Basel Committee
on Banking Supervision

Report on open banking and application programming interfaces

November 2019

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-304-9 (online)

Contents

Executive summary

Open banking[1] is an evolving trend in many jurisdictions and authorities have responded by taking a broad range of actions in recent years. For this report, the Basel Committee on Banking Supervision (the Committee) focused on aspects of open banking related to customer-permissioned data sharing where the customer initially grants permission to a third party firm ("third party"[2]) to access their data, either directly, or through the customer's bank.

The Committee recognises the importance for banks and bank supervisors to understand these open banking developments and the implications for banks and banking supervision. Accordingly, the Committee decided to conduct monitoring work, particularly on developments in open banking and the use of application programming interfaces (APIs) that were highlighted in the Committee's Sound Practices paper on "Implications of fintech developments for banks and bank supervisors".[3] The Committee gathered information on current practices from its members[4] and had discussions with industry practitioners to examine how open banking is evolving across Committee jurisdictions and to identify potential implications for banks and bank supervisors.

Below are the key findings of open banking frameworks and related challenges identified for banks and bank supervisors.

Key findings of open banking frameworks

1. Traditional banking is evolving into open banking

While the sharing of bank-held customer-permissioned data with third parties has been taking place for many years, increased use of digital devices and rapidly advancing data aggregation techniques are transforming retail banking services across the globe. This sharing of customer-permissioned data by banks with third parties is leveraged to build applications and services that provide faster and easier payments, greater financial transparency options for account holders, new and improved account services, and marketing and cross-selling opportunities. A number of Committee jurisdictions have adopted or are considering adopting open banking frameworks to require, facilitate, or allow banks to share customer-permissioned data with third parties.

2. Open banking frameworks vary across jurisdictions in terms of stage of development, approach and scope

Authorities have either taken or are considering a range of actions related to open banking in their respective jurisdictions. Some jurisdictions have taken a prescriptive approach, requiring banks to share

[1] Open banking is defined as the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, including for example those that provide real-time payments, greater financial transparency options for account holders, marketing and cross-selling opportunities. Individual jurisdictions may define open banking differently.

[2] As documented in the Annex, for the purposes of this report, a "third party" is defined as any external legal entity that is not a part of the supervised banking organisation. Third parties can be supervised entities (eg banks, other regulated financial firms) or non-supervised entities (eg financial technology firms, data aggregators, commercial partners, vendors, other non-financial payment firms).

[3] Basel Committee on Banking Supervision, "Sound Practices: Implications of fintech developments for banks and bank supervisors", 19 February 2018. www.bis.org/bcbs/publ/d431.htm

[4] This report is focused on issues related to data sharing by banks supervised by Committee members.

customer-permissioned data and requiring third parties that want to access such data to register with particular regulatory or supervisory authorities. Some other jurisdictions have taken a facilitative approach by issuing guidance and recommended standards, and releasing open API standards and technical specifications. Remaining jurisdictions follow a market-driven approach, currently having no explicit rules or guidance that require or prohibit the sharing of customer-permissioned data by banks with third parties.

- **Open banking is still in the early stages of development in a number of jurisdictions.** Approximately half of Committee members have not observed significant open banking developments in their jurisdictions. Given that open banking frameworks and initiatives are still in the early stages of implementation in many of these jurisdictions, notable activity or data on bank practices and market developments are yet to be observed.

- **There are benefits and challenges with each approach to open banking when balancing bank safety and soundness, encouraging innovation and consumer protection.** Jurisdictions taking a market-driven approach, with few requirements related to sharing of customer-permissioned data, nonetheless observed data-driven financial services with a range of consumer-centric options. Jurisdictions with more defined open banking frameworks noted the benefits and efficiencies of having clear and consistent expectations and standard APIs. However, it is unclear whether these open banking frameworks were driven by, or will drive, consumer demand and market developments.

- **Open banking frameworks also vary in scope and requirements.** Some frameworks, such as the EU's revised Payment Services Directive (PSD2), apply only to specific types of data, like payments processing data, and provide third parties with both "read" and "write" access to data and payment initiation. PSD2 does not prevent member jurisdictions from adopting a broader scope. For example, the UK's open banking initiative additionally requires the inclusion of publicly-available information on branch and ATM locations, bank products and fees. In contrast, Australia's framework provides "read-only" rights for data aggregation purposes and will eventually cover industries beyond banking, such as the telecommunications and energy sectors.

3. Data privacy laws can provide a foundation for an open banking framework

Many jurisdictions that have adopted open banking frameworks also updated or plan to update their data protection and/or privacy laws. Data privacy laws in some jurisdictions are anchored on the principle that the customer owns their data and has the right to control it. Some other legal frameworks view banks, and sometimes third parties, as the data owner, but limit their rights to control the use of such data to the boundaries of the consent provided by the customer. Many jurisdictions' consent rules also place restrictions on downstreaming data to fourth parties, and on reselling customer data for purposes beyond the customer's initial consent.

4. Multi-disciplinary features of open banking may require greater regulatory coordination

Within each jurisdiction, multiple authorities can have a role in addressing issues related to banks' sharing of customer-permissioned data with third parties owing to the multi-disciplinary aspects of open banking. Relevant authorities may include, for example, bank supervisors, competition authorities, and consumer protection authorities, among others. Given the variety of authorities involved and various mandates of these authorities, greater coordination may be needed to address potential inconsistencies or gaps in regulation.

Identified challenges for banks and supervisors

5. Open banking brings potential benefits but also risks and challenges to customers, banks and the banking system

Many banks would acknowledge that open banking has the potential to transform banking services and bank business models. However, banks and bank supervisors will have to pay greater attention to risks that come with the increased sharing of customer-permissioned data and growing connectivity between banks and various parties.

6. Challenges of adapting to the potential changes in business models

Banks may face challenges in adopting strategies needed to remain competitive and profitable in the changing digital environment. Related challenges reported include increased competition and potential loss of revenue and deposits to new competitors, namely fintechs, that offer financial services and other types of services (eg accounting, tax, financial advice and marketing).

7. Challenges of ensuring data and cyber security in an open banking framework

Data sharing brings many benefits, but also results in a bigger surface area for cyber attacks. Data collected by third parties, whether via screen scraping, reverse engineering or tokenised authentication methods through APIs, can be stolen or compromised. Furthermore, as more data is shared and with more parties, the possibility of a data breach increases and therefore effective data management has become more crucial.

8. Some of the challenges hindering the development of APIs to share customer-permissioned data include the time and cost to build and maintain APIs and the lack of commonly accepted API standards

In jurisdictions where screen scraping or reverse engineering is still prevalent, banks are challenged with balancing security against ease of access. Banks generally prefer, or in some jurisdictions, are required to use more secure methods for sharing data for certain types of accounts, such as tokenised authentication through APIs, as opposed to screen scraping or reverse engineering. These secure methods enable banks to exercise greater control over the type and extent of data shared, and enable more secure access management and monitoring. Furthermore, APIs provide advantages for third parties and customers, including potential improvements to efficiency, data standardisation, customer privacy, and data protections. However, some challenges associated with the universal use of APIs remain. The time and cost to build and maintain APIs (particularly when done on a bilateral basis with multiple organisations), the lack of commonly accepted API standards in some jurisdictions, and the economic cost for smaller banks to develop and adopt APIs have been cited as challenges.

9. Oversight of third parties can be limited, especially in cases where banks have no contractual relationship with the third party, or where the third party itself has no regulatory authorisation

Jurisdictions typically have standards for data transmission, storage and other information security requirements for banks, but most of these supervisory requirements are applied to banks and not necessarily to non-bank third parties that are part of open banking business models.

- **There can be a wide range of third party arrangements in an open banking model.** Third parties can include fintech firms directly servicing consumers, intermediary data aggregator firms and potentially other parties that may not have contractual relationships with banks. Third parties can also include non-contracted entities that are authorised or licenced by particular authorities. In jurisidictions with no defined open banking frameworks, the setting of specific requirements or expectations for these third parties may be challenging due to the absence of contracts with banks or other regulatory controls. Moreover, third parties may be able to further partner and share customer-permissioned data obtained from banks with fourth parties without the bank's knowledge.

- **In the absence of a contractual relationship, banks may find it challenging to exercise oversight and monitoring over such third parties.** In many instances, the customer engages the third party firm directly, and therefore, the bank does not have a direct contractual relationship with the third party.

- **Supervisory oversight of third parties can depend on each jurisdiction's regulatory framework and on the contractual relationships between banks and third parties.** Many bank supervisors enforce security and control requirements through outsourcing expectations for banks, but may have limited, or no direct oversight of third parties. Similar to banks' own third party oversight challenges, depending on the jurisidction, bank supervisors similarly find it difficult to enforce their supervisory expectations in cases where banks do not have contracts in place with the third party or in cases where the relationships do not fall under existing supervisory expectations.

10. Assigning liability in the event of financial loss, or in the event of erroneous sharing or loss of sensitive data, is more complex with open banking, as more parties are involved

With more parties and intermediaries involved in the provision of financial services in an open banking model, it is more difficult to assign liability and the amount of damages to the customer, if any. The level of clarity and granularity of regulations governing customer redress vary across jurisdictions and, in some cases, may not have been updated to take open banking business models into consideration.

11. Banks may face reputational risk, even in jurisdictions where there are established liability rules

Many banks view themselves as custodians of their customers' data and customers place great confidence in the banks' ability to safeguard their data. In addition, customers often turn to the regulated entity (ie their bank) first with complaints and disputes, even if the third party is responsible for the erroneous transaction or data breach.

1. Introduction

The Basel Committee's Sound Practices paper on "Implications of fintech developments for banks and bank supervisors", published in February 2018, identified the impact of two scenarios; the "distributed bank scenario" (ie fragmentation of financial services among specialised fintech firms and incumbent banks) and the "relegated bank scenario" (ie incumbent banks becoming commoditised service providers and customer relationships being owned by new intermediaries), to be potentially relevant for banks in an increasingly digitised economy. The impact of these scenarios are a consequence of the evolution of technological advances that enable fast and ubiquitous access to information and services by consumers, which present challenges to the traditional retail banking model. Elements of these scenarios are currently playing out, as evidenced by the increasing adoption of various open banking frameworks, and the use of APIs, across several jurisdictions.

This report examines open banking developments across Committee jurisdictions with the aim to better understand the implications of open banking for banks and bank supervisors. The Committee gathered information from 25 Committee members from 17 jurisdictions[5], focusing on supervised banks and customer-permissioned data.

For the purposes of this report, the Committee focused on aspects of open banking regarding forms of customer-permissioned data sharing where customers initially grant permission to a third party firm ("third party") either directly or through the customer's bank to access their data.[6] This sharing of customer-permissioned data by banks with third parties could be leveraged to build applications and services that provide faster and easier payments, greater financial transparency options for account holders, new and improved account services, and marketing and cross-selling opportunities. These could be services provided along different segments of the financial service delivery chain that have traditionally been provided by banks, or new non-financial services that create additional value to the delivery chain.[7]

2. Background

With the development of online and mobile banking, many customers explicitly grant third party firms permission to access their personal banking data in order to obtain other services. Data sharing, has contributed to innovative new financial services and products. This includes, for example, financial management tools that aggregate all of one's financial accounts into one dashboard, seamless payment transmissions between accounts at different banks, small-value transactions including intra-day payments and bank fees and mortgage comparison tools. The delivery of financial services to customers, once vertically integrated, is now being unbundled and offered by non-bank third parties, such as fintech firms. At the same time, these third parties may also create new services that banks can leverage, adding value to the delivery chain. These developments are all aspects of open banking.

[5] This report includes information from Basel Committee member jurisdictions of Asia: China (CN), Hong Kong (HK), India (IN), Japan (JP), South Korea (KR), Singapore (SG), Thailand (TH); the Americas: Argentina (AR), Brazil (BR), Canada (CA), Mexico (MX), United States (US); the European Union (EU) – Belgium (BE), Germany (DE), France (FR), Italy (IT), Luxembourg (LU), Netherlands (NL), Sweden (SW), Spain (ES), United Kingdom (UK); and Other regions: Australia (AU), Russia (RU), Turkey (TR), South Africa (ZA).

[6] As discussed in the report, open banking frameworks differ across jurisdictions. In addition to customer-permissioned data, some jurisdictions include publicly available information in the scope of their frameworks. Where relevant, these additional aspects of open banking are discussed.

[7] The Annex contains a glossary of key terms used in this report.

To facilitate such data sharing and to access these new services, many bank customers give permission to third party firms to access their banking information, including, for example, tax preparers, accountants, financial advisors and payment fund transmitters. These third parties have also engaged the services of data aggregators, which traditionally employ screen scraping or reverse engineering techniques to collect customer-permissioned data held by banks. The practice of screen scraping, a form of extracting data from websites, first began as manual copying-and-pasting and evolved into an automated process. To collect customer-permissioned data from banks, screen scraping methods require that a customer provides the third party with their authentication credentials (eg username and password) that the customer uses to log into their bank's internet banking website. The practice of reverse engineering, decompiles the code of the mobile banking applications to figure out which information is exchanged between the application and the banks' servers (through the non public API) and subsequently build a 'reverse engineered' version of the mobile application which is capable of directly exploiting the communication from and to the banks' servers. It requires a second enrolment of a mobile application (in this case the reverse engineered version) upon receipt of the customer's authentication credentials and the subsequent use of these credentials or even the creation of a proprietary set of authentication credentials (to the third party). This technique is often favoured by data aggregators over screen scraping because it is much more scalable and robust as its performance is not influenced by changes made by banks to their customer interface. Both techniques are unsecure for the customer, since the third party maintains the credentials that provide full access to the customer's account, including for example, the ability to access data that has not been authorised by the customer, to execute financial transactions and to change the aforementioned customer authentication credentials. In some jurisdictions, proprietary interfaces and communication protocols have also been developed and used.[8]

Banks, third parties and regulators recognise the security and customer protection risks associated with screen scraping and reverse engineering. Third parties use these methods to collect and store customer credentials (ie username and password), which could be stolen or misused, including for payment fraud purposes. Screen scraping or reverse engineering can undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the customer, data aggregator, and an unauthorised third party that is logging in and extracting sensitive data. Additionally, after obtaining the customer's consent, third parties (such as data aggregators) can log into the bank's customer interface and extract large volumes of data at multiple intervals, which can put a strain on the bank's IT systems. Nevertheless, banks often do not deny access to third parties where there is evidence that the customer provided consent.

Banks are now finding that tokenised authorisation methods through APIs provide more control over the type and extent of data shared and are a more secure way to interact with third parties. APIs allow software programs to communicate with each other and to share information without human intervention. APIs are not a new creation; they have a long history of use in software applications for communication over the Internet. However, building and maintaining public APIs can be time consuming and expensive for banks (particularly when implemented on a bilateral basis between individual banks and third parties). This can be particularly challenging for smaller banks that lack the economies of scale of larger institutions. The lack of commonly accepted API standards in some jurisdictions is an additional challenge.

Third parties often also prefer tokenised authentication methods through public APIs over screen scraping, as it is more efficient and does not require them to adjust their automated processes each time an individual bank redesigns its customer interface.

Adoption of public APIs for data sharing could lead to opportunities for both banks and third parties to gain insights and stimulate innovation in financial services. A data sharing economy could change the traditional banking business model. However, despite the potential opportunities, expanded

[8] For instance, FinTS was developed in Germany.

data sharing could also expose the banking sector to an expanded set of operational and reputational risks.

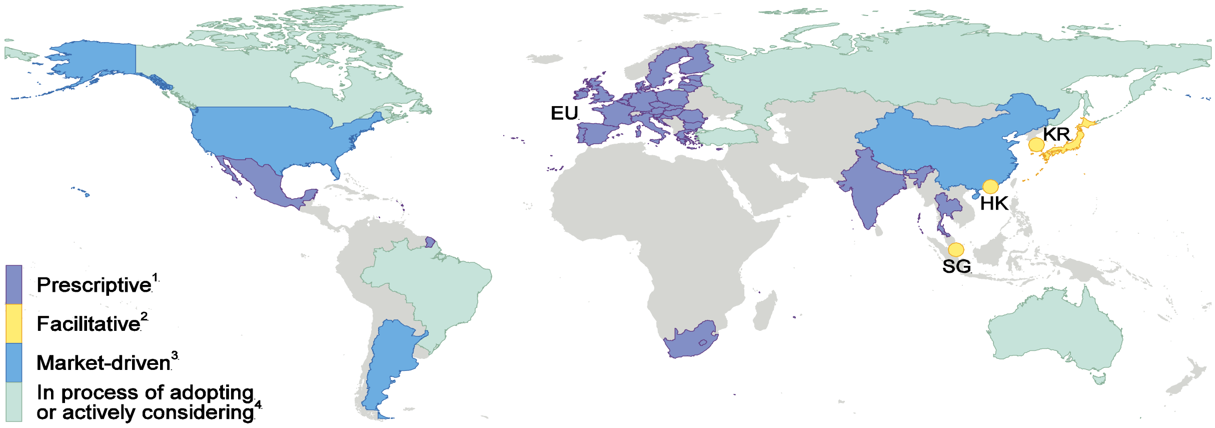
3. Legal and regulatory developments in open banking[9]

Open banking adoption is a general trend across Committee jurisdictions. Regulatory scope and oversight of open banking activities varies across jurisdictions but often includes fundamental consent and privacy expectations, as well as data security requirements. While there is a growing focus on using APIs that rely on tokenised authentication methods to share data, most jurisdictions do not currently prohibit the practices of screen scraping and reverse engineering.

Authorities have taken a range of actions related to open banking in their respective jurisdictions. Some jurisdictions require banks to share customer-permissioned data and require third parties to register with a particular regulatory or supervisory authority. Other jurisdictions have issued guidance and recommended standards, and published open API standards and technical specifications. Remaining jurisdictions follow a market-driven approach and currently have no explicit rules or guidance that either require or prohibit the sharing of customer-permissioned data by banks with third parties (see Figure 1 below).[10]

Global view of open banking developments

Figure 1



The boundaries shown and the designations used on this map do not imply official endorsement or acceptance by the BIS.

EU = European Union, HK = Hong Kong SAR, KR = Korea, SG = Singapore.

[1] Requires data sharing, [2] Encourages data sharing, [3] No explicit rule/guidance requiring data sharing, [4] In process of adopting or actively considering adopting.

Source: Based on information gathered from Committee jurisdictions

[9] For the purposes of this report, "laws" refer to legislation, "regulations" refer to implementing rules often issued by the implementing agency, and "rules" refer to laws, regulations, or both.

[10] AR, CN, US. In the US, the US Consumer Financial Protection Bureau issued consumer protection principles under the Dodd-Frank Act Section 1033 to help safeguard consumer interests as the consumer-authorised aggregation services market develops.

Among Committee members, several have some form of open banking rules in place that require banks to share customer-permissioned data with authorised third parties.[11] Others have either issued guidance rather than rules[12], communicated they are in the process of developing rules, or are actively considering adopting some form of open banking framework which may include rules[13]. Some jurisdictions are relying on market-driven initiatives[14] and are not currently considering the adoption of a rules-based approach to open banking. Nonetheless, there are benefits and challenges with each approach when balancing bank safety and soundness, encouraging innovation and consumer protection.

A comprehensive open banking framework can include rules, standards and/or industry practices across a range of issues, as well as different regulatory authorities. This is especially true for cases where unregulated third and fourth parties gain access to bank customer-permissioned data. Authorities involved in open banking can include:

- Bank Supervisor: a traditional authority that sets requirements and supervises regulated banks.
- APIs or Technical Standards Setting Body: a body that establishes standards and certifies entities that comply with such standards.
- Competition Authority: an authority that monitors, promotes and, when necessary, takes action to ensure well-functioning markets.
- Consumer Protection Authority: an authority that ensures consumers are generally not disadvantaged by monopolistic and oligopolistic practices by organisations. In some jurisdictions, their mandates may include ensuring consumers are not disadvantaged by unfair, deceptive, or abusive acts or practices.
- Data Privacy Authority: an authority that sets requirements relating to protection of personal and/or customer data.
- Alternative Dispute Mechanism: a body that provides a platform or process to mediate disputes between consumers and organisations.
- Others: any other body that has a mandate over entities engaged in open banking.

In some jurisdictions, such as Australia, competition authorities are responsible for the implementation of open banking frameworks to increase competition in the banking sector and to foster innovation. In other jurisdictions, such as the EU, India, Hong Kong and Singapore, the central bank or bank supervisor oversees the framework to facilitate faster and easier payments and to foster innovation. The scope and degree of prescription varies across jurisdictions. For example, in the EU, the focus has been on payment accounts data. Furthermore, the UK has implemented additional measures, such as the requirement for the nine largest banks and building societies to share publicly available information about branch and ATM locations, services and fees. In contrast, Australia plans to initially provide read-only rights to third parties with no ability to transfer funds, but consumer data from other sectors, such as energy and telecommunications, will eventually be covered such that data can be shared across sectors. Other jurisdictions, such as Hong Kong and Singapore, issued recommendations on open API designs and technical specifications, aiming to facilitate adoption of open banking practices (See figure 2).

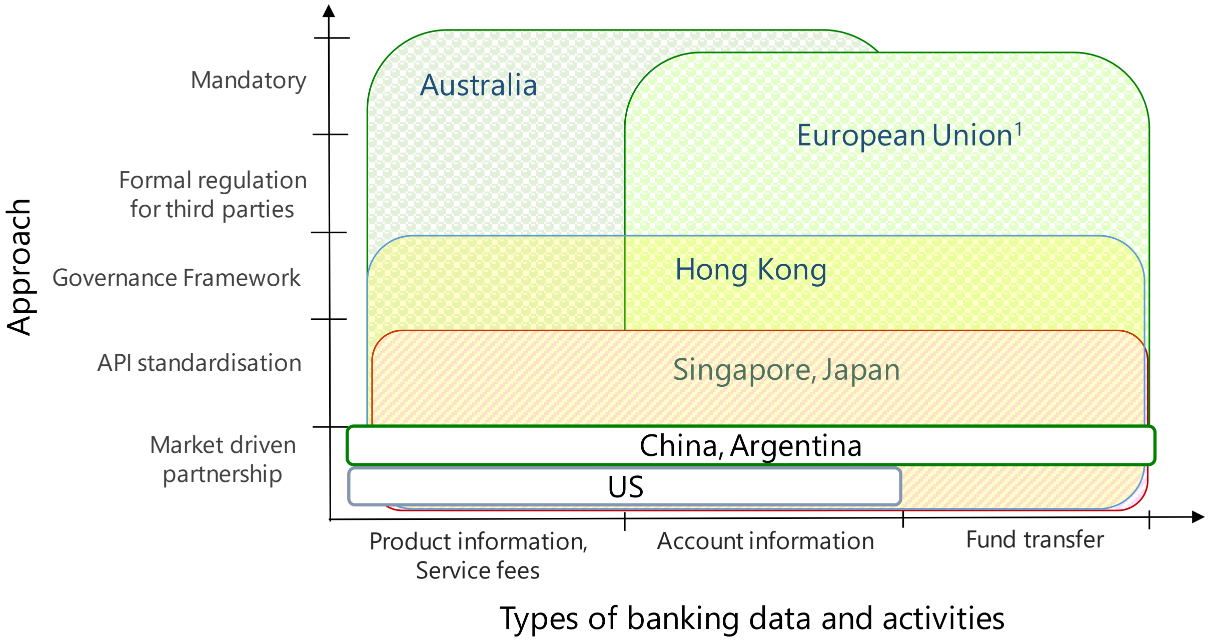
[11] IN, TH, MX, ZA, EU (under PSD2)

[12] HK, SG, KR

[13] As of November 2018 - In process of developing rules: AU, BR, RU. Actively considering adopting open banking framework: CA, TR.

[14] AR, CN, US

Comparison of open banking frameworks Figure 2



[1] EU: perimeter depicted in this figure represents the scope of the EU's PSD2, which only applies to payment services. Individual jurisdictions within the EU may choose to broaden the scope of their open banking frameworks beyond the requirements of PSD2 (eg FR and UK).

Sources: Based on information gathered from Committee jurisdictions

Generally, open banking regulatory frameworks may cover enabling third party access to customer-permissioned data, requiring licencing or authorisation of third parties, placing restrictions on screen scraping and reverse engineering practices and implementing data privacy and disclosure and consent requirements. Frameworks may also contain provisions related to whether third parties can share and/or resell data onward to "fourth parties", use the data for purposes beyond the customer's original consent and to whether banks or third parties could be remunerated for sharing data. Open banking frameworks may also contain expectations or requirements on data storage and security.

Figure 2 helps to illustrate how open banking frameworks compare by approach and type of banking data covered across certain Committee jurisdictions.

4. Roles of banks, third parties and regulatory authorities in an expanded digital financial ecosystem

4.1 Licencing and authorisation of third parties

Most Committee jurisdictions do not require third parties to be authorised or licenced in order to access bank customer-permissioned data (whether via screen scraping, reverse engineering or APIs). Bank supervisors in these jurisdictions generally require or expect banks to have bilateral agreements with third parties that access data. However, a few jurisdictions do not require or expect banks and third parties to have bilateral contracts before sharing data.

For the jurisdictions that do require third parties to be authorised or licenced, the scope of their rules may limit the types of third parties that require authorisation. The scope of authorisation may range from narrow to broad; ie from only payment providers that access payment accounts-related data to all third parties that access various kinds of customer-permissioned data. Under frameworks requiring licencing or authorisation, particular authorities must approve these third parties. Nonetheless, depending on the licensing or authorisation framework, covered third parties may still be required to have contracts or agreements in place with banks before accessing customer-permissioned data.

In some jurisdictions with prescriptive open banking regulations, such as in the EU, data sharing requirements are imposed on authorised third parties that are licenced or approved by regulators. The banks are required to accept access requests from these approved third parties, unless there are objective reasons not to, such as the risk of fraud. In particular, the EU's PSD2 does not allow unauthorised account aggregators to access customer-permissioned payment data. Assuming that exemptions would be granted to banks with sufficient API standards, approved third parties would generally not be allowed to revert to screen scraping or reverse engineering of PSD2-covered data (ie payment account data). On the other hand, screen scraping and reverse engineering may continue for non-payment account data, such as securities account data not covered by PSD2[15].

4.2 Third party risk management

Jurisdictions typically have data sharing, storage and security requirements, but most of these requirements are for banks and outsourced bank services, not necessarily for third parties contracting directly with bank customers. In general, bank supervisors have limited authority over third parties, especially over those without contractual arrangements with the banks that they supervise and over those that are not registered with a separate authority.

In some jurisdictions, outsourcing policies place responsibility on banks to ensure third parties are compliant with these rules, and generally stipulate documentation as part of contractual arrangements. In other jurisdictions, bank supervisors have supervisory authority over registered third parties.

The EU outlines its data storage and security requirements for data sharing under PSD2's *Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication*.[16] Where the third party is authorised or supervised by an authority, EU banks generally are not expected to inspect or monitor the data security frameworks put in place by the authorised third party.

Regardless of the type of framework in place, depending on the jurisdiction, a regulatory gap could exist where a third party has a customer's consent to access its banking data but does not have contractual obligations with the bank and is not required to be authorised by a particular authority (eg third parties that practice screen scraping). In this case, both the authorities and the bank would have

[15] PSD2 is technology-agnostic, but the *Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication* requires that access to data be provided by the account servicing payment service provider (ie the data holder, usually the bank) through a secure interface, either through a dedicated interface (ie API) or through the adapted customer interface. Authorised and regulated third parties must also be identified with an eIDAS certificate and the same rules on strong customer authentication apply whether a third party is used or not. EBA/GL/2018/07, https://eba.europa.eu/documents/10180/2250578/Final+Report+on+Guidelines+on+the+exemption+to+the+fall+back.pdf/4e3b9449-ecf9-4756-8006-cbbe74db6d03

[16] PSD2's implementing rules: European Union Delegated Regulation (EU) 2018/389: the Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication, https://eur-lex.europa.eu/eli/reg_del/2018/389/oj

limited ability to stipulate risk control requirements over the unauthorised third party (and any fourth party).

5. Customer liability and redress

Determining ultimate liability in fraudulent or erroneous transactions may be challenging in jurisdictions where national liability frameworks are not adjusted to account for open banking and data sharing between multiple parties. Third parties may rely on or support the services of fourth parties (ie data aggregators in some jurisdictions). When an erroneous or fraudulent activity occurs, it is not always clear which party (bank, third or fourth party) is liable. In addition, when customer-permissioned data is incorrectly shared (eg incorrect type or scope of data, or incorrect party), it may be unclear how damages to the customer should be quantified.

Customer liability framework. Half of Committee jurisdictions have existing or planned laws or regulations addressing customer liability with respect to data access by third parties. For example, PSD2 requires authorised third parties to have professional indemnity insurance, or a comparable guarantee, against specified liabilities, such as unauthorised transactions or non-execution, and defective or late execution of payment transactions. In other jurisdictions, customer liability may be addressed by national personal data protection laws, general banking laws covering customer protection against fraudulent transactions, consumer protection laws, and civil, commercial and criminal codes. In some jurisdictions, customer liability is included in the bilateral contracts or agreements between the bank and the third party service provider.

Complaint or alternative dispute mechanisms[17] specific to open banking. Half of Committee jurisdictions have existing or planned complaint handling or alternative dispute resolution mechanisms that cover open banking issues.

Among jurisdictions with existing or planned complaint handling or alternative dispute resolution mechanisms, the EU PSD2 requires payment service providers, including authorised third parties, to put in place adequate and effective complaint resolution procedures. In Hong Kong, terms addressing the complaint handling mechanisms are expected to be included in contracts with third parties, as customers should not be responsible for any direct loss suffered resulting from unauthorised transactions conducted unless the customer acts fraudulently or with gross negligence. In Japan, the Association for Electronic Payment Services, a private body, is responsible for handling customer complaints related to open banking, while in Luxembourg and Russia, that responsibility belongs to the financial authorities. In Singapore, the Personal Data Protection Commission facilitates the complaint between the customer and the provider. India has an Ombudsman Scheme for Digital Transactions.

For jurisdictions that do not have regulatory guidance requiring complaint or dispute handling mechanisms, customers often initially take their complaints and disputes to the regulated entity (ie their bank).

[17] Defined as a body that provides a platform or process to mediate disputes between consumers and organisations.

6. Consumer Data Protection

Data privacy laws. Many jurisdictions that are adopting or plan to adopt open banking frameworks have general data privacy laws. These data privacy laws have helped to provide a foundation for the jurisdiction's open banking framework. However, differences in data privacy laws across jurisdictions have implications for developments of various open banking frameworks. For example, the EU's General Data Protection Regulation (GDPR)[18] is notable for its primary principle that consumers own and control their data. In contrast, some other jurisdictions' data privacy laws are premised on the principle that firms, including banks, own the data they maintain. For example, in some jurisdictions, permission is required from the initial bank before data is shared by the third party to a fourth party. However, nearly all Committee jurisdictions restrict third parties from reselling or using data for purposes outside the scope of the customer's initial consent, and they generally require that third parties obtain further consent from the customer before reselling the customer's data.

Disclosure and Consent. A majority of Committee jurisdictions have, or are in the process of developing, rules requiring disclosure and/or customer consent. Of these, many jurisdictions require customer consent but do not prescribe the exact contents of the disclosure form. Disclosure and consent requirements are primarily observed in contractual agreements between the banks and third parties.

Screen scraping. A few jurisdictions have developed, or are developing, limitations on screen scraping. For example, in the EU, third parties cannot screen scrape for payment account data through banks' standard customer interface as of September 2019.[19] Banks instead either offer dedicated APIs or a modified customer interface that enables third parties to identify themselves using authentication certificates when accessing customer data. Third parties use screen scraping techniques from this modified user interface, but the interface may limit or control the data available to the third party. This modified customer interface would also be used as a contingency mechanism when the bank's API is unavailable. In the EU, banks can be exempted from setting up a contingency mechanism if their competent authorities determine that the bank's dedicated interfaces (ie APIs) comply with certain conditions. While many jurisdictions have no specific laws or regulations regarding the practice of screen scraping, several jurisdictions are issuing guidance on user authentication based on open API frameworks that require the use of tokenised protocols such as OAuth 2.0[20] open APIs, which will assist industry in transitioning away from screen scraping.

7. Potential future of API use in open banking

As part of their API strategies, industry practitioners are adopting different combinations of open APIs (interfaces based on public standards), partner APIs (based on standards designed by strategic partners), and closed APIs (based on the bank's private standard). In some jurisdictions, banks have adopted both partner APIs and open APIs. While in a few EU jurisdictions, banks have started adopting various API strategies, it is reasonable to presume that more EU banks will adopt open APIs in response to PSD2.

[18] https://eugdpr.org/the-regulation/

[19] PSD2 provisions on strong customer authentication and on secure communication are directly specified in the regulatory technical standards (RTS). These include provisions on accessing customer-permissioned data through the use of "screen scraping".

[20] OAuth 2.0 and its most recent versions provide specific authorisation flows for applications that usually run on the internet such as APIs and web applications. Oauth 2.0 is the implementation example of a tokenised authentication method.

API-facilitated services. Nearly two-thirds of Committee jurisdictions believe open banking and the expanded use of APIs will have an impact on banking services. The main types of shared banking services expected to be impacted are payment services, lending services (eg loans and mortgages), investment products and services (including financial planning and management) and account services.

While Committee jurisdictions indicated expectations that there will more likely be an impact on banking services than non-banking services, nearly half of Committee jurisdictions believe that non-banking services will be facilitated by the sharing of customer-permissioned data. The top two services mentioned by Committee jurisdictions are lifestyle applications (eg ride hailing, concierge, real estate and leisure services) and business services (eg accounting, expense management, tax and budgeting services).

The impact of API banking on banks' business models will likely depend on the extent and manner of data sharing, the emergence of new financial service providers, changing market share, and the speed of change.

8. Third party uses of customer-permissioned data

Third party entities. Data aggregators and payment service providers are the most common types of third party entities that access customer-permissioned data. Other third parties cited to a lesser extent include financial advisors, investment advisors, insurance underwriters, accountants, tax agents, property evaluators, credit reference agencies, and mortgage and loan processors. EU jurisdictions also referenced PSD2 and the supplementing *Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication*, which contains provisions for authorised payment initiation service providers and account information service providers (which can also be banks) to access customer-permissioned data. EU jurisdictions observed an increase in such third parties when PSD2 went into effect in January 2018.

Third party uses. Common uses of customer-permissioned data include credit card payment processing, cash management services, and financial services, such as robo-advisory and personal finance management services provided by fintech companies. A common theme identified among Committee jurisdictions is that many third parties leverage data to enrich the user experience by providing aggregated views of users' finances for better financial planning. Examples include rebalancing accounts to enable payments, expense pattern monitoring, including user alerts and reminders, investment advice based on customers' financial assets, cross-selling products including credit products and loyalty programs, and accounting, tax reporting, and expense management services for corporate customers.

Data related to payment services is more commonly accessed via APIs, while data for information purposes (such as balances and transaction histories) are commonly accessed via screen scraping. This phenomenon may also be due to regulatory requirements in some jurisdictions, such as in the EU where payments-related data is expected to be shared via APIs. [21]

Remuneration for sharing customer-permissioned data. Many Committee jurisdictions do not have regulatory restrictions on banks' ability to charge fees to third parties for sharing customer-permissioned data or other remuneration arrangements. Some jurisdictions have, or are actively contemplating, restrictions on remuneration, or on charging fees to either third party data recipients or to customers.

While most jurisdictions do not have restrictions on remuneration, some have reported that there are limited instances where banks are being remunerated. These jurisdictions do not have regulations to cap or govern such fees, but described remuneration as being included in contractual agreements between

[21] Note that the requirement to use a specific interface to access data applies from September 2019.

banks and third parties. In the EU, although access to payment account information must be provided "in a non-discriminatory way" under PSD2 (ie without fees and providing the same level of access to all authorised third parties), remuneration for additional services may be subject to bilateral agreement and is typically provided on a commission-basis with partially fixed fees.

Customer Consent. Half of Committee jurisdictions require banks to obtain customer consent to share a customer's data with third parties, while in the other half of jurisdictions, banks can accept customer consent via confirmation provided by the third party. The latter is especially prevalent in the EU. One jurisdiction requires third parties to notify banks of the customer's consent in advance of sharing data in order to accommodate safe and secure authentication protocols. Two other jurisdictions have no explicit rules in place regarding customer authentication, so either method could be used. However, one of those jurisdictions has supervisory expectations in place to ensure controls for authentication of customer consent and digital authorisation are valid.

Data sharing with fourth parties. Most Committee jurisdictions have indicated that third parties could provide data to fourth parties as long as this is specified in contractual arrangements. Some jurisdictions have implemented laws or regulations that allow third parties to share data onward to fourth parties (eg credit bureau-related laws and the PSD2 regulations for the EU).

9. Data access and transmission

Data access and transmission by third parties can range from a basic copy and paste screen scraping process to the transmission of standardised data elements using APIs. Despite broad emphasis on the importance of ensuring the security of customer-permissioned data, approaches for data access and transmission varied across jurisdictions according to the respective legal and regulatory frameworks.

In jurisdictions without explicit regulatory requirements, banks and third parties have more flexibility in data access and transmission practices. In these jurisdictions, the scope and process of data sharing may be governed by a contract executed between the bank and the third party, in particular where data is accessed using APIs. Data security protection, including designated access and transmission architecture is generally set as a requirement in those contracts. Even in jurisdictions that have an established regulatory framework, a standardised contract format is often required, and banks usually exercise their judgment to accept or refuse the API connection requested by third parties.

In jurisdictions that do not prohibit screen scraping or reverse engineering, there is a risk that third parties rely on these methods to mitigate their costs (eg legal and IT). Concerns with screen scraping or reverse engineering include the risk that the scope of data collected by third parties could extend beyond the customer's original consent, the risk of straining a bank's IT systems not designed for high-volume automated queries and high frequency logins by data aggregators. Other concerns include the risk of incorrect data collection, as a result of changes to a bank's customer interfaces.

Some bank supervisors directly monitor third parties' data security, while others do so indirectly through the risk management programs of supervised banks. In either case, banks often have a primary role in ensuring the security of customer-permissioned data throughout their delivery chain of services to the customer by ensuring their own data security or ensuring data security at third parties via contracts.

Secure transmission. Secure transmission of sensitive data over the Internet is a necessary control to mitigate operational risk for banks and third parties. Common practices that banks use to securely transmit data to third parties and to restrict access to sensitive data include exchange of certificates and end-to-end encryption.

Legacy systems. In a few jurisdictions, banks are directly implementing APIs that are compatible with legacy systems (eg via middleware layers) while others are directly working with modern infrastructure solutions. One jurisdiction reported that banks are upgrading their systems and infrastructure because of the cost and operational issues related to maintaining and interfacing with legacy systems. Other authorities also indicated that, in some cases, banks have had to upgrade their IT resilience and recovery arrangements for selected back-end systems, as a result of the higher availability expectations of APIs.

Local and regional API standards. API standards are a set of rules and specifications that could be used by multiple banks and third parties to communicate using the same set of communication protocols, security profiles and data dictionaries. Thus, third parties that wish to access customer permissioned data from banks can streamline their operations to leverage such API standards rather than designing individual programs that communicate with each bank.

A number of different API standards are evolving around the globe. Half of Committee jurisdictions indicated that there are commonly used API standards in their jurisdictions. Development of these standards often includes industry participation. However, there is no globally adopted API standard. As regional and local API standards develop around the globe, third party firms may need to use different API standards in order to communicate with banks in different jurisdictions. This could lead to potential challenges, such as inefficiencies for third parties or fragmentation of the digital financial ecosystem.

10. API Risk Management

Committee members have identified a variety of potential operational and cyber security issues related to the use of APIs, including data breaches, misuse, falsification, denial of service attacks and un-encrypted login. Other types of identified risks include infrastructure malfunction, speed of execution and operations, man-in-the-middle attack, token compromise and IP address spoofing. An API gateway could also be a single point of failure if not designed to be resilient.

Mechanisms used by some banks to mitigate these risks include stricter access privileges, authorised end-to-end encryption, authentication mechanisms, vulnerability testing, establishing an audit trail, setting expiration times for tokens, IP whitelisting, firewalls and monitoring cyber incidents related to APIs as part of the overall cyber incident monitoring program.

Many jurisdictions indicated that their supervised banks leverage existing risk management policies, particularly for cyber security and operational risk. For some EU Committee jurisdictions, separate assessments must be conducted to evaluate data security compliance with GDPR. This could bring challenges for banks and third parties in meeting open payment requirements under PSD2 while ensuring compliance with personal data security requirements of GDPR.

11. Conclusion

Many Basel Committee jurisdictions have adopted, or are considering adopting, some form of an open banking framework. Open banking frameworks vary in scope and substance depending on national and regional factors, but they share many common risks and challenges. Many jurisdictions' legal, regulatory frameworks have limited authority over some of the parties that interact with banks. Open banking has the potential to transform banking services and bank business models. However, banks and bank supervisors will need to pay greater attention to the risks that accompany: (i) the increased sharing of customer-permissioned data; and (ii) the growing connectivity of various entities involved in the provision of financial services.

Annex: Glossary

This report uses the following definitions:

- **Open banking** – the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities. Individual jurisdictions may define open banking differently.
- **Application Programing Interfaces (APIs)** - a set of rules and specifications for software programs to communicate with each other, that forms an interface between different programs to facilitate their interaction.
  - **Open API** – an interface that provides a means of accessing data based on a public standard. Also known as external or public API.
  - **Internal/Closed API** – an interface that provides a means of accessing data based on a private standard. Also known as internal API.
  - **Partner API** – an API created with one or two strategic partners who will create applications, add-ons, or integrations with the API.
- **Customer-permissioned data** – retail customer data held by banks (eg customer transactions, personal identification data, and customer financial history) that is permissioned by the bank's customer to be accessed by a third party (and possibly shared onwards with fourth parties).
- **Data aggregators** – Affiliated and/or third party entities that collect data, including customer-permissioned data, through the use of APIs, screen scraping or other means. These entities may offer services directly to the customer, to other parties that provide services to the customer, or to other parties (ie "fourth parties").
- **Fourth party** – a strategic partner or provider that a third party outsources some work to.
- **Reverse engineering** – a process of analysing the compiled application to extract information about its source code. The goal of reverse engineering is to understand the code in order to determine which information is exchanged between an application and a server.
- **Screen scraping** – The process of using automated scripts to collect displayed data elements from one application so that the data can be used by another application. Scraping from online platforms generally requires the use of customer credentials to log in and access the data as if the screen scraper was the customer.
- **Supervised banks** – Internationally-active banks in line with the scope of the BCBS framework, but for some Committee jurisdictions, other banks are also included.
- **Third party** – any external legal entity that is not a part of the supervised banking organisation. Third parties can be supervised entities (eg banks, other regulated financial firms) or non-supervised entities (eg financial technology firms, data aggregators, commercial partners, vendors, other non-financial payment firms).
- **Tokenised authentication** – Use of a software-based token that substitutes the security credentials that identify the user and the user's privileges for the purposes of accessing applications and customer-permissioned data.