# Open Banking: Navigating the Emerging Regulatory Landscape

Skadden

10 / 28 / 20

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

Open banking is an important driver of the fintech revolution. Regulators have recognised open banking as a means of introducing competition and innovation in the banking sector. Likewise, fintechs are seizing the opportunities arising from emerging facilitative regulatory regimes designed to encourage disruption of traditional retail banking services. The fintechs, which in this context are referred to as third-party providers (TPPs), are the main drivers of change in this sector.

Below, we consider the development of regulations affecting TPPs and financial institutions in this space and highlight some of the key regulatory developments in the European Union, which has one of the more advanced regulatory frameworks governing open banking services. We also consider data protection issues that give rise to their own particular challenges. Finally, we touch upon the potential for use of open banking techniques to break up other "information monopolies" outside of the banking space.

## Regulation of Open Banking in the EU

Open banking denotes a range of activities and services. The Basel Committee on Banking Supervision has usefully defined open banking as "the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, including for example those that provide real-time payments, greater financial transparency options for account holders, marketing and cross-selling opportunities". This is a broad definition that captures payments functionality as well as financial planning and sales tools.

In the EU, the Second Payment Services Directive (PSD 2) recognizes two types of open banking services as regulated activities: (i) account information services; and (ii) payment initiation services. Account information services are defined as online services that enable the provider to provide consolidated information on one or more accounts held by the customer with either another bank or with more than one bank. Payment initiation services are intermediary services enabling the customer to initiate a payment transaction between two account providers.

Account information services providers (AISPs) are subject to a light touch regulatory regime under PSD 2. They are not required to comply with the prudential (financial resources) requirements, safeguarding standards or governance requirements that are applicable to other payment service providers. By contrast, payment initiation services providers (PISPs) are subject to all of the requirements applicable to other payment service providers, including prudential requirements. Entrant TPPs with limited experience in the provision of payment services would therefore likely find it easier initially to be registered as AISPs and limit their services accordingly and to subsequently obtain authorization as PISPs, once they are in a position to expand their functionality (and their attendant regulatory compliance capabilities).

## Development of Open Banking APIs

A key element for fintech applications and services, and emerging regulatory regimes for such applications and services, are application programming interfaces (APIs). APIs generally allow for a more controlled and robust interface between the fintechs, financial institutions and other data repositories. APIs enable TPPs to collect, model and utilise customer account and other related information to offer new services without the need for customers to access the underlying accounts. They provide for a more structured and secure solution, particularly relative to screen-scraping and reverse-engineering alternatives.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

40 Bank St., Canary Wharf
London, E14 5DS, UK
44.20.7519.7000

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

# Open Banking: Navigating the Emerging Regulatory Landscape

An open banking API facilitates interaction involving the customer, the customer's banks and the TPP in an open environment using common standards of communication. The API should ensure secure communication between the financial institution, customer and TPP and should limit the transfer of information only to data that has been permissioned by the customer. The API should also offer a similar level of functionality to TPPs as the interface used by the customer when interacting directly with the financial institution to access account information and execute payment orders.

Banks and other account providers are not incentivised to provide access to customer data through an API even if it meets these standards. Many of the major jurisdictions around the world have therefore developed minimum standards for APIs and required banks to allow TPPs to access customer information through dedicated APIs, with the current notable exception being the United States. These rules are not uniform, and different jurisdictions have taken different approaches to balancing the need to protect customer data against the need to ensure that TPPs can access a sufficient degree of customer data to provide open banking services.

Where jurisdictions have provided limited or no frameworks governing the development of APIs, as is currently the case in the United States, TPPs have tended to rely on screen-scraping or reverse-engineering to provide open banking services. Reverse-engineering involves the TPP building its own API to gain access to the customer's account, via analysis of information shared between the customer and the bank on the bank's customer interface. Screen-scraping involves the use of the customer's username and password to gain access to the customer's data directly via the bank's customer interface. While reverse-engineering and screen-scraping may sometimes be undertaken with the knowledge and even assistance of the banks, these solutions are often suboptimal in terms of the protection of customer data and customer credentials, as there may be limited transparency where the bank is not made aware of the identity of the TPP or its purpose for accessing the customer's account.

Accordingly, there is a global drive to implement regulatory regimes requiring the use of dedicated open banking APIs. However, there is wide variance in the scope of these regimes and the specific rules for API development, which makes the provision of open banking services on a cross-border basis very challenging. Some jurisdictions such as Hong Kong have developed light-touch regulatory frameworks with minimum API standards and minimum requirements applicable to onboarding TPPs. By contrast, jurisdictions with a restrictive approach (such as India) have limited the provision of account information services only to entities established in their respective jurisdictions, and TPPs are required to comply with stringent data protection requirements. In most jurisdictions in which common API standards exist, the standards are subject to change at short notice and are often not widely adopted by market participants. For developers, this adds to the time and cost associated with building APIs. Many jurisdictions also have limited oversight of TPPs compared to financial institutions, as such entities are not usually regulated. Assigning liability for regulatory breach is therefore complex, and the increased intermediation associated with open banking more generally further increases the challenge for meaningful customer redress.

## APIs Under PSD 2

The EU is an advanced jurisdiction in terms of imposing minimum requirements on the establishment of open banking APIs. Under PSD 2, banks are required to establish APIs that meet the following minimum standards:

- allow AISPs and PISPs to identify themselves to the bank;
- allow AISPs and PISPs to communicate securely to request and receive information with respect to one or more accounts and associated payment transactions; and
- allow PISPs to: (i) initiate a payment order from the customer's payment account; (ii) receive all information on the initiation of the payment transaction; and (iii) receive all information accessible to the bank regarding the execution of the payment transaction.

Further, the APIs provided to AISPs and PISPs must provide at least the same level of availability and performance, including support, as the interfaces made available to banks' customers for directly accessing the customer's payment account online.

These robust requirements applicable to APIs provided by banks give some comfort to AISPs and PISPs that they will have access to real-time customer account data necessary to provide open banking and related services. However, the development of APIs that are compliant with the PSD 2 standards has in practice been uneven amongst EU member states and amongst banks themselves. Common API standards to be implemented by all banks have been developed by authorities in some jurisdictions (including the UK); however, these standards are still in the process of development in most jurisdictions, and banks are at differing stages of implementation of open banking APIs and related technologies.

As a corollary to the requirement to develop APIs, screen-scraping is now prohibited under PSD 2, except as a contingency measure in the event that the API used by AISPs/PISPs is not available. Further, only a modified version of screen-scraping in which the AISP/PISP is identified to the bank is allowed as a contingency mechanism. There is also a divergence between EU member states on the current state of implementation of the screen-scraping contingency option. Some EU member states, such as Sweden and Spain, have exercised regulatory forbearance such that participants may continue to rely on "unmodified" screen-scraping (in which the service provider is not identified to the bank) as a contingency option until 31 December 2020. Other EU member states, by contrast, have strictly adhered to the requirement to only allow screen-scraping in which the AISP/PISP is identified to the bank; Finland has prohibited any form of screen-scraping entirely, even as a contingency. It is not clear whether all jurisdictions will ultimately prohibit all forms of screen-scraping, as this outcome depends primarily on there being technical infrastructure available in the relevant jurisdiction to support open banking APIs. Once there is such an infrastructure, it is more likely that the jurisdiction will consider that recourse to screen-scraping is not required.

In contrast to the EU, regulators in the United States have thus far taken a much more laissez-faire approach. In November 2016, the Consumer Financial Protection Bureau (CFPB) considered, but ultimately determined not to recommend, implementing binding regulations with respect to open banking. Instead, in October 2017, the CFPB promulgated a list of nonbinding principles to guide consumer protection, which were intended to "reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data". As a result, currently only a few of the largest U.S. banks have developed and implemented open banking APIs and, consequently, reverse-engineering and screen-scraping remain the norm for TPPs seeking to access consumers' accounts. The CFPB held a symposium in February 2020 to further consider whether open banking or similar regulations may be warranted. It recently announced that it plans to issue an advance notice of proposed rulemaking on this topic later this year, which may ultimately lead to the adoption of open banking regulations in the United States.

## Strong Customer Authentication

Under PSD 2, there is a general obligation for payment service providers to apply "strong customer authentication" whenever a customer: (i) accesses its payment account online; (ii) initiates an electronic payment transaction; or (iii) carries out any action through a remote channel that may imply a risk of payment fraud or other abuses. Strong customer authentication is a cumbersome process requiring two-factor authentication of open banking customers. For providers that compete on the basis of ease of use and a seamless customer experience, these requirements can be an impediment to the development of user interfaces. Whilst AISPs (and in some circumstances, PISPs) can benefit from an exemption enabling strong customer authentication to be required only once within a 90-day period, any access involving disclosure of "sensitive payment data" (such as to make new payment orders) is not subject to this 90-day exemption.

## Data Protection Considerations

Open banking service providers obtain and process significant customer data as part of their operations, and they are increasingly making use of data analytics relating to customers' transactions and financial data. Given the expanded categories and volume of personal data gathered by such providers, there is a strong interplay in the European Economic Area (EEA) between PSD 2 and data protection laws, in particular the General Data Protection Regulation (2016/679) (GDPR) as supplemented by national laws of EEA member states.[1] As PSD 2 permits TPPs to access EEA customers' payment account information, the processing of such data falls within the remit of the GDPR. While PSD 2 and the GDPR share certain common approaches to protecting data, there are also a few noteworthy differences.

### The Concept of Data Minimisation Under PSD 2 and the GDPR

The notion of data minimisation is reflected in both PSD 2 and the GDPR. The underlying objective of data minimisation under both regimes is to ensure that TPPs do not process or have access to more data than is needed to provide their services to customers. PSD 2 specifies that payment service providers are only allowed to access, process and retain such personal data necessary to provide payment services. This is consistent with the GDPR's data minimisation principle, which requires that personal data be adequate, relevant and limited to what is necessary for the purposes of the processing activity. These concepts are important for developers building out their APIs.

### Diverging Contextualisation of Consent

While PSD 2 and the GDPR both adhere to the concept of data minimisation, a key difference lies in how each regime treats customer consent. In the context of PSD 2, explicit consent

[1] The EEA member states are the EU member states together with Liechtenstein, Norway and Iceland.

from customers is a precondition for TPPs and banks to execute payment transactions or carry out payment services. The European Data Protection Board[2] has further clarified that "explicit consent" under PSD 2 is contractual, meaning that customers give consent for their data to be processed by TPPs when accepting the providers' terms and conditions. The parties may agree on the form and procedure for a customer to provide consent and stipulate that consent can only be withdrawn under certain conditions, within a specific time frame.

Beyond and in addition to the contractual consent requirement in PSD 2, TPPs and financial institutions separately rely on consent as a lawful basis for processing data under the GDPR where required for certain purposes (*e.g.*, more extensive data sharing globally, geolocation tracking, marketing data). The GDPR's notion of consent places a greater emphasis on the rights of individual data subjects, and accordingly, the threshold to obtain a valid consent under the GDPR is high. This means that consent must be: (i) explicit; (ii) clear; (iii) informed; and (iv) freely given.

In this context, consent also comes with some uncertainty for data controllers under the GDPR, as individuals may withdraw their consent at any time (as opposed to within a contractually agreed time frame as permitted under PSD 2). Consequently, when open banking providers rely on consent as a lawful basis to process data, they should implement appropriate consent management platforms and suppression lists to ensure that individuals' consent is validly obtained and maintained.

### Increased Data Protection and Cybersecurity Risks

In addition to the issues noted above, the ease of access to personal data facilitated by open banking technologies may increase the possibility of personal data breaches. Recent transactions and trends in the fintech space have revealed certain concerns around these risks, most notably:

- TPPs may potentially share or sell customer data to third parties without the data subjects' (or the banks') consent or knowledge;
- TPPs, many of which are fast-growing start-up companies, frequently receive legacy data as part of the assets in M&A transactions, but: (i) the target company's data protection compliance program under which such data was collected may have been below the standards required by regulators and the TPPs acquiring them; and (ii) the legality of integrating such data with the TPPs' own data sets is unclear;
- TPPs commonly engage the services of subcontractors (who may in turn themselves engage additional sub-subcontractors), and the status of GDPR compliance for such subcontractors is often not transparent to financial institutions as data controllers, and subcontractors' diligence on their own subcontractors may be insufficient from the perspective of the financial institutions;
- Consent might not be validly obtained, as customers may not know that the data shared with their financial institutions is also being provided to and processed by TPPs;
- Some TPPs store data indefinitely to carry out real-time data analytics and payment transactions, which increases the risk of cybersecurity attacks; and
- TPPs may not have in place the appropriate technical and organisational safeguards to adequately protect personal data (including frequent external cybersecurity testing, audits and scans), which could lead to a cybersecurity incident and subsequent personal data breach.

As a counterpoint to these risks, it is worth noting the efforts of and the potential for TPPs to improve data protection and cybersecurity practices of financial institutions. They can do so by spearheading innovation with respect to technologies to achieve the goals of open banking in a more secure manner without undermining the user experience.

As independent data controllers, both financial institutions and TPPs may face steep administrative fines under the GDPR (up to the greater of €20 million or 4% of annual global turnover) in the event of noncompliance. They could also be subject to additional financial and nonfinancial liability stemming from a personal data breach or violation of the GDPR, such as claims, regulatory investigations, reputational harm and class action lawsuits.

Given such severe consequences, subcontractor due diligence is especially important for financial institutions. It should involve carefully ensuring that TPPs' data protection and cybersecurity governance, infrastructure and processes are adequate. In addition to thoroughly vetting TPPs, these financial institutions should properly evaluate GDPR compliance across the entire value chain of the various subcontractors or subprocessors that TPPs and their subcontractors may engage.

Moreover, under PSD 2, additional obligations apply in relation to "sensitive payment data". Sensitive payment data is defined as data, including personalised security credentials, that can be used to carry out fraud. PISPs are prohibited from storing sensitive payment data; AISPs are not even able to request such data in

[2] The European Data Protection Board is an independent body that seeks to ensure the consistent application of data protection rules throughout the EU, for instance by publishing guidance.

the first place. The broad definition of sensitive payment data has far-reaching consequences for AISPs and PISPs whose business models rely entirely on access to, and processing of, customer data that is inherently sensitive. Whilst PSD 2 does specify, in relation to AISP and PISP activity, that the account holder's name and account number are not sensitive payment data, arguably this does not go far enough in clarifying the scope of sensitive payment data and the obligations of AISPs and PISPs that access and use a broad range of customer data (*i.e.*, not just an individual's name and account number) on a day-to-day basis.

### Information Monopolies

TPPs have identified "information monopolies" outside of the payment accounts arena, including consumer energy accounts, pension funds and personal investment accounts. An information monopoly exists when customer data is siloed with a single service provider as the sole source of such data. In many cases, the data may even be inaccessible (or not easily accessible) to the customer itself. Where such information monopolies exist, the techniques of open banking (such as API development) described above can be applied. Enacting rules requiring holders of information monopolies to make customer data available to the customers themselves would also go some way to facilitating the use of open banking techniques in new contexts.

* * *

Fintechs, TPPs and API developers will need to bear in mind the changing regulatory environment when developing and designing their products. The push to promote the digitalization of financial services through open banking presents a significant opportunity for innovative new products and services. Successfully navigating and anticipating regulatory change will be key to fully benefiting from these opportunities.

## Contacts

**Simon Toms**
Partner / London
44.20.7519.7085
simon.toms@skadden.com

**Azad Ali**
Of Counsel / London
44.20.7519.7034
azad.ali@skadden.com

**Eve-Christie Vermynck**
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

**Christopher Hobson**
Associate / London
44.20.7519.7039
christopher.hobson@skadden.com

**David Wang**
Associate / London
44.20.7519.7168
david.wang@skadden.com