "an electronic distribution channel through which customers or parties acting on behalf of customers can perform banking transactions or instruct the bank to perform their banking transactions by remotely accessing the financial services offered by the bank through methods such as API, web service, file transfer protocol".

Figure 1.1. Defining Open Banking and Open Finance



Source: OECD Survey.

In Korea, the Financial Services Commission, which oversees Korea's financial policy, established an open banking policy in order to enhance competition in the financial market and maximise the welfare of consumers. The policy allowed competitors such as third-party companies to have fair access and to use of financial infrastructure, targeting holders of essential facilities such as banks that had a monopoly nature. In particular, open banking in Korea refers to policies and systems related to open financial payment infrastructure that provide core financial functions to third-party institutions in the form of standardised open APIs, and through this, fintech companies and financial companies can provide payment and settlement services.

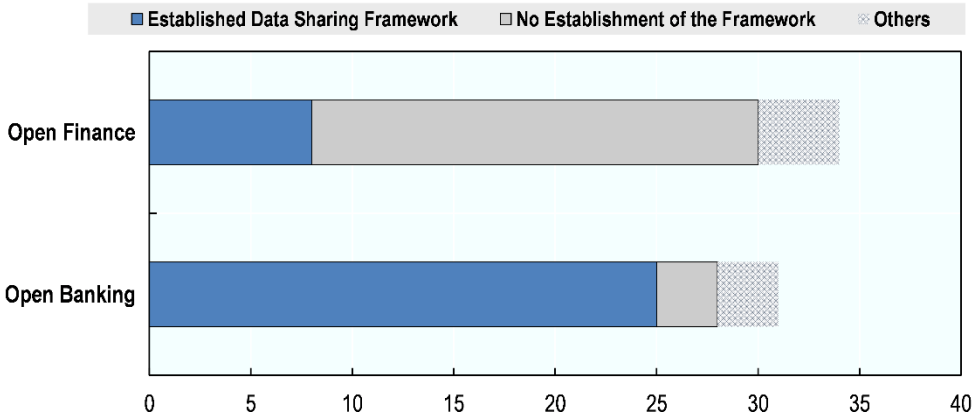
Open Finance is defined in even fewer jurisdictions and generally builds on the Open Banking definition to expand to other data sources and types. In Israel, Open Finance includes a scope of data that is wider than for Open Banking and relates to current accounts, card data, deposits, saving, loans and securities. In Australia, Part IV of the Competition and Consumer Act 2010, enacts and establishes a consumer data right. The Consumer Data Right (Authorised Deposit Taking Institutions) Designation 2019 designates the banking sector (also known as authorised deposit-taking institutions) as subject to the CDR. In Australia, Open Finance is defined as non-bank lending, general insurance, and superannuation. Targeted datasets from non-bank lenders are being designated in a similar way to banks. Datasets of other sub-sectors within Open Finance, including general insurance and superannuation, are being assessed for designation. In the Netherlands, the term Open Finance is used to refer to an opening up of financial institutions' business model to collaborations with third parties, fuelled by data sharing and adoption of APIs. This can enable "banking/insurance-as-a-service" or platformisation strategies, where banks/insurance offer a platform to third parties. Korea's open finance is a concept that expands existing open banking to other financial sectors, functions, and products.

1.1.1. Frameworks for Open Banking and Open Finance

Most OECD countries have established specific frameworks for Open Banking. EU member countries have transposed PSD2 into national law, setting the basic requirements for allowing access to accounts. Being authorised under PSD2 to provide account information services means that the TPP can access an existing payment account (such as a payment account held with a bank) in order to collect data from that account and provide a service to the owner of that bank account. This access is limited to the retrieval of data and the aggregation of information stemming from different payment accounts; additional services that can be provided in that context are of a different nature, notably price comparisons, proposal of tailored products, etc. The powers of a payment initiation service provider are larger as he can initiate payments on the customer's behalf, from their bank account.

In Japan, the Banking Law was amended in 2018 to promote open banking initiatives by which banks are required to open their APIs as a non-binding obligation so that FinTech companies (e.g. electronic settlement agents) can access the banks' system. More than 90% of banks have concluded API agreements with one or more electronic payment service providers as a result of the amendment of Banking Law, which requires banks to enable API connections within a certain period of time after the law comes into effect.

Figure 1.2. Established framework for Open Banking and Open Finance



Source: OECD Survey.

In some countries, the frameworks have been introduced into law but the secondary regulation allowing for their implementation has not been issued. For example, in Mexico, the main obligation to provide open banking information on payments and transactions is contemplated in law, but the implementing regulation has not been issued yet. Under a statutory provision included in the Law for the Regulation of Financial Technology Institutions passed by Congress in 2018 (Article 46), all banks in Mexico, among all other financial institutions, are obligated to set up, according with rules issued by the competent regulator (the National Banking and Securities Commission), standardised application programme interfaces (APIs) that allow the connectivity with and access by other APIs developed or operated by other financial institutions or third parties specialised in information technology, so that such banks are able to share information within the following categories: open financial data; aggregated data; and transactional data. Conversely, in Israel, Directive 368 sets up open banking framework in payments, but due of lack of legislation it is limited and has not yet been implemented.

Other countries are in the process of setting up their frameworks. Canada, for example, issued a mandate in March 2022 for the development of a “made-in-Canada” regime based on the recommendations in the final report of the Advisory Committee on Open Banking. The current focus is on establishing the open banking system and the initial focus is to look at “read-access” whereas “write-access”, such as payments, is not in scope at this time.

The US and Switzerland are the OECD countries with a primarily market-led open finance approach. In Switzerland, an association is in charge of co-ordinating API standards. Formal and informal fora dedicated to open finance have been created, also between the regulator and market participants. The Swiss framework is designed to cover the whole financial sector. For now, standards have been created and used in areas beyond payments (e.g. wealth management data).

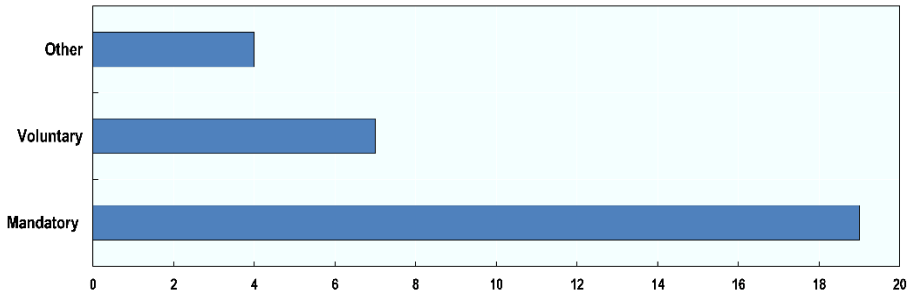
The regulation of the open finance model in Colombia was recently issued through Decree 1 297 of July 2022 which provides for the initiation of payments and the offering of products and services through schemes like banking as a service (BaaS). There it indicates that the Financial Supervisor (SFC) will establish the technological, security and other standards that it deems necessary for the development of the open financial architecture in Colombia. In this sense, the Financial Supervisor is designing its strategy that allows defining interoperable open financial architecture standards that promote competition.

When it comes to extending the framework to Open Finance more broadly, Australia has explicitly extended its framework to other sectors: a framework for energy data sharing has been established; the telecommunications sector has been designated; other open finance sectors are under consideration by the Australian Government. In Brazil, other areas covered under Open Finance include insurance, open

pension funds, investment and foreign exchange. In Israel, sharing of information includes securities and deposits, but does not include insurance. However, the Financial Information Service Act allows the Finance Minister of Israel to add other financial information to the frame of the Act but that is not likely to take place in the near future.

In Korea, the Korea Financial Telecommunications and Clearings Institute established an open banking platform in 2019, which supports the exchange of various information data such as payment, transaction, insurance, investment between fintech companies and financial companies and between financial companies.

Figure 1.3. Mandatory or voluntary character of data sharing arrangements



Note: Other include mandatory character for some intermediaries only; time-limited mandatory requirements that have now expired or work-in-progress frameworks that are yet to be implemented.
Source: OECD Survey.

Data sharing arrangements in OECD countries are in their majority mandatory. In the EU context, PSD2 and all relevant Regulatory Technical Standards and Guidelines are mandatory for payments accounts. In particular, sharing of user payment account data is mandatory for the intermediary that supplies online/mobile banking services to their customers, upon request and with consent by the user; the account access is restricted to licensed TPPs acting on behalf of the user and under her/his consent. In Australia, any CDR designated data holders are required to participate and make available certain data under the Consumer Data Right Rules. In Türkiye, the top 10 banks are obliged to open their Payment Initiation and Account Information API Services by December 2022, while the rest of the banks have until December 2023 to oblige.

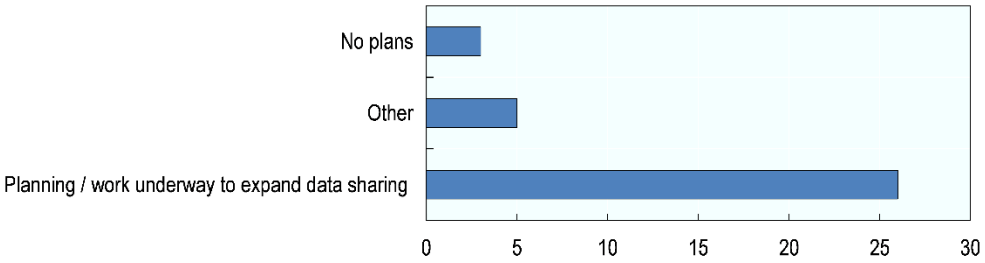
In the case of the UK, Open Banking is mandatory for Account Servicing Payment Service Providers (ASPSPs) under the PSRs, and detailed technical and operational requirements apply additionally to the CMA 9 under the CMA Order. ASPSPs are required to allow access to customers' payments account data without contract, without charge and without restriction or discrimination. Open Finance is not currently mandatory. Smart Data[2] will impose mandatory data sharing across specific sectors for which a scheme is established. Establishing such a scheme would require government to bring forward secondary legislation setting out the specific parameters of the smart data scheme within the context of a particular sector. Open finance could be established as one of the sector specific schemes under Smart Data, in which case it would become mandatory, but there has been no decision or policy commitment by Government to do so at this stage.

[2] 'Smart Data' refers to the secure, consented sharing of consumer and product data with third-party providers (TPPs) who can use this data to provide innovative services for consumers and SMEs. We consider this an extension of the "right to consumer data" under the General Data Protection Regulation (GDPR). For more see (Siobhan Dennehy, 2022[3]).

The timing of adoption of mandatory or voluntary frameworks also differs across OECD economies. In the case of Japan, a non-binding obligation for banks to enable API connection was a time-limited measure that is no longer effective. In Chile, a Fintech and Open Finance bill is being discussed in Congress at the time of the writing of this report, in an advanced constitutional stage. This bill contains a sharing framework in areas other than payments, covering directly for a broader framework of Open Finance, and the bill establishes a mandatory framework for such data sharing. In the case of Canada, where the framework is still being designed, requirements have yet to be established, however, Canada's Advisory Committee on Open Banking recommended that all Canada's federally regulated banks be required to participate in the open banking system, while provincially regulated financial institutions (credit unions) may participate voluntarily.

The character of the frameworks differs by countries. Currently, Korea's open banking has been implemented in the private sector in accordance with the policy direction of the Financial Services Commission without a separate law. In fact, it is operated in accordance with regulations set by the Board of Directors, which consists of the Korea Financial Telecommunications and Clearings Institute (KFTC), a specialised payment and settlement institution, and banks. Outside the OECD, Hong Kong China has adopted a collaborative, non-legislative, approach. In Brazil's framework, participation for data sharing is mandatory for the largest institutions and conglomerates, while other licensed firms might participate by observing a data reciprocity requirement. Regarding payment initiation, participation is mandatory for all institutions that hold accounts that can be used via digital means.

Figure 1.4. Work underway for the expansion of data sharing arrangements



Source: OECD Survey.

Most OECD countries are planning or are in the process of discussing further development of their data sharing frameworks and/or their expansion to other sectors beyond payments/transactions. In the EU, the revision of the PSD2 legislation and the Open Finance consultation pave the way for developments in this area. In Australia, the government is currently progressing its policy agenda to strengthen and deepen the CDR's functionality, including through the implementation of third-party action initiation reforms, including payment initiation. This will require amendments to the primary legislation followed by the development and maintenance of rules and standards. This will be a multi-stage process as the CDR continues to expand and new use cases are brought into the CDR. A similar phased approach is promoted in Türkiye, where there are plans to include different payment types such as recurring payments and batch payments in the second phase of implementation of such framework. Korea plans to continue to upgrade the functions of its open finance framework, expand its scope, and secure additional participating institutions in the future.

In the US, a July 2021 Executive Order encouraged several efforts to promote competition, including encouraging the Consumer Financial Protection Bureau (CFPB) to pursue rulemaking to facilitate the portability of consumer financial data. (The White House, 2021[1]) The CFPB added open banking to its rulemaking priorities for 2022. In Japan, JFSA continues to explore to further develop open banking ecosystem through dialogue with banks and various FinTech companies. In Switzerland, the framework

already covers the whole financial sector, however, its implementation does not yet cover every sector and additional standards are in the workings.

Non-OECD members are also advancing the development of Open Finance frameworks. In December 2020, the Financial Sector Conduct Authority (FSCA) of South Africa published an Open Finance research paper requesting comment to initial thinking. Stakeholders provided valuable comments and suggestions ranging from identifying topics to be explored further to suggesting possible standards needed to implement a successful Open Finance framework. Following several workshops with the industry, and discussion around consent, customer protection and dispute mechanisms for Open Finance, as well as discussions around data sharing standards, commercial models and data protection for open finance, the FSCA is planning to release a potential Open Finance Position Paper during 2022.

Brazil is also planning to further enhance its data sharing framework by putting in place a service regarding forwarding loan proposals, which will allow banking correspondents that have established agreements with some financial institutions to forward several loan proposals to clients. The expectation is to have credit marketplaces in the medium/long term. Open Finance is not meant to be taken as a static model, but rather an evolutionary one. Although defining the technical standards is a challenge in the short term, the scope is understood by Brazilian authorities as dynamic in nature, enabling new solutions in the long run.

1.1.2. Objectives of data sharing arrangements

Open Finance arrangements have multiple objectives with common themes around innovation, competition and customer empowerment and choice found across the OECD countries' frameworks. By way of illustration of such objectives enshrined in law, the PSD2 regulation in Europe aimed at ensuring an efficient and competitive market that allows existing and new service providers, regardless of their business model, to offer their services within a clear legal framework, while ensuring a high level of data security and privacy (to safeguard payment transactions) in order to enhance consumer protection. Similar objectives are pursued by data sharing frameworks in other OECD economies; for example, the objectives of the Korean framework are the support for the launch of innovative financial services through payment infrastructure and the increase of consumer welfare through fair competition.

Innovation can be promoted through the development of new products and services in the banking and payments sector and even beyond. Such schemes can provide a secure, controlled and convenient operating environment to allow banks and FinTechs or other third-party service providers to work together and develop innovative and integrated banking services that improve customer experience, while keeping up with international developments in the delivery of banking services. In Japan, the 2018 amendments to the Banking Law established an institutional framework aimed at promoting open innovation between financial institutions and Fintech companies while ensuring user protection.

Such promotion of innovation can have a knock-on positive effect on competition conditions. In the UK, the CMA's requirement on the nice banks to maintain and release data in accordance with Open APIs was put in place as a remedy to the adverse effects on competition in the UK retail and SME banking market which were identified in its Retail Banking Market Investigation Final Report (2016). The aims of the remedy are to address barriers to accessing information, enable customers to properly assess products and remove information asymmetries and incumbency advantages, and facilitate the growth of a dynamic intermediary sector.

Customer experience can be enhanced by allowing for the possible provision of more efficient and less costly services, while fostering competition in the market for financial services in particular. Client empowerment is being sought, as financial services customers become masters of their data and possess and control the data they provide and compile for them under such data access and sharing arrangements. The Australian CDR is designed to give consumers greater choice and control through the convenience of a simple, easy-to-use process. In Brazil, one of the most important objectives of Open Finance is to put

consumers back in control of managing their financial data. This occurs from the recognition that the consumer is the owner of their data and has the right to its portability to other regulated institutions. Open Finance initiatives also have the potential to improve financial access through FinTech applications built on the basis of such data sharing arrangements, with the potential to encourage financial inclusion.

Bringing third parties into a regulatory framework to ensure data security and consumer protection is another important objective. In the US, while there are no specific open banking initiatives, other legislation, GLBA, establishes the principles of consumer information protection and privacy. In Canada, the Advisory Committee on Open Banking established six key consumer outcomes to guide the vision and provide a basis for an open banking system in Canada: consumer data is protected; consumers are in control of their data; consumers receive access to a wider range of useful, competitive and consumer friendly financial services; consumers have reliable, consistent access to services; consumers have recourse when issues arise; and consumers benefit from consistent consumer protection and market conduct standards.[3]

1.2. Financial data intermediaries

In the EU context, account information service providers (AISPs) are regulated financial data intermediaries under PSD2. Moreover, under the new EU Data Governance Act, data intermediation services could also include providers that enable consent management or provide technical intermediation. Such a broader definition of data intermediaries would therefore cover additional entities.

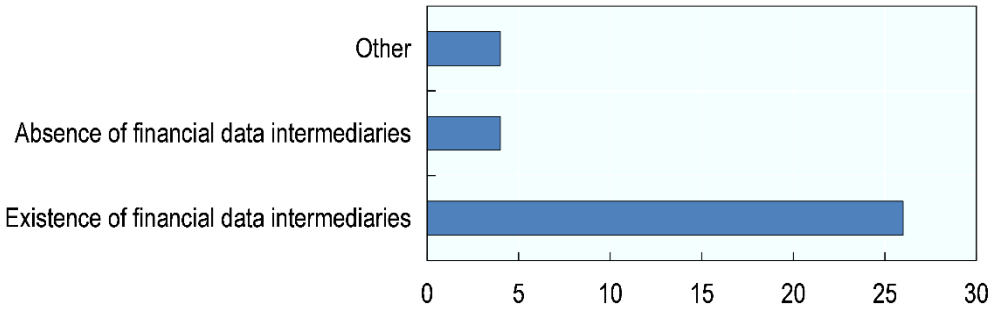
So-called “API aggregators” entered the EU market following the introduction of PSD2 regulation. These are companies with a PSD2 licence that have developed API interfaces for many different ASPSPs (being mostly banks) and position themselves between the third party that provides account information services (AIS) and the ASPSP. Examples of such aggregators include Trask in the Czech Republic, the Dutch Invers, the Spanish Salt Edge. Similar aggregators exist in the US (Plaid; Finicity), and the UK (TrueLayer).

If a company wants to offer its services to customers based on payment account data, and it wants to do so by means of access to payment accounts as the PSD2 regulates, then such a company can choose to do so via an aggregator. This has two advantages for the company concerned. Firstly, the company itself may not need to apply for a PSD2 licence, saving time and cost and avoiding the ongoing compliance activities that would be required otherwise. Secondly, the company also saves on IT investment costs for software development for example, because TPPs offering payment initiation services (PIS) and/or AIS no longer have to develop and maintain the APIs themselves, but rather outsource this to the aggregators. However, aggregators are themselves costly and add an extra layer of intermediation.

[3] https://www.canada.ca/en/department-finance/programs/consultations/2021/final-report-advisory-committee-open-banking.html

1.2.1. Current financial intermediaries

Figure 1.5. Existence of financial data intermediaries



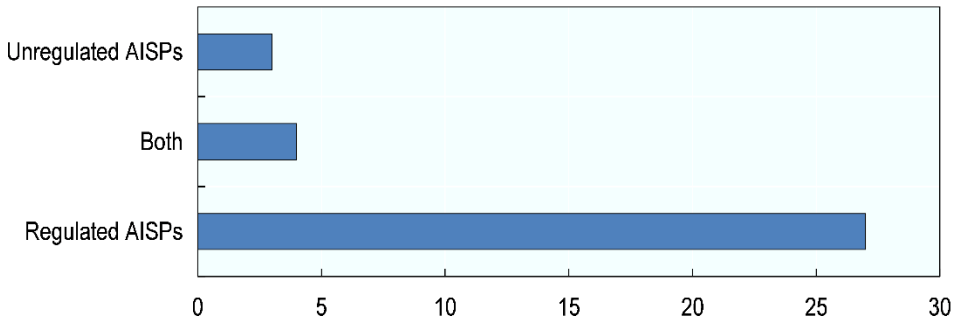
Note: Other includes countries where financial data intermediaries exist but are not regulated or countries where the size of such activity is insignificant.
Source: OECD Survey.

In the UK, the Open Banking Implementation Entity (OBIE), the entity that helps the ecosystem to function, has developed open-source technical standards and industry guidelines that support Open Banking. In this ecosystem, the FCA manages the licensing of TPPs that are authorised to access consumer data with consumers' explicit consent (and / or initiate payments). Under the regulations, consumers can determine who has access to their data and can revoke access at any point (UK Government, 2021[2]).

In Australia, commercial intermediaries collate financial data from banks and other parties, provide value-add services, and make this data available via APIs. These intermediaries are also able to operate under the consumer data right, subject to them becoming accredited data recipients and meeting regulatory requirements.

Intermediaries in some OECD countries, such as the US and Israel, as still using screen scraping techniques to source the data, a practice that involves additional risks (see Figure 3.2). In Israel, there are also intermediaries that are giving services using the Credit Data Register.

Figure 1.6. Existence of regulatory and supervisory framework for financial data intermediaries



Source: OECD Survey.

In the EU, PSD2 provides for the primary legal framework for both AISPs and so called "API aggregators", or so-called "technical service providers" in the context of PSD2 and such financial data intermediaries are regulated and supervised by domestic authorities. Such providers must observe the necessary data

protection and security requirements established by PSD2 and the national secondary regulations transposing PSD2, which may differ between different EU member states. Indicatively, in Ireland, AISPs must be registered by the Central Bank of Ireland and listed in the Registers on the Central Bank of Ireland website, and are subject to AML/CFT obligations, fitness and propriety requirements, and other. In Estonia, according to Payments Institutions and E-money Institutions Act (PIe-MIA) an activity licence for provision of payment services, including account information services, shall be issued to a company founded in Estonia or revoked by a decision of the Financial Supervision Authority (FSA). The FSA exercises supervision over compliance of the activities of a payment institutions and persons who have a qualifying holding in the payment institution. In Poland, there are 22 non-bank AIS providers and 13 non-bank PIS providers based in the country (defined as entities licensed to provide these services by the Polish FSA). Taking into account the possibility of cross-border provision of PSD2 services within the EU, a total of 103 EU entities licensed to provide AIS services and 87 ones licensed to provide PIS services declare the intent to provide these services in Poland. Moreover, seven banks in Poland provide AIS services and five banks provide PIS services. Three additional banks use AIS procedures to verify customer identification during the credit granting process.

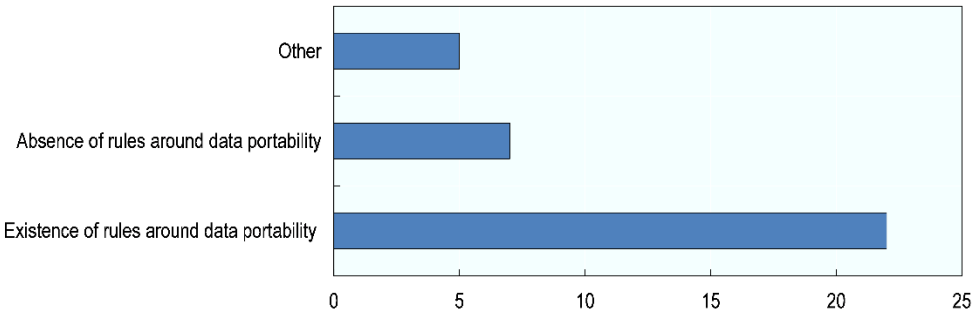
In Australia, financial data intermediaries are required to comply with the general privacy laws in Australia (Privacy Act 1988) to the extent that they handle personal information. Other requirements exist where intermediaries deal with taxation, accounting, payroll and superannuation related data. Where financial intermediaries/service providers wish to receive data under the consumer data right they must become an Accredited Data Recipient (or use one of the legislated pathways), which is subject to a number of obligations under the CDR framework including privacy safeguards which regulate the handling of collected data.

In Japan, Electronic Payment Service Providers (or Electronic Settlement Agent), which correspond to AISPs and PISPs under PSD2, are required to obtain license under the amended Banking Law. In the US, while a number of the largest bank service providers are under the supervision of the Federal Banking Agencies (Federal Reserve, FDIC, and OCC), not all data intermediaries are included in the supervision programme. Similarly, in Brazil, AISPs are not regulated, but licensed institutions may also provide the service of data aggregation, including payment initiation institutions.

1.3. Data portability

When it comes to data portability provisions, the situation is straightforward for EU member states, where data portability among jurisdictions is regulated by the requirements of EU legislation for the General Data Protection Regulation (GDPR) (art.44-48). Article 20 of the GDPR (“right to data portability”) provides that the data subject under that Regulation shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another without hindrance from the controller to which the personal data have been provided, where specific circumstances are met. In some countries, such as Spain, GDPR is complemented by domestic legislation (in this case Law 3/2018) protecting personal data and guaranteeing digital rights, where the right to data portability is established in the same terms.

Figure 1.7. Existence of rules around data portability



Source: OECD Survey.

In the UK, the Information Commissioner's Office (ICO) has stated that PSD2 and Open Banking are a keyway in which financial institutions meet their data portability obligations. With regard to Open Banking, the Application Programming Interfaces (APIs) allow individuals and SMEs to share the financial information that is held by their banks with TPPs.

In Australia, the Competition and Consumer (Consumer Data Right) Rules 2020 outline the rules of data portability for the CDR and its participants, while in Brazil data portability, credit portability and payroll portability have been established by law since 2006.

Reforms are underway in other OECD countries to promote such data portability. In Switzerland, the revised data protection regulation will enter into force in 2023; a right to data portability has been introduced in this new framework. Similarly, in Canada, the government has tabled proposed legislation in the Parliament of Canada related to data portability.[4]

In the case of the US, there are no specific federal regulations regarding data portability. Section 1 033 of the Dodd-Frank Act only states that "information shall be made available in an electronic form usable by consumers." At the state level, CCPA stipulates that information requested for disclosure must be in a usable format allowing for easy transmittal "without hindrance." VCDPA has similar language. In Korea, data portability is stipulated in laws other than open banking (Credit Information Act).

Last, in some countries the financial services authorities have no jurisdiction over data portability in general. This is the case in Japan for the JFSA, as well as in Hong Kong China, where the relevant authority is the Office of the Privacy Commissioner for Personal Data (PCPD).

1.4. Attribution of liability and accountability

Data sharing arrangements incorporate liability provisions in order to provide legal clarity on who is accountable when issues arise with respect to data access, data quality, data privacy and confidentiality, processing, sharing, and storage of data as well as cyber security breaches. Attribution of liability is a complex matter that is often resolved on a case-by-case basis given the different authorities involved; the fact that any provisions of data sharing arrangements need to be consistent with existing data protection regimes and possible contractual arrangements that may be used for data sharing, depending on the case.

[4] See section 123 of the proposed Consumer Privacy and Protection Act (https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading). The Province of Québec has similar data mobility provisions included in its privacy legislation (http://www.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html).

The way liability is attributed in OECD country data sharing arrangements varies. In Switzerland, the liability depends on the different co-operation models that can be used. For example, if based on outsourcing, it is usually the bank (or another financial institution granting access to data) that is held liable. If the services are based on a platform or a common offer, it usually depends on the contractual arrangements. In the US, liability for consumer data privacy and protection is generally addressed through the Gramm Leach Bliley Act requirements (GLBA). Regulation P, implementing the GLBA, notes that "The regulation establishes rules governing duties of a financial institution to provide particular notices and limitations on its disclosure of non-public personal information".[5] In Brazil, all regulated and licensed institutions (all participating institutions are licensed) are accountable for those issues and have to comply with regulations on those topics. In Korea, the financial company or company that is facing an issue is responsible, and the consumer protection department of each financial company or company is responsible for handling and correcting customer complaints.

In the EU, these provisions should be consistent with GDPR and should also include specifications on redress and dispute resolution as well as consent mechanisms for consent beyond the usage of the data controller. In addition to the Open Finance Framework setting out liability provisions, it should also support and enable contractual agreements as these are crucial to fill any gaps in new use cases, or specialised scenarios which may require additional clarity on the legal, technical and other conditions governing data sharing.

Under the UK Open Banking framework, account providers and open banking firms need to be aware of their obligations under the PSRs 2017 relating to user information, under other applicable data protection law such as the Data Protection Act 2018, as well as under the General Data Protection Regulation (the GDPR). In addition, the firms must comply with regulatory requirements, including conduct, security and operational requirements as described in detailed under the FCA's Strong Customer Authentication and Common and Secure Methods of Communication (SCA-RTS). Conditions of authorisation include a requirement for payment service providers (PSPs) to have a data security policy including a detailed risk assessment, and security control and risk mitigation measures.[6]

In terms of settlement of liability and associated compensation, there are examples where compensation can be sought. In the UK, where an unauthorised, non-executed or defectively executed transaction is initiated through a PISP, it is the ASPSP's responsibility to provide a refund.[7] If the PISP is liable, the ASPSP can then seek compensation from the PISP which must, on request, provide that compensation immediately.[8] The amount of compensation should cover the full amount which the ASPSP was required to refund to the customer. However, PSPs may put in place voluntary arrangements for the settlement of such liabilities between themselves. Where an ASPSP has been required to compensate the customer for an unauthorised transaction, but that liability is attributable to an AISP, the ASPSP may exercise its right of recourse to seek compensation from the AISP. [9]

Liability-related provisions need to also include framework for complaint handling and redress and dispute resolution mechanisms. In terms of complaints handling, in most cases customers can complain to either the data source entity (AISP) or the third-party service provider (TPP). In Mexico, financial institutions and

[5] Financial institutions are defined as, "any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities, as determined by section 4(k) of the Bank Holding Company Act of 1956. Financial institutions can include banks, securities brokers and dealers, insurance underwriters and agents, finance companies, mortgage bankers, and travel agents.

[6] Regulation 5(1) of the PSRs 2017 (as set out in paragraph 10 of Schedule 2 of the PSRs 2017).

[7] In line with regulation 76 and regulation 93 of the PSRs 2017 and FCA's Approach Document.

[8] Under regulation 76 or regulation 93 of the PSRs 2017.

[9] Idem.

authorised third parties that breach the data sharing requirements imposed on them by law or regulation become liable for such breach and may be penalised by the relevant financial authority. In these cases, financial authorities have the legal power to suspend the information sharing, produce observations, and impose corrective measures to ensure the integrity of the information and compliance with the legal and regulatory framework. Customers and affected third parties may inform the relevant financial authority about cases of violation by banks and other financial institutions, so that such authority can carry out its supervisory activities to confirm such violation and impose the respective penalties on them.

2 Data access provided to third party providers

2.1. Data access provided to third party providers

In the EU, payment account data of retail and business customers can be shared through licensed third-party service providers (AISP, PISP), provided that an additional customer consent has been already granted to the third-party service provider. According to PSD2, a registration from the national competent authority (NCA) of an EU Member State where the AISP is located is required in order to provide account information services.[10] There is a lighter licensing regime for AISPs compared to credit, electronic and payment institutions, as AISPs do not at any time hold funds, and are therefore not subject to particular prudential requirements.

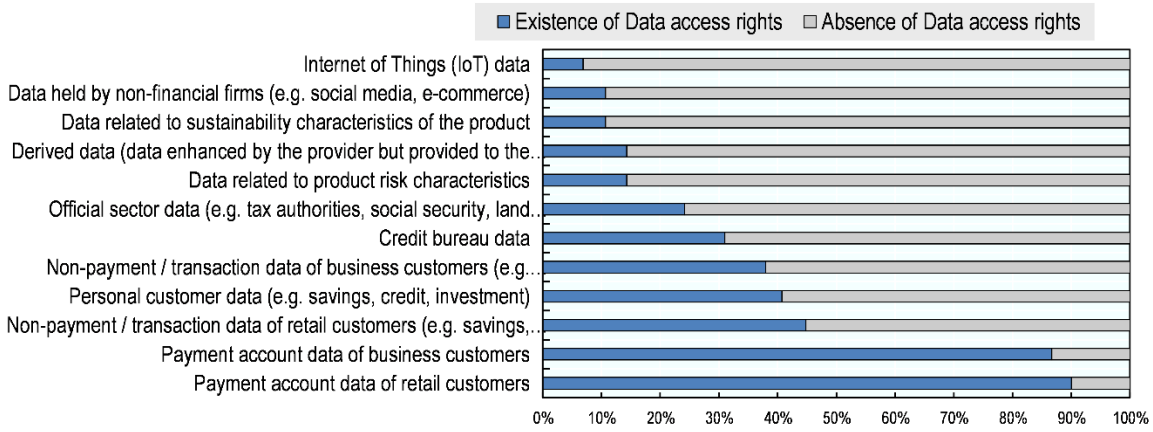
TPPs have data access rights to payment account data of retail and business consumers in most OECD countries, provided that there is customer consent. In the US, non-payment/ transaction data of retail and business customers are also allowed to be shared with TPPs, although generally have to be customer-permissioned. Brazil also allows access to non-payment data but only for regulated and licensed TPPs/FinTechs who can participate in Open Finance and have access to client data. However, unlicensed TPPs can also have access to customer data through bilateral contracts with participating institutions. In the EU, this kind of access can be provided outside the perimeter of PSD2, only after bilateral agreements between account servicing service providers and third-party service providers, provided a customer's consent has been already granted to the third-party service provider. The same holds for personal customer data.

PSD2 allows for TPPs to access the accounts of consumers in two ways if explicit consent is provided: (i) TPPs that use current account data and allow the customer to see them all in one place without having to log in to separate online banking profiles, and/or use transaction information from current accounts to provide a personalised recommendation on what current accounts offer customers the best price or the most relevant features; and (ii) TPPs that can initiate payments directly from the customer account, rather than paying with credit or debit card (also known as PISs).

In the UK, the requirement is different depending on the type of TPP: for AISPs, the FCA expects ASPSPs to make the same information available to a customer via an AISP as would be available to the customer if they accessed their account online directly with the ASPSP, provided this does not include sensitive payment data. For PISs, ASPSPs are required to treat the payment order in the same way, in particular in terms of timing, priority or charges, as a payment order initiated by the customer directly.

[10] Point (8) of Annex I to PSD2.

Figure 2.1. Types of data access rights provided to third party providers



Source: OECD Survey.

In the Czech Republic, although there is no legal claim, there are use cases of contractual arrangements that allow for data access to all types of data listed in the OECD survey (Figure 4.1).

When it comes to data held by non-financial firms (e.g. social media), in the US, this varies by firm. In the EU, the upcoming EU Digital Markets Act (DMA) would enable automated sharing of customer data held by gatekeeping platforms. DMA has been adopted by the European Council but has not yet entered into force. An interesting category is also the credit bureau data, with only seven OECD countries allowing access to such data.

Official sector data (e.g. tax, social security, land registry) are allowed for access only in 5 OECD countries, and in some of them it depends also on the source (e.g. US). In Lithuania, publicly available – open data – is non personal data and defined entities (e.g. financial institutions, notaries) are granted access to the official data required for their activities or to comply with the established requirements (e.g. under AML/CTF framework). A similar case for Open Data exists in Estonia.[11] In the Netherlands, proposals for a credit register are under discussion, which could in the future give third party providers access to corporate financial information that has been reported to tax authorities; while in Costa Rica, FinTechs and any type of institution or person can have access to land registry, but not within an open data framework (i.e. with APIs).

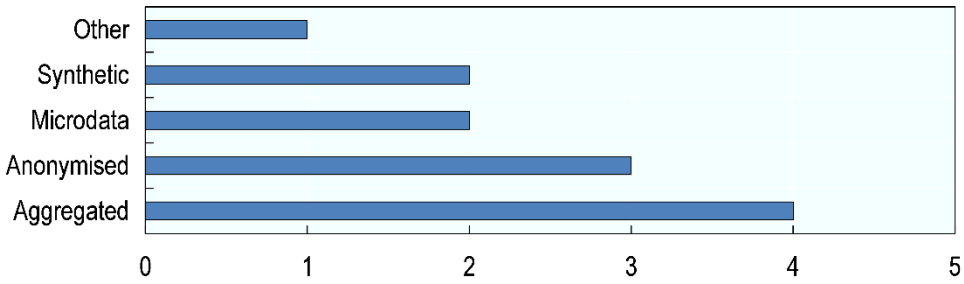
2.1.1. Public sector data and data sharing among institutions

Some countries are considering providing access to supervisory data for research and innovation purposes (e.g. Colombia, Greece, Italy, and Türkiye[12]). In Australia, the Data Availability and Transparency Act 2022 (DATA 2022) is the main channel for increasing access to government data in the Australian context. Under the consumer data right, consumer data is only permitted to be used for research purposes where an express consent is given by the consumer and the data is de-identified. In terms of types of data that this would include aggregated data, other anonymised datasets, and to a lesser extent micro data or synthetic data.

[11] https://www.rik.ee/en/open-data

[12] In the case of Türkiye, any data containing bank secret and/or customer secret is protected by the Article 73 of the Banking Law No.5411.

Figure 2.2. Potential sharing of supervisory data



Source: OECD Survey.

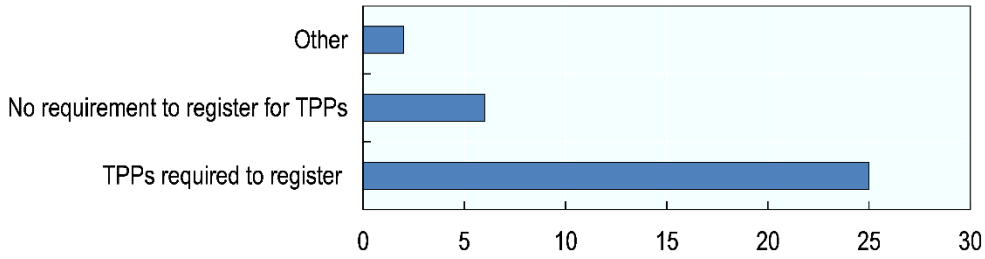
Additionally, a number of OECD countries are considering promoting data exchange among institutions to improve risk management and compliance. For example, in Estonia, data exchange is allowed between supervision authorities, central bank, Financial Intelligence Unit and Tax Board. In the UK, the FCA is considering promoting the sharing of fraud data between account providers to facilitate early detection and prevention of fraud cases. Similarly, in the US, while not broadly applicable or targeted at data sharing, Federal Banking Agencies have encouraged collaborative approaches to meeting certain requirements, such as the Interagency Statement on Sharing Bank Secrecy Act Resources. France is conducting an experimentation with some financial institutions to share data related to AML.

Such efforts are increasingly related to cyber-security risk management by Authorities. For example, in Italy, Banca D'Italia has sponsored information data sharing among Financial Institutions with reference to cybersecurity risks. Türkiye is considering the establishment of a cyber-security intelligence framework that would rely on such data sharing arrangements across institutions. Related, in Austria, there are numerous measures in place to improve risk monitoring and compliance in the payments sector, e.g. periodic reports of PSPs to the Oesterreichische Nationalbank (OeNB) with regard to fraud cases in relation to the different instruments of payment or the obligation for ASPSPs to inform the FMA instantly whenever they refuse TPPs the access to PSU accounts or decide not to share transaction data due to security concerns.

2.2. Rules and liabilities for data access

TPPs are required to register with the authorities and/or obtain a license in the vast majority of OECD countries. Canada, Colombia, Switzerland and the US are the exceptions. In Israel, non-regulated entities providing third party services need an Information Service Provider licence from the Securities Authority. In the UK, AISPs who access consumer data with their explicit consent and provides consolidated information on a payments account held by a payment service user need must be authorised (registered) by the FCA to get access. An agent of the AISP must be registered with the FCA by the principal (the regulated entity, i.e. the AISP). The Payment Services Regulation set out requirements for registration for account information service providers. Payment initiation service providers that access payment accounts on behalf of consumers must also be authorised by the FCA. In Australia, to be eligible to receive consumer data under the CDR framework, data recipients must be accredited by the Australian Competition and Consumer Commission (ACCC).

Figure 2.3. Registration/authorisation requirement for TPPs



Source: OECD Survey.

2.2.1. Data storage rules

Under PSD2, PISPs and AISPs are not permitted to use, access, or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer, in accordance with data protection rules. Moreover, the general provisions regarding technical and organisational measures to ensure a level of security appropriate to the risk of the GDPR also apply.

Some countries allow for storage with explicit consent, while they may require specific technical conditions in order to ensure security (e.g. encryption). For example, in the UK, the PSRs 2017 do not prohibit PISPs from using and storing the payment service user's account number and sort code for the purpose of providing a payment initiation service, with the customer's explicit consent. In order to safeguard the confidentiality and the integrity of data, Article 35 of the SCA-RTS seek to ensure the security of communication sessions between parties involved in open banking payment transactions. They require that secure encryption is applied between banks and open banking service providers when exchanging data. Data protection law, including the GDPR, may require a PSP to obtain a data subject's explicit consent (or satisfy another condition) to process any personal data classified as "sensitive personal data" under current data protection law or a "special category" under the GDPR. In Korea, third party providers must obtain consent from the user on the storage period, purpose and collection items for data storage, and sensitive information among stored personal information must be encrypted.

Specific technical requirements for storage systems may exist in some jurisdictions. For example, in the Czech Republic, the Czech Payment System Act stipulates the obligation (for the so-called payment account information administrator) to have in place and maintain a management and control system that includes strategic and operational management, risk management system, internal control system (managerial control, compliance, internal audit), conflict of interest management, control and security measures in processing and recording information. The management and control system must be effective, comprehensive and proportionate to the nature, scale and complexity of the risks associated with the administrator's business model and activities (principle of proportionality).

Other OECD countries have time-limits in terms of storage of data under data sharing frameworks. In Israel, service providers cannot retain the data more than three years and these need to be deleted after that time period. The data needs to be stored in a separate data storage than other data. Similarly, in Australia, data recipients must comply with information security controls, and consumer data must be deleted or de-identified where a consumer's consent is withdrawn or expires unless required to retain under Australian law. In Brazil, although there is no explicit time limit, access to consumer data is linked to a specific purpose and storage after completion is prohibited by data protection law, except for regulatory purposes or for studies by research bodies.

Other countries, such as Japan, require specific governance frameworks around such storage. In the case of Japan, electronic payment service providers must develop a policy, prepare organisational readiness, introduce in-house rules, and develop an internal control environment in order to appropriately manage

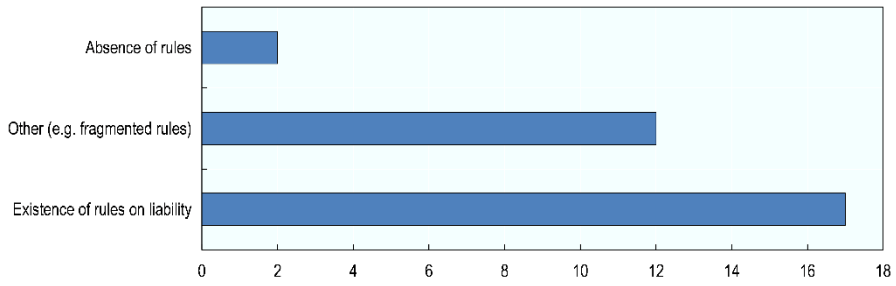
information assets, and regularly revises these policies, rules, and control environment in line with the relevant regulations and guidelines.

In the US, such activity must be conducted within the same expectations of supervised financial institutions. Under GBLA, third parties may receive non-public personal information (NPI) from a non-affiliated financial institution ("originating financial institution") under the section 14 (NPI transfer necessary for financial transactions) or 15 (NPI transfer necessary for fraud prevention) exceptions. In these situations, third parties may only disclose and use the information in the ordinary course of business to carry out the purpose for which it was received.

2.2.2. Liability attribution in case of incorrect, outdated or inappropriate data

In addition to the general provisions around liability in data sharing arrangements (Section 2.4), there is a question about liability attribution in case data shared is incorrect, outdated or otherwise inappropriate. As with standard liability, rules are fragmented across regulatory jurisdictions. In some cases, these fall under applicable data protection laws (e.g. GDPR), while in others they are subject to bilateral agreements between the AISP (e.g. bank) and the TPP (e.g. FinTech).

Figure 2.4. Rules on liability if data shared are incorrect, outdated or otherwise inappropriate



Source: OECD Survey.

2.2.3. Compensation for data access

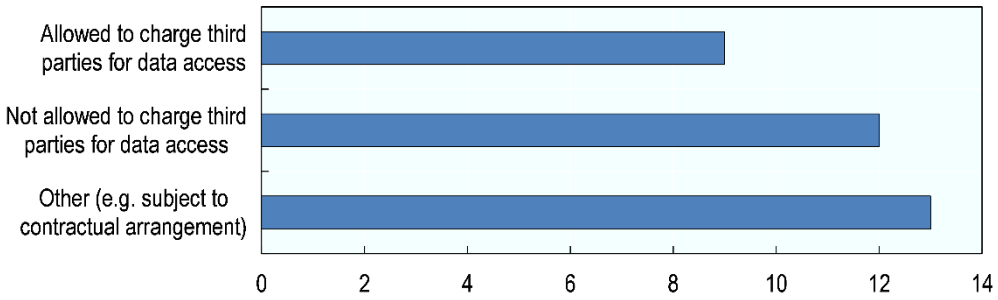
Compensation for data access is another key issue that relates to the motivation by banks and other ASPSPs to open up their data to third party service providers and the cost associated with such access provision. Compensation terms may differ even within the same framework, as is the case in Korea: There are differences depending on the data infrastructure and data type provided by the financial company. In some cases, it is provided free of charge according to the law, and in some cases, it is set at the level of 2-10 Korean Won per case by agreement between financial companies.

In the EU context, PSD2 prescribes that ASPSPs offering payment accounts that are accessible online for their PSUs, must allow TPPs to provide PIS or AIS to those PSUs without compensation. Banks may not require contracts with – no charge – the third-party service provider in order to have account-access. However, the European Payment Council (EPC) is now working on a SEPA Payment Account Access (SPAA) that also takes into account that ASPSPs are able to provide innovative 'premium' solutions (e.g. services that go beyond the PSD2 legal baseline) to TPPs, which can be charged. In that sense, other data access, beyond payment account data sharing is based on contractual arrangements.

Contractual arrangements are defining the terms and possible fees for data sharing arrangements in a number of OECD and non-OECD countries outside the EU. In Japan, fees are determined by the contract between the bank and the electronic payment service provider. In Hong Kong China, fees are subject to

bilateral arrangements. In other countries, however, as in the case of Chile and Brazil, any fees are prohibited.

Figure 2.5. Charging third parties for data access



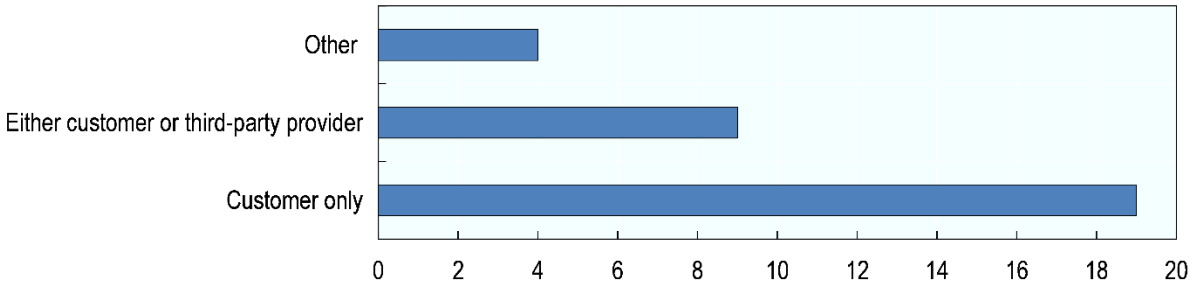
Source: OECD Survey.

2.3. Consent for data request

Initiation of data requests and associated customer consent is another very important feature of data sharing arrangements that helps inter alia safeguard customer data and their privacy, while it also has operational implications for data providers. In most OECD countries, only the customer can initiate a data access request. Data access request can only be initiated with customer's explicit consent in the UK and Japan, for example. In other countries, such as Switzerland and Mexico, there are no specific rules, and the general legal framework applies. In the Czech Republic, anyone can initiate a data access request to the Open Data portal.

In some countries, such as Brazil, Colombia, Germany and South Africa, data access request may be initiated by the customer or the third-party provider. However, the prerequisite is always the customer's consent. Similarly, in the US, while not exclusive to customer-only, most firms generally require customer-permissioned access. In Australia accredited data recipients initiate the data access request on behalf of a consumer if the consumer provided their expressed consent for the data recipient to collect their data.

Figure 2.6. Initiation of data access request



Source: OECD Survey.

When it comes to consumer consent, the vast majority of OECD countries require explicit consumer consent ahead of any data sharing, and in the majority of countries such consent needs to be renewed periodically. In the EU, According to PSD2, PSPs must perform Strong Customer Authentication (SCA) each time a payment service user (PSU) accesses her payment account online directly or via an AISP.

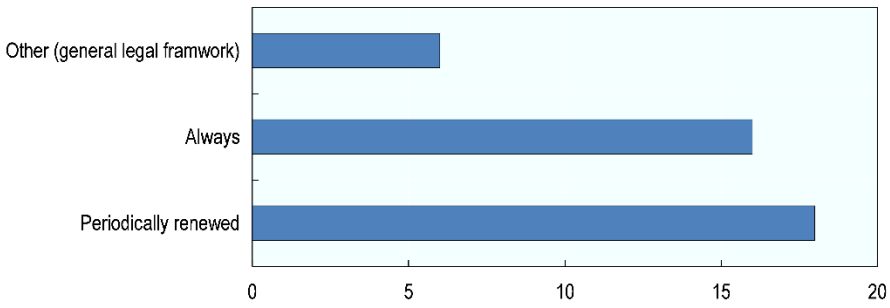
SCA ensures that electronic payments are performed with multi-factor authentication, to increase the security of electronic payments. By way of derogation from this requirement, the regulatory technical standards of the European Banking Authority (EBA) for SCA allow PSPs an exemption from SCA, under some special conditions: (i) access is limited only to the balance of the account and/or the recent transaction history; (ii) no sensitive payment data are disclosed, and (iii) SCA is applied when the information is accessed for the first time and at least every 90 days after that. This exemption was introduced by the EBA when drafting the RTS in 2016 because, without it, SCA for each individual access would have undermined the economic viability of AISPs, which PSD2 was explicitly intended to promote. It should be noted that such exceptions, as well as all other exceptions to SCA in the technical standards, have been interpreted by the EBA as voluntary. In Korea, all data opening and access is based on the customer's express consent, and consent has an expiration date in accordance with applicable laws. Therefore, if the validity period agreed by the customer expires, it must be renewed periodically.

Importantly, customers can withdraw their consent in all different jurisdictions. The mechanism for such withdrawal depends on the specific country framework, or on the general legal framework covering data sharing, depending on the country. For example, in the EU, consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability in accordance with Article 80 of PSD2. Consumers withdraw consent via the third-party provider (e.g. France), electronically (e.g. Hungary) or through the credit institution direct interfaces and/or directly through the third-party provider (e.g. Latvia).

Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorised. In the US, this is generally done through a request to the technology service provider.

Integrated systems providing data around consent status information and providing the interface for withdrawal have been developed in some OECD countries. In Korea, consumers can revoke consent to data sharing through third-party applications or financial institutions providing the data. Interestingly, Korea also provides an integrated system that allows separate data consent status confirmation and withdrawal, so that consumers can withdraw directly from there.

Figure 2.7. Required request for consumer consent for data sharing



Source: OECD Survey.

The time lag for period renewal of consent differs between OECD countries. In Australia, the CDR consumer can choose the period of consumer consent (as appropriate), and 12 months is the maximum ADR can provide. In Israel, the customer can give her consent for up to a three-year period. In Japan, even in the case where the electronic payment service provider has obtained consent for the provision of personal information to a third party from an individual user in the past, if the third party to which the information is provided or the content of information to be provided is different from the past case or if the scope of provision of such information exceeds the necessary extent to achieve the purpose of utilisation

specified before, the electronic payment service provider has to obtain consent from such individual user again. In other countries, such as Switzerland and the US, there are no specific open finance rules, and the general legal framework applies, so this may vary depending on the firm.

In the case of the UK, the FCA published in 2021 a Policy Statement (PS21/19) "Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach", where it introduced several changes to the SCA-RTS. This includes the creation of a new exemption to strong customer authentication (SCA) for when customers access account information through a TPP. Where an ASPSP adopts the exemption, their customers will not need to re-authenticate when they access their account information through a TPP. Instead, TPPs will be required to obtain explicit consent from customers at least every 90 days. TPPs must not access information without the customer actively requesting it unless the customer has reconfirmed their consent within the previous 90 days.

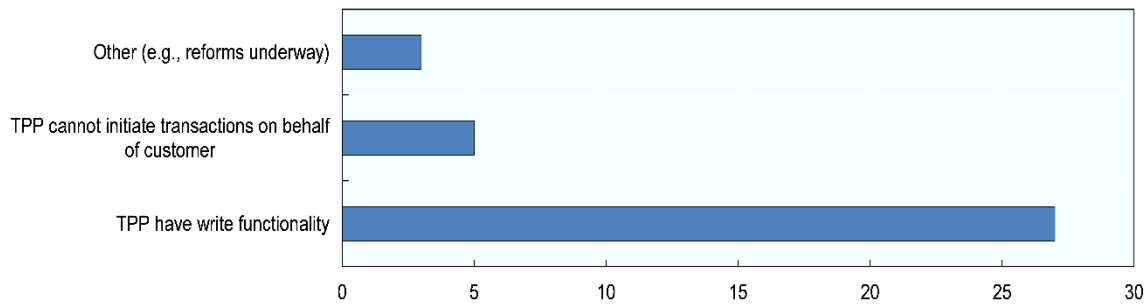
Consumer consent may involve part of a customer's data set. For example, under the UK framework, AISPs must have in place suitable and effective mechanisms to prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the user's explicit consent.[13] This means that where a customer only provides explicit consent to the AISP for a sub-set of their account data to be accessed (e.g. their current account but not their credit card account), only this should be accessed by the AISP.

TPPs have the right to perform actions on behalf of the customer in relation to data sharing (e.g. initiate transactions) in the majority of OECD countries. In the EU, such 'write functionality' is provided for in the EU PSD2 which prescribes that ASPSPs that are accessible online for their payment services users (PSUs), must allow TPPs to provide Payment Initiation Services (PIS) or Account Information Services (AIS) (e.g. PSD2 payment services 7 and 8) to those PSUs. In the UK, Account providers are required to provide authorised PISPs access to perform payment initiation services under the PSRs.

Consumer consent, discussed above, remains a requirement. For example, write functionalities are allowed in Japan only when instructed by the customer. In Brazil, such functionalities apply to the payment initiation service, while it should be highlighted that only licensed and regulated TPP can initiate transactions in Brazil.

Reforms are underway in Australia, where currently the CDR is a data sharing framework that provides accredited entities with 'read' access of CDR data. The Australian Government is currently progressing third-party action initiation reforms, with payment initiation expected to be the first action type in the CDR.

Figure 2.8. Third party provider's right to perform on behalf of customer



Source: OECD Survey.

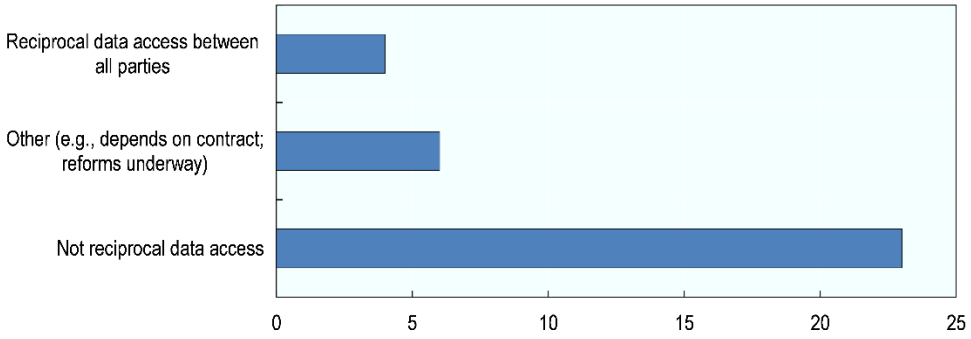
[13] Under SCA-RTS Article 36(3).

2.3.1. Reciprocal access to data

Another important issue that relates to bank incentives around data sharing has to do with reciprocal access to customer data between all parties under data sharing frameworks. Only Germany, Türkiye and Brazil were noted to allow for reciprocal data access between all parties involved in data sharing arrangements. In Ireland, whereas the right to personal data portability under GDPR has a cross-sectoral scope, data sharing under PSD2 is limited to payment account data (for business and retail customers).

In some cases, reciprocity depends on the financial institution and the technology service provider relationship (e.g. in the US) and on the contractual relationship between relevant parties (e.g. Japan). In the case of Australia, only data holders within designated classes are required to share data. However, if a party becomes accredited and they offer a product that is equivalent to a product that the designed data holders must provide, then they also become a data holder for that product. Countries in the process of developing specific frameworks for data sharing, such as Canada and Chile, plan to include reciprocal data sharing in those frameworks. In the case of Canada, this will require accredited participants to enable consumer permissioned-data mobility requests.

Figure 2.9. Reciprocal access to customer data between all parties under data sharing frameworks



Source: OECD Survey.

3 Operational and technical specifications

3.1. Rules around APIs

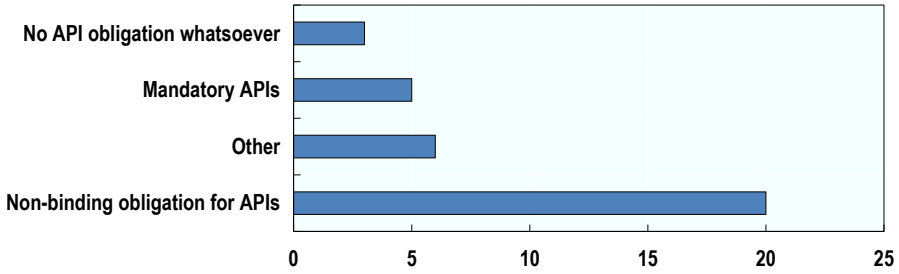
Open finance APIs allow third party providers to access consumers' transaction data without the consumers having to share usernames and passwords and eliminate the technical burden of screen scraping. Direct connections replace credentials with tokens, delivering higher levels of security, faster speeds, and higher connection success rates.

Five countries in the OECD survey reported having APIs as a mandatory obligation for banks and other financial institutions under data sharing frameworks (e.g. Australia, Brazil). In the case of the UK, the CMA order has imposed a binding obligation on the nine largest banks to implement and maintain specified read and write access APIs. Other banks are subject to more general access requirements under the PSRs which do not mandate APIs, although the FCA mandate the use of dedicated interfaces (which are typically APIs) for certain payment accounts. In practice many of these other UK banks use the Open Banking APIs as the de-facto industry standard, while in Israel open banking is based on NextGenPSD2 standards.

In the EU context, PSD2 prescribes that ASPSPs that are accessible online for their PSUs, must allow TPPs to provide PIS or AIS to those PSUs. This access should be realised via either (i) the consumer interface of the ASPSP; or (ii) via a dedicated API-based interface, offered by the ASPSP to TPPs. in implementing such interfaces, PSPs have two options i) modified e/m-banking services (TPP can access the user account via the normal user interface), ii) dedicated interfaces only for TPPs access. The majority of EU PSPs opted for the second option, based on API technical standards. Similarly, in Türkiye, APIs are neither the sole nor the mandatory way for open banking service provision; web services and file transfer protocols are alternative methods to APIs according to on Information Systems and Electronic Banking Services of Banks Regulation enforced by the Banking Regulation and Supervision Agency.

Switzerland has a recommendation to use certain API standards. Similarly, in the US, the CFPB has promulgated a list of principles to guide consumer protection but there is no binding obligation about the use of any technological means. The technology neutral principle in financial regulation across most OECD countries does not allow for the prescription of concrete technical specifications, and this was also the case in PSD2 in the EU.

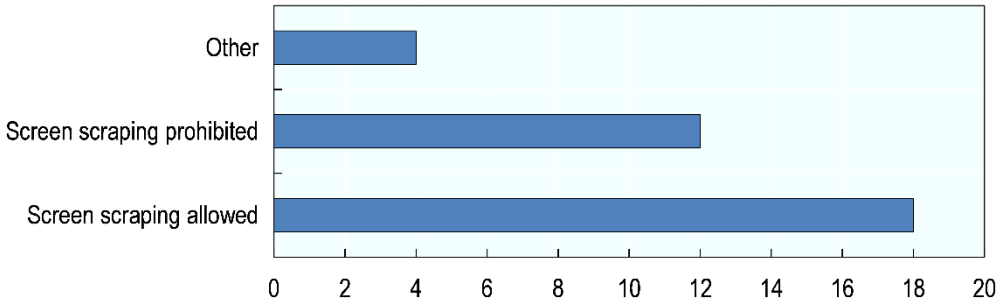
Figure 3.1. Existence of APIs as a mandatory or non-binding obligation for banks and/or other financial institutions



Source: OECD Survey.

In the absence of APIs, screen scraping, or credential sharing are the alternative solutions for data access and sharing. These require customers to share their credentials with TPPs to gain access to their data. Screen scraping, in particular, is considered to be a less secure way to access data than more modern connectivity solutions like APIs, with diverging associated customer experiences. In a July 2018 report, the US Treasury Department noted the significant security risks and liability burdens of screen scraping and the potential for APIs to provide a more secure method of accessing consumer financial data.

Figure 3.2. Screen scraping still practiced



Source: OECD Survey.

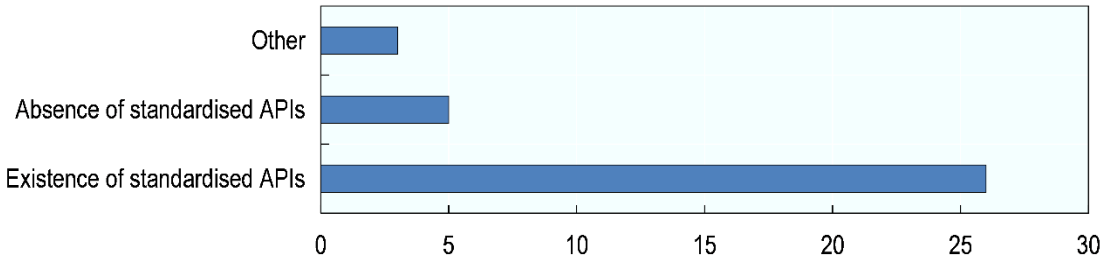
In the EU, there is currently no single pan-European PSD2 or Open Banking API standard. PSD2 and the regulatory technical standards (RTS) prescribe principles for PSD2 APIs, stating that the same data must be shared via the API as via the consumer interface and also what authentication functionalities must be available via the API. The RTS also contain various technical specifications, such as when an API is "down", but no technical standard has been set for APIs (it remains a reasonably open standard). Instead, several industry initiatives have been undertaken in terms of standardisation of APIs. However, even in the absence of specific technical standards in the regulation, secondary regulation in some countries, such as Austria, forbids ASPSPs to make the customer journey more burdensome for users of PIS than for their own PSU (Del. Regulation 2018/389).

Indeed, standardised APIs exist in most OECD countries, although these are industry-led. Industry associations co-ordinate the standardisation of APIs in many countries and/or regions. Examples of such standards include the Berlin Group standards (https://www.berlin-group.org/), STET standards (https://www.stet.eu/) or national standards (e.g. Czech or Polish API standards). In the UK, The UK Open Banking Implementation Entity (OBIE) sets the standards. The OBIE is an independent body with accountability to the CMA tasked with agreeing, maintaining and overseeing the roll out of Open Banking

standards across the UK.[14] The UK is currently working on a transition to a future entity to manage the Open Banking standards and further develop the ecosystem, which will have a different long-term funding and governance model.

In the US, API standards are generally provided by private standard-setting bodies such as the Financial Data Exchange (FDX) which align a cross section of financial institutions, FinTechs, large technology companies, and card networks around common data-sharing standards. In Australia, in the context of the CDR, data standards, including standardised APIs, are developed by the Data Standards Body to be made by the Data Standards Chair. In Brazil, in the Open Finance ecosystem, the BCB establishes the main guidelines for the APIs standardisation. Based on these guidelines, technical requirements have been set by the governance structure and submitted to the BCB, who has ultimately incorporated them in the regulatory framework that must be observed by all participants.

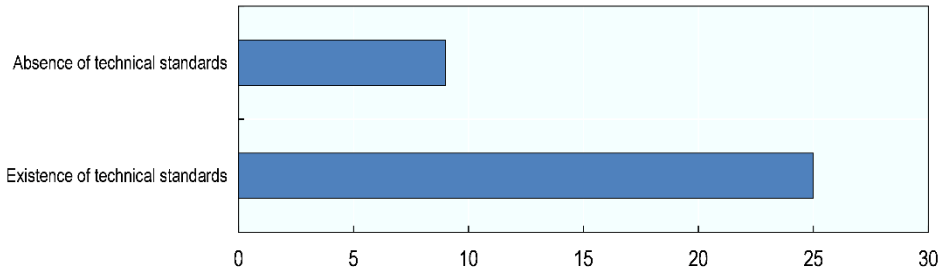
Figure 3.3. Existence of standardised APIs in the domestic market



Source: OECD Survey.

Technical standards associated with data sharing interfaces also exist in most OECD countries. In EU member states, the Regulatory Technical Standards concerning access to accounts and third-party providers under PSD2 are developed by the EBA. In some countries (e.g. Türkiye) the Central Bank is the one setting the standards, although this is still not operational and is at the implementation stage. In Australia, in the CDR, the Data Standards Chair is informed by the Data Standards Body which is part of the Australian Treasury. In Canada, industry-led efforts to facilitate connections between banks and FinTechs are ongoing and some of the larger banks have begun announcing partnerships with major data aggregators. The Department of Finance Canada, which is in the process of implementing an open banking framework, is considering such standards.

Figure 3.4. Existence of technical standards for data sharing interfaces/ connections between banks and FinTech companies



Source: OECD Survey.

[14] The CMA nine banks were directed to create and fund the OBIE by the CMA Order.

The diversity of APIs, despite industry-led standards, renders market access, from a technical perspective, somehow cumbersome and costly for providers of AIS and PIS, as service providers have to deal with a relatively large diversity in the dedicated interfaces / APIs offered by ASPSPs (mostly banks) for accessing payment accounts (and associated IT costs) in the absence of concrete technical specifications prescribed by regulation. Certain service providers ("API aggregators" or "API hubs") have responded by offering aggregation services. Aggregation services (API aggregators or API Hubs) are also emerging in response to the different options for the design of these interfaces available in the market.

3.1.1. The discussion around standardisation

Making an API the legally mandatory standard of a country would not be in line with the principle of technology and business model neutrality, which is a cornerstone of financial services regulation across most OECD economies. However, it cannot be denied that implementing a mandatory and uniform API standard could foster the user-friendliness of customer journeys and improve technical compatibility, as well as reduce costs associated with data access by FinTech start-ups. Increased standardisation can also promote a level playing field and further encourage innovation and FinTech creation. It may also address in some part the lack of incentives by ASPSPs to provide access to their customer data, *inter alia* for cost and competition reasons.

Standardised APIs, whose development would be industry-led but with a mechanism for the NCAs to potentially provide guidance and steer in its development, could contribute to a clearer legal framework to be complied with by the industry. The lack of standardisation of API standards has some unintended consequences, which are exacerbated by the strongly diverging interests between market participants in the Open Finance ecosystem and the lack of incentives by ASPSPs (mainly banks) to provide access to TPPs. It also has cost implications both for ASPSPs and TPPs, both in terms of time and investment in technology, leading to sub-optimal results for the overall system.

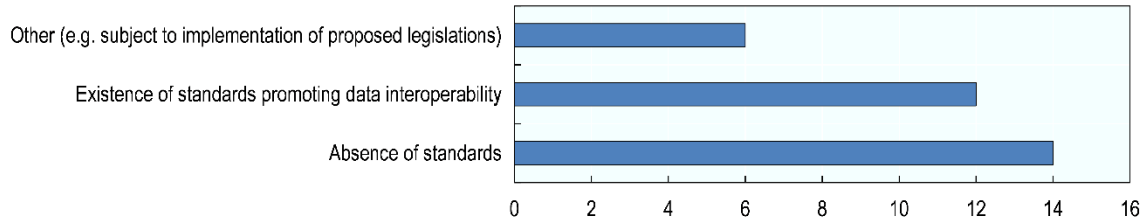
Also, in the absence of standardisation, extra layers of intermediation are emerging in the API space with the emergence of API aggregators. The emergence of such players who are in effect standardising the variety of APIs for the third-party provider who does not have the capacity to interact with all different models and can be regarded as a sub-optimal solution given additional costs introduced to the process of data access.

Even at the regional space, such as the EU for example, and in spite of an increased level of harmonisation given the existence of technical space, a possible future convergence of API standards could be seen as a positive evolution of the existing framework. The current legal review of PSD2 by the European Commission offers a good opportunity for such consideration.

3.1.2. Data interoperability

There are currently limited examples of the existence of other standards promoting or ensuring data interoperability in OECD countries, over and above the API standards mentioned above. Initiatives are, however, being planned in some OECD economies, such as the UK, where the proposed smart data legislation would encourage smart data schemes to be interoperable with other open data initiatives in the UK. In other countries, such standards for data interoperability exist but outside the financial services space or in specific parts of the financial services sector, such as card payment networks. For example, standards apply only for specific cases of network operations, mainly on card payments. Standards on data interoperability apply only in cases of mandatory interoperability by financial institutions contemplated by law, mainly on network operation such as those relating to card payments.

Figure 3.5. Existence of standards promoting data interoperability



Source: OECD Survey.

3.1.3. Portable digital identity in data sharing initiative

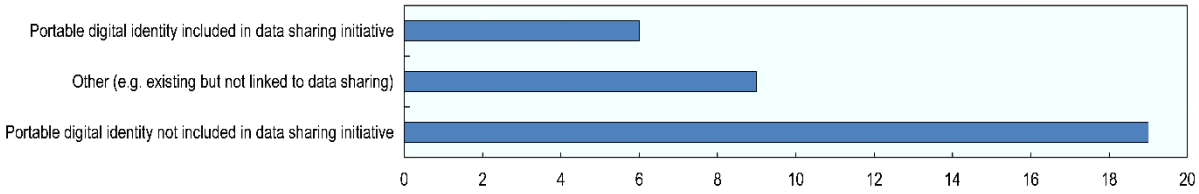
The link between data access and Digital Identity is indispensable for the successful implementation of comprehensive Open Finance frameworks. Identity underpins the entire financial system, and poor identity infrastructure opens the path for bad actors exposing consumers and businesses to important risks. Implementation of such frameworks is currently predicated on the data holder (primarily on banks) on identifying and verifying the individual requesting a transaction before the data is released.

PSD2 introduced the requirement for the entities holding accessible payment accounts to apply SCA in the following instances: (a) each time a payment service user (PSU) accesses its payment account online; (b) initiates an electronic payment transaction, and (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. The existence of portable ID could significantly alleviate such processes. The regulatory technical standards (RTS) issued by the EBA specify, amongst others, the requirements of SCA and the exemptions to SCA. These RTS try to strike a balance between the security of payment services and the promotion of user-friendly services for the consumer.

Efforts are underway in many parts of the world to address portable digital IDs. At the national level, the Czech Republic, Estonia and Finland have made progress. Bank-IDs are another method for performing electronic identification in some OECD countries, for instance, in public sector e-services. At the regional level, in the EU, EIDAS 2.0 is being pursued to that end.

Efforts are also underway by private sector participants, although any ID that is issued outside of government-issued credentials gives rise to additional risks.

Figure 3.6. Inclusion of portable digital identity in data sharing initiative



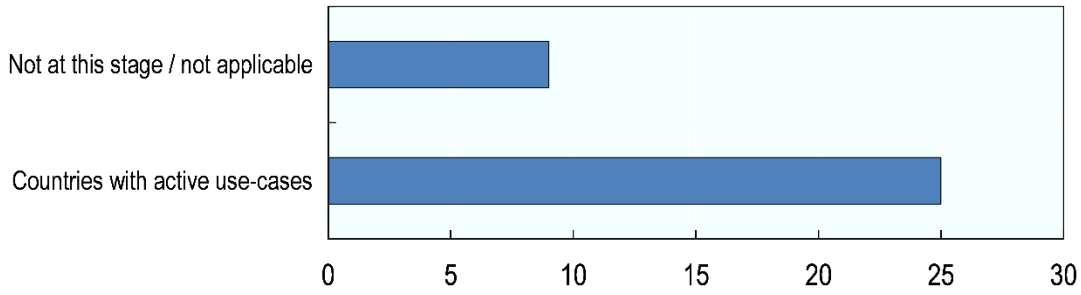
Source: OECD Survey.

4 Learnings from existing frameworks

4.1. Main use-cases emerging as a result of data sharing frameworks

The establishment of the open banking and other data sharing frameworks have contributed to the emergence of various active use-cases in a variety of areas within the financial services space. These are found primarily in the payment space, with payment account information services by AISPs, payment initiation services by PISPs, and aggregation services. Other services based on innovative business models emerging on the basis of such frameworks include credit scoring applications, debt management tools, wealth management applications, alternative payment services, product comparison, account verification and balance checks by third parties and other. Twenty-five out of 34 countries have reported active use cases resulting from the Open Banking and other data sharing frameworks in their jurisdictions, with the remaining respondents in countries where frameworks exist reporting that they have not yet analysed this development at this stage. In some countries, the data sharing framework is only allowing for certain defined use-cases. For example, in Mexico, the Open Finance framework has been recently implemented only in regard to general aggregated information on products and activities by financial firms.

Figure 4.1. Countries with active use-cases



Source: OECD Survey.

Account information services are the most widely observed service resulting from data sharing frameworks (e.g. Germany, Greece, Lithuania, Luxembourg, the Netherlands and Spain). In the Netherlands, various banks offer their own payment account information services to give their own payment account holders the opportunity to obtain a total overview in the online banking environment of the payment accounts held at other banks as well.

As part of AISP, some countries reported payment aggregation services by the Open Banking framework, allowing customers to see all their banking products from different providers in one interface (e.g. Australia, Estonia, Japan, Italy and Brazil). For example, Italy has account data aggregation services active for retail and corporate, and in Estonia account aggregation is offered by banks acting as third-party providers, to allow customers to aggregate payment account data from different banks. Account aggregation in Australia is allowing the customers to see all of their banking products from different providers in one interface. Other account services include cloud-based accounting services in Japan. In Italy, the account data is used for corporate customers to support financial scheduling, to set instalment plans, and for invoice reconciliation.

The second dominating use-case is the Payment Initiation Service Provision (PISP) (e.g. Estonia, Greece, Lithuania, Luxembourg, the Netherlands, and Brazil). Italy has used the account data for simplifying the initiation of user payment transactions. In the Netherlands, it is used as initiating payments by businesses. Although the main use-cases will be clear over time, payment initiation has been one of the main application areas of Open Finance framework in Brazil.

The PISP is expanding the scope of payments by the customers by providing alternative payment methods. For example, payment initiation service is used as an alternative to card payments to serve customer e-commerce payments in Lithuania, as well as Spain providing alternative payment methods in stores by payment initiation service. Buy Now Pay Later (BNPL) is serving as an alternative payment method in Greece. In the UK, Open Banking has expanded the payment choices. For example, since 2021, UK taxpayers have been able to pay their self-assessment tax returns to HMRC using Open Banking account-to-account payments as an alternative to a credit card scheme, and over GBP 4 bn in payments have been transacted in this way at the date of writing of this report. In the Czech Republic, the Open Banking framework has been used by payment institutions and FinTechs benefit from this framework to build innovative business models.

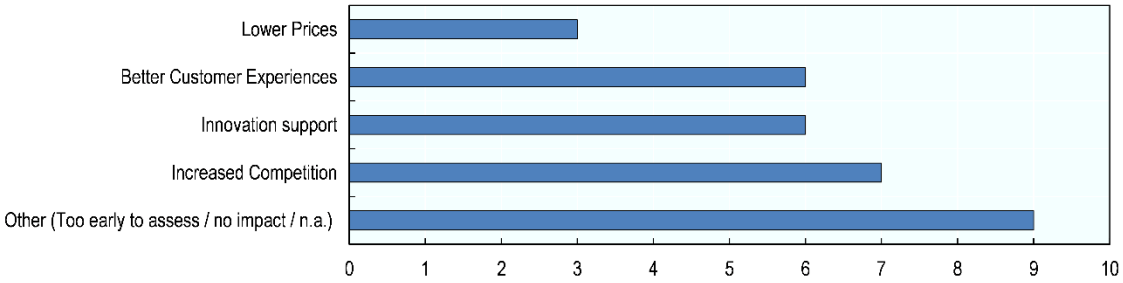
Credit Scoring Services are increasingly being provided on the basis of account data accessed through data sharing arrangements for the assessment of creditworthiness (e.g. Germany, Greece, Italy, Lithuania, Spain and Brazil). Debt management services are active in the Netherlands and Australia. These include online services offering an overview of the current paid subscriptions, provide tips for saving and switching and/or to help customers budget in order to avoid debts, followed by collaboration with municipal debt assistance in some cases. Financial Management is also serving as a main use-case for several countries. In Greece, the Open Banking framework is used for Personal Financial Management (PFM), while Italy and Brazil are using both Personal and Business Financial Management (BFM). In Switzerland, wealth management applications have emerged on this basis. Other, more niche, use-cases include customer acquisition tools (Hong Kong China) and customer on-boarding (Brazil), as well as assisting customer transactions by topping up digital wallet and analysis of expenditures (Slovenia).

In Australia, the CDR has also provided the basis for a variety of use cases including providers using consumer and product data, with consent, to get a deeper understanding of consumers' financial situation to help them reduce their debt faster. Other niche use cases in Australia have emerged responding to particular needs, such as using credit card transaction data to help consumers trace their movements and then alert them to COVID-19 exposure sites they may have visited. Other reported active use cases in Australia include services that help smooth and expedite the application and switching of loans by transferring and prefilling data used by brokers and/or lenders. Further use cases are emerging to help consumers calculate their carbon footprint and suggest alterative 'greener' purchasing options.

4.2. Impact of data sharing frameworks on customers and financial services

Data sharing frameworks in place are reported to have been producing positive impacts on customers and financial services, fostering innovation, increasing competition, lowering costs, and delivering better customer experiences. Twenty-one out of 33 countries responding to the OECD Survey have reported positive effects by Open Banking frameworks to customers and financial services, whereas the rest of the countries with data sharing arrangements in place responded that it is too early to analyse the effects at this stage.

Figure 4.2. Impacts of data sharing arrangements on customers and the market for financial services



Source: OECD Survey.

The main effect of Open Banking and other data sharing frameworks to the market for financial services has been the fostering of innovation. In Japan, the number of banks allowing access to FinTech companies through APIs has significantly increased since the amendment of Banking Law in 2018, which encouraged the development of novel financial services by electronic payment service providers such as account aggregation services. In the Netherlands, PSD2 encouraged providers to offer existing services in a different way, while in Lithuania the breadth of services offered to customers due to new services available on the basis of data access.

Open Finance is expected by OECD countries to stimulate competition by de-monopolising data and improving information availability, while also encouraging the emergence of cheaper and better financial products for consumers. Another important effect reported by OECD countries relates to increased competition in the market for financial services, observed for example in Estonia, Germany, Lithuania, and the Netherlands.[15] For example, although accounting packages already existed in the Netherlands prior to the implementation of PSD2, competition between providers in this market has increased since its implementation. The case is similar for Estonia and Lithuania, where Open Banking led to greater competition and choice in e-commerce payment solutions. Nevertheless, many OECD countries expect the largest impact to be observed in the future.

Lower prices are another important impact to the customers and financial services, which is observed in Estonia Lithuania, the UK, and Brazil. The merchant fees in Estonia and the merchant paid fees in Lithuania for collecting e-commerce and bill payments have decreased. Brazil has reported lower interest rates and fees; however, further analysis is needed to establish Open Finance's contribution in this regard. For UK, as a leading nation with extensive use of Open Banking and data sharing framework, found out that customers find Open Banking services easy to set up and significant proportions of customers claim that these platforms are helping them keep to budgets, reduce unnecessary expenditure, shop around and minimise fees and charges.

Especially in the UK, more than 6 million consumers are benefitting from open banking-enabled products and services, including 660 000 small and medium enterprises (SMEs) (data as of June 2022). It is estimated that open banking-enabled services will create potential benefits of GBP 12 bn for consumers and GBP 6 bn for small businesses. In March 2022, it was estimated that 10-11% of digitally enabled consumers and small businesses used Open Banking, which was a 6-7% increase from March 2021. Business penetration (11%) is slightly higher than retail (10%), but the gap between the two has closed significantly since 2021. In the six months to March 2022, there were 21.1 million Open Banking payments,

[15] And Brazil from non-OECD countries.

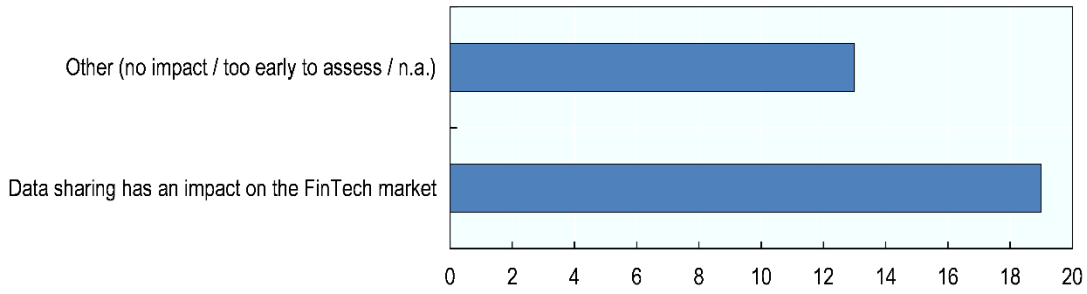
compared to 6.1 million in the same period the prior year, signifying that the month-on-month growth is running at around 10%.

Other beneficial impacts of Open Finance reported include better customer experiences for countries including Estonia, the UK and Brazil. In Brazil, Open Finance is expected to contribute to create new business models and reach customers that were previously unassisted, underserved, or that expected a better customer experience including merchants. In Estonia, the framework is granting more convenience for customers due to the aggregated account view. UK is providing its customers with services to save more and build financial cushion. The last example reported is the enhanced credit risk assessment observed in Brazil due to the improved information availability.

4.2.1. Impact of data sharing frameworks on FinTechs in terms of growth and diversity

The impact of Open Banking and other data sharing frameworks on the FinTech industry can be observed in regard to growth and diversity of companies active. Nineteen out of 32 countries responded that there has been an impact of such frameworks on their FinTech industry, whereas the rest of respondents with such frameworks in place responded that it is too early to examine the effects. However, in some of the cases of countries reporting impact on their FinTech market, it is still too early to define and assess such impact (e.g. Israel, Spain), and in some cases the impact is so far negligible in terms of size (Israel, Greece). In Mexico, no such effect has been observed excluding so far information on customer transactions.

Figure 4.3. Impact of data sharing arrangements on the FinTech market



Source: OECD Survey.

The most significant impact of Open Finance-related arrangements for the FinTech market is the introduction of new entrants and the creation of FinTech firms with new business models. It is estimated that more than 400 non-bank providers have been created since the introduction of the PSD2 in the EU. In the Czech Republic, Open Banking allowed new entrants into the market, opening up new opportunities for FinTechs, start-ups, and other tech companies in the Czech Republic that are looking for ways to disrupt traditional financial models. In Estonia, the Open Banking has paved the way for the emergence of new e-commerce payment initiation service providers, both local and cross-border (mainly Baltic and Scandinavian FinTechs/PISPs) have entered the Estonian market.

UK has witnessed substantial growth and an increase in diversity of new FinTech third-party providers since the implementation of Open Banking, with 24/7 regulated third-party providers. There are reportedly close to 300 unique firms that operate in this field in the UK. Market analysts also expect the Open Banking sector to double its size by 2026, surpassing the total market value of USD 40 bn.

Korea has observed benefits on the FinTech side relative to small start-ups and SME FinTech companies, including start-ups with insufficient funding, thanks to the proportional nature of the data sharing framework. The open finance framework allows them to launch services in a fast manner providing an opportunity for fair competition. A single connection through the Korea Financial Telecommunications and Clearings Institute (financial infrastructure hub) is provided to all parties without the need to access individual financial companies and sign contracts. As such, even start-ups and small SME FinTech companies, which lack negotiating power or financial capacity compared to existing large companies, can launch competitive services as long as they have technological prowess and creative ideas. In addition, the fees set by the framework are such that start-ups and SMEs can use APIs at a lower cost. Lower financial infrastructure fees collected by banks is also helping them to focus on service innovation and development of tailored-financial services that reflect customer needs.

Regulatory sandbox environments are also being used for the testing of PSD2 services in the EU or equivalent frameworks elsewhere in the world. For example, the Polish Financial Supervision Authority takes an active role in providing market participants and prospective market entrants with information on the legal requirements applicable to their business mode through the Innovation Hub programme as well as by providing a sandbox environment for the testing of PSD2 services. Similarly, the UK Financial Conduct Authority in the UK has established data sandboxes that make use of such arrangements, among other things.

Another possible impact for the FinTech market involves greater and closer co-operation between banks and FinTechs as seen in Japan. The Open Banking initiative in Japan would encourage the FinTech industry to provide financial services in co-operation with banks. In Australia, the establishment of CDR provided a new market based on providing CDR-enabled services for consumers, as well as other FinTech solutions for data holders and recipients offering assistance with compliance, on boarding and participation. In Italy, according to the Fintech survey carried out by Bank of Italy in 2021, the open banking related initiatives represented about 27% of all FinTech initiatives carried out in 2021 in the Italian financial market (44% in terms of the total FinTech investments). The survey involved about all the Italian supervised institutions. Forty-eight institutions had at least one Open Banking-related initiative active in 2021, but about 94% of investments were concentrated among ten institutions. Similar benefits are also observed in Korea, as financial institutions have the opportunity to grow into comprehensive financial platforms, while they also generate synergy effects from new business models created in partnership with FinTech companies. Additionally, they can attract customers of other financial companies as new customers and have chances to exert influence on development and distribution in the financial industry.

Broader benefits to the industry are also observed, for example in the case of Korea, where the efficiency of payment markets has improved thanks to the open finance framework. This is also reported to be contributing to job creation and promoting innovation across the industry. Similarly, in France, legal certainty and harmonised rules at the EU level have promoted innovation through the development of third-party providers active in the country.

4.3. Observed interaction between FinTechs and incumbent financial institutions or BigTech

Views differ over the effect that the introduction of data sharing arrangement has had on the relationship between FinTechs and incumbent financial institutions or BigTech. As highlighted by several countries, it is also too early to observe such impact, while in other countries there has been no significant impact in the co-opetitive (co-operative competition) relationship between FinTechs and incumbent financial institutions.

Several countries have reported new innovative services and increase in activities offered by incumbents as a result of Open Banking-related frameworks. Germany has observed many established financial

institutions offering new innovative services, due to the competition with the non-bank payment service providers. In the same sense, Lithuanian Open-Banking created business opportunities and inspired new market entrants as well as the activity of incumbent financial institutions that engaged in the provision of the new services. In Mexico, non-regulated companies and BigTechs have started to establish contact with financial authorities to explore ways through which they may carry out and increase their activities in the financial market. In Poland, incumbents have been able to respond to product challenges from FinTechs (e.g. by introducing multicurrency payment cards in response to such offerings by FinTechs). Therefore, market niches that could be addressed by FinTechs, including through the use of Open Banking solutions, are less obvious. Banks have also acquired solutions developed by FinTechs and integrated them in their offering, including through investment/takeover of FinTechs.

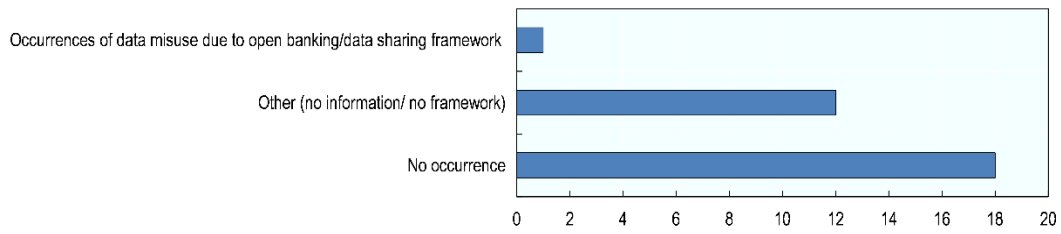
BigTechs may start offering payment services as a result of such arrangements. In Austria, for example, BigTechs have started to offer payment services (e.g. in the form of mobile wallets), a development that has been identified by the EBA as one of the future key challenges to the payment sector. However, no major issues have arisen so far. In Luxembourg, all institutions including FinTech and BigTech that provides online payment accounts have to give access to the third parties to these accounts via API. So far, however, the adoption levels are low.

Incumbent co-operation with BigTech is another very important part of the system that may need to be further analysed. Financial services are closely intertwined with BigTechs, since new services will enable the strengthening of the platform by attracting more users and increasing revenues. Furthermore, the co-operation with financial services will allow BigTechs to offer financial services without becoming subject to financial supervision themselves, benefitting from consumer's higher levels of confidence in banks and insurers. The co-operation is also playing a significant role for financial institutions, since BigTechs will provide digital convenience to the consumers, increasing the market share, and enhance the innovative power and flexibility. In the Netherlands, the co-operation between BigTech and financial institutions is mainly focused on improving digital convenience of payment services, while credit provision services are limited. Also, at the global level, including in the Netherlands, financial institutions are increasing the purchase of cloud services from BigTechs. The acquisition of FinTechs by incumbent financial institutions, including acquiring part of their equity, is observed in several prominent FinTechs in the Czech Republic, although BigTech is not yet having a major role in the Czech FinTech environment.

4.4. Occurrences of data misuse due to Open Banking

The occurrence of data misuse, data leaks, or cyber-attacks due to the establishment of Open Banking or other data sharing frameworks is one of the biggest concerns when it comes to the extensive adoption of data sharing frameworks. However, so far, there has been only one country with reported case of data misuses in the sample of the OECD Survey.

Figure 4.4. Reported occurrences of data misuse due to data sharing frameworks



Source: OECD Survey.

The reported case of data misuse is associated with a firm that collected and stored data based on screen scraping and which was found to be in violation with data protection requirements. This case supported the emerging view that screen scraping gives rise to increase security risks and is not the optimal underlying technology for Open Finance or other data sharing frameworks.

4.5. Conclusion

Open Finance is expected by OECD countries to stimulate competition by de-monopolising data and improving information availability, while also encouraging the emergence of cheaper and better financial products for consumers.

Open Finance arrangements have multiple objectives with common themes around fostering innovation, encouraging competition and customer empowerment and choice found across the OECD countries' frameworks. Innovation can be promoted through the development of new, innovative products and services in the banking and payments sector, and even beyond. The promotion of innovation can have a knock-on positive effect on competition conditions in financial services in particular. Customer experience can be enhanced by allowing for the possible provision of more efficient and less costly services. Client empowerment is indeed being sought, as financial services customers possess control of their data and decide on which data they provide under such data access and sharing arrangements.

The OECD Survey provides an overview of the different frameworks in place for Open Banking and other data sharing arrangements and showcases the gradual evolution of such frameworks towards other types of data and other sectors of the financial system, in what is being described as Open Finance. While this evolution is taking place at different paces, common themes appear between different OECD and non-OECD countries approaches and experiences, and common challenges remain to be addressed, such as security, privacy, consent management, liability, reciprocity and provision of incentives to ASPSPs, and interoperability.

OECD countries have reported evidence that data sharing frameworks in place produce positive impacts to customers and financial services, fostering innovation, increasing competition, lowering costs, and delivering better customer experiences. Such frameworks encourage third party providers, such as FinTech start-ups, to offer existing services in a different way, or to provide new services to customers on the basis of data access. The impact of Open Banking and other data sharing frameworks on the FinTech industry can be observed both in regard to growth and diversity of companies active in several OECD countries. This has a knock-on effect on competition in the market for financial services, which has indeed been reported since the implementation of data sharing frameworks in several OECD economies.

Building on the results of the OECD Survey, further analysis may be warranted on how access to financial customer data can be ensured in a responsible and safe manner; how liability should be attributed and what other consumer safeguards need to be in place (e.g. around consent); but also whether and how there is a need to support the development of technical infrastructure that will promote data interoperability, without undermining the technology neutral approach to regulation that most OECD economies endorse.

References

Siobhan Dennehy, B. (2022), “Regulatory Powers for Smart Data Initiatives Impact Assessment (IA) Summary: Intervention and Options RPC Opinion: Informal Sighting”. [3]

The White House (2021), *Executive Order on Promoting Competition in the American Economy - The White House*, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/ (accessed on 28 October 2022). [1]

UK Government (2021), *Unlocking the value of data: Exploring the role of data intermediaries - GOV.UK*, https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries#fn:5 (accessed on 28 October 2022). [2]