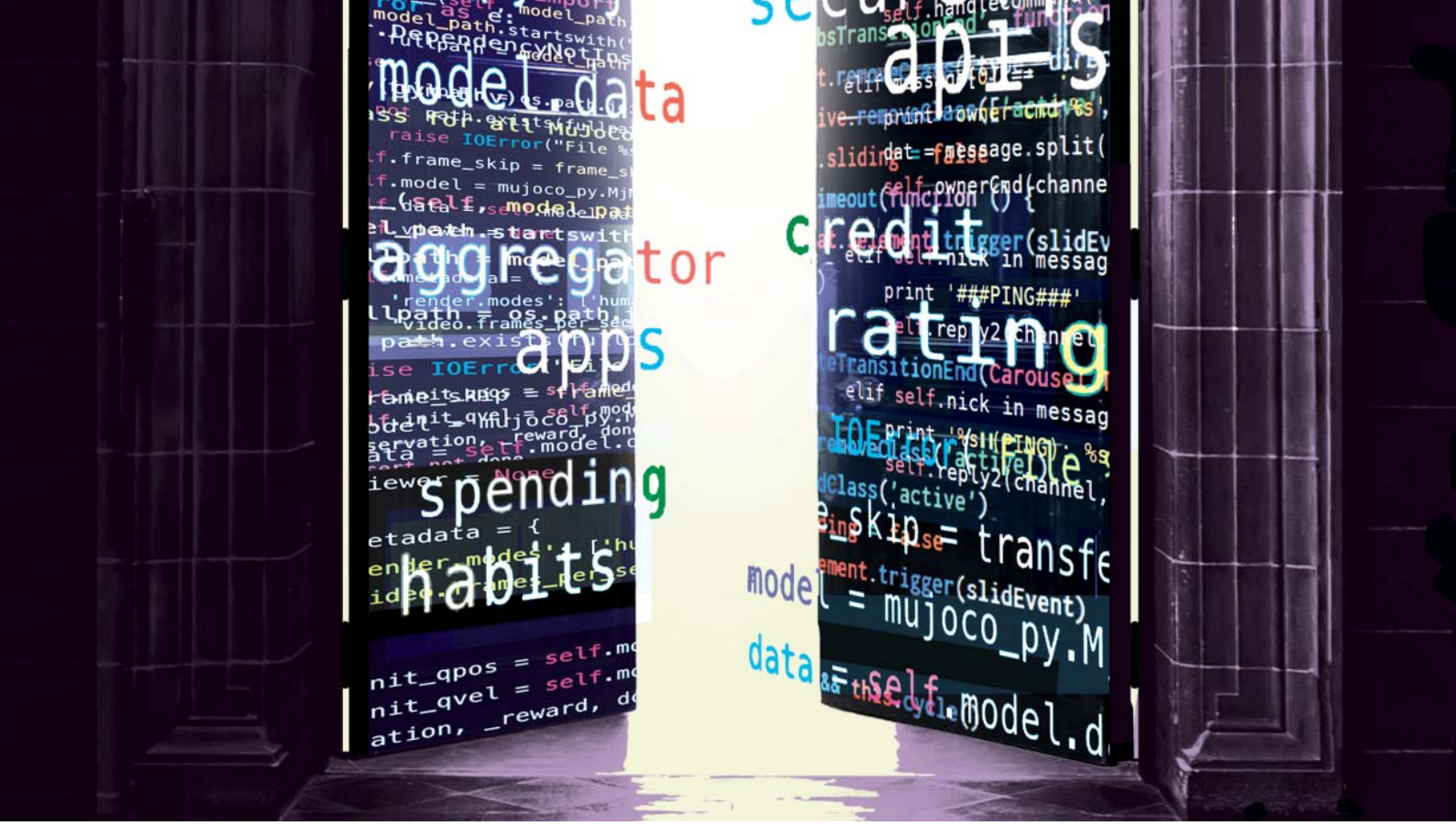


# OPEN BANKING
## AN EMERGING TECHNOLOGY GROWS TO MATURITY

James Black of Hogan Lovells examines the key issues in open banking for in-house lawyers.

Arguably one of the buzzwords of 2018, as adoption rates in the UK increased and public awareness grew, open banking looks likely to grow in significance and popularity through 2019 as this nascent technology grows towards maturity.

Far from being a fly-by-night millennial phenomenon, the early signs are that open banking is here to stay and is going to be an integral part of the landscape for any lawyer working at the intersection of technology and finance (*see Briefing "Fintech regulatory round up: taking a step back", www.practicallaw.com/w-014-9586*).

The primary focus of this article is on open banking in the UK. It addresses:

- What is open banking.
- The legislative framework.
- The objectives of open banking.
- The current status of open banking in the UK.
- Some regulatory issues that are particular to open banking.
- The key issues that lawyers advising in this sphere should be aware of.
- The status of open banking globally.

### WHAT IS OPEN BANKING?

Essentially, open banking is a framework to allow banking customers to open up their banking data and accounts to trusted third parties. Historically, the relationship between bank and customer has been a private relationship hidden behind closed doors and documented in secure ledgers. In this relationship, the key guardian and controller of data has been the bank. The challenge that open banking presents to this historical practice is that the customer gains unprecedented control of their data and the data become the customer's to share or to give away.

In this way, open banking dovetails seamlessly with recent developments in privacy law such as the General Data Protection Regulation (*2016/679/EU*) (GDPR) in the EU, the central tenet of which is to put the data subject in control of their own data (*see box "Data protection"*) (*see feature article "General Data Protection Regulation: a game-changer", www.practicallaw.com/2-632-5285*).

Data are a goldmine that the digital world is voraciously tapping into (*see feature article "Data use: protecting a critical resource", www.practicallaw.com/w-012-5424*). Financial data are a particularly rich resource, which open banking is aiming to extract and put into the hands of customers to enable them to gain access to more and better products and services.

At its most basic level, however, open banking remains a very broad and ill-defined concept and is essentially little more than a guiding principle to be applied to bring banking into the modern world. The way that it is being put into practice across the globe illustrates the myriad ways that it can be implemented and shows that there is no one-size-fits-all solution (*see "Open banking globally" below*).

## THE LEGISLATIVE FRAMEWORK

The UK has a relatively advanced and well-defined open banking system. There are a number of examples that help understand what open banking is, how it works and what factors are driving it. Open banking in the UK is delivered through the Open Banking Implementation Entity (OBIE), an organisation established by the Competition and Markets Authority (CMA) and funded by the nine largest current account providers in the UK (CMA9), whose very existence highlights the uneasy interaction of two separate and, in some ways, competing pieces of legislation, that is:

- At EU level, the Directive on payment services in the internal market (*2015/2366/EU*) (2015 Directive), also known as the second Payment Services Directive or PSD2 (*see box "The second Payment Services Directive"*) (*see feature article "New payment services regime: preparing for a revised landscape", www.practicallaw.com/8-630-5425*). The 2015 Directive has been transposed in the UK primarily by the Payment Services Regulations 2017 (*SI 2017/752*) (2017 Regulations). The 2015 Directive requires all payment account providers to permit open access to payment accounts for third parties with the necessary permissions. It does not specify the means of access or prescribe the scope of access in any detail.

- In the UK, the CMA's Retail Banking Market Investigation Order 2017 (the Order) (*see box "The Retail Banking Market Investigation Order"*) (*www.practicallaw.com/4-633-7678*). This legislation, which is applicable only to the CMA9, established the OBIE as a central standards body and explicitly mandated the use of specified application program interfaces (APIs) to provide open access to very specific data.

Reconciling the requirements of these two contrasting pieces of legislation in a single market-wide solution has been probably the greatest challenge for open banking in the UK from a lawyer's perspective (*see "Legislative tensions" below*).

## OBJECTIVES

Open banking is generally being implemented to try to achieve one or more of the following objectives: more innovation; improved competition and increased choice; and enhanced financial inclusion.

### Innovation

The 2015 Directive introduces regulation for:

- Account information service providers (AISPs), for example, an account aggregator.

- Payment initiation service providers (PISPs), for example, a service provider that automatically transfers money between an individual's accounts to avoid overdraft fees.

- Card-based payment instrument issuers (CBPIIs).

The purpose of regulation is primarily to promote innovation by providing statutory rights of access to encourage these providers to flourish. It is hoped that this will enable AISPs, PISPs and CBPIIs to bring more product and service options to consumers. In particular, the recitals in the 2015 Directive note how PISPs will be able to improve access to e-commerce by providing a way to pay online without having a credit or debit card.

### Competition

In the UK, the Order is focused, in particular, on improving competition and innovation. In its final report on its market investigation into the supply of retail banking services (the report), the CMA noted that open banking could enhance competition and improve outcomes for customers with overdrafts (*https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf*). Specifically, opening up access to balance information on current accounts can enable third-party providers to help customers assess risk and move away from relying on their overdrafts. New payment services, such as sweeping services provided by PISPs, can help customers to move their money around more easily and can help to avoid overdraft charges by enabling the automated use of other sources of funds. Another example that the CMA has highlighted is the use of PISPs to automatically transfer cash from a lower interest rate account to a higher interest rate account, which helps to overcome customer inertia and disinterest.

### Financial inclusion

An important goal for many jurisdictions that are implementing open banking is improving access to financial services (*see "Open banking globally" below*). The open banking project in Mexico, for example, has identified that open banking could bring better products

## Data protection

Given that the new services being delivered through open banking are based on access to, and use of, data, the interaction with the General Data Protection Regulation (*2016/679/EU*) (GDPR) is another area of difficulty for lawyers. For example, the Directive on payment services in the internal market (*2015/2366/EU*) (2015 Directive) introduced the restriction that payment service providers access, process and retain personal data only with the "explicit consent" of the payment service user (*Article 94*). This led to months of debate as to whether this was the same as "explicit consent" under the GDPR, an outcome that might have stifled open banking innovation at birth, given the limitations of explicit consent as a ground for processing under the GDPR.

Eventually, the position was clarified by the European Data Protection Board and, subsequently, by the Financial Conduct Authority, with the simple analysis that explicit consent in the Payment Services Regulations 2017 (*SI 2017/752*), which implement the 2015 Directive in the UK, is an additional requirement of a contractual nature and is not the same as the use of explicit consent in the GDPR, therefore leaving providers free to rely on more flexible grounds for processing data (*https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf; www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf*).

and services to customers who are currently unbanked (that is, people who do not have bank accounts) or underbanked (that is, people who do not have adequate access to mainstream financial services and products). A practical example is that opening up access can allow accurate transaction data to be used to create a better credit score for individuals and small businesses that otherwise would not have access to traditional credit products. For underbanked customers, open banking can help them to identify products that are best suited to their particular financial circumstances.

## CURRENT STATUS

Open banking in the UK is at an extremely advanced stage compared to many open banking projects in the world, as it has been operational for live access since early 2018. Open banking initiatives around the world will benefit from analysing the OBIE framework and the processes that have been put in place, and it would not be surprising to find other initiatives adopting approaches inspired by the OBIE.

### The OBIE's achievements

The key achievement of the OBIE to date is the successful launch of its open APIs in 2018, and the number of successful integrations it has managed between account servicing payment service providers (ASPSPs) (that is, a bank or building society that provides a current or business account) and third-party providers (TPPs) (that is, an AISP, PISP or CBPII).

That was merely the first step, however, in a much longer journey. 2019 will see a major extension with the launch of common open standards that promote a unified application of some of the more general requirements set out in the 2015 Directive (the OBIE standards). The OBIE standards deal with a whole host of technical issues that arise from the 2015 Directive's general mandate to require account providers to give TPPs access to customer data with the customer's consent. The OBIE standards provide the rules by which all the participants agree to play.

### Legislative tensions

The implementation and development of open banking in the UK has not occurred without challenges, however. Many of the key issues arise from the tension between the Order and the 2015 Directive. The Order and the 2015 Directive have very different goals: the Order is competition-focused and limited to the UK markets while the 2015 Directive is a major revision of the Payment Services Directive (*2007/64/EC*) which aims to improve competition and innovation, and harmonise the approach to payments across the EU. It is no surprise, therefore, that there are nuanced differences to how certain issues must be addressed.

As with any regulatory project, there is a balance to be struck between a high-level approach, which allows flexibility in implementation by setting a goal to be achieved, and a prescriptive approach, which imposes detailed obligations to ensure consistency and conformity across an industry but removes flexibility and risks stifling innovation. The UK's implementation of open banking is no exception to this and illustrates it perfectly.

The 2015 Directive's requirements are relatively general, setting out a very broad requirement on all ASPSPs to provide access to online payment accounts for the provision of TPP services. While some details are given on how access could be provided, the technical details were left to delegated legislation in the form of regulatory technical standards (RTS), which were significantly delayed. This delay left market participants, regulators and open banking initiatives to develop the 2015 Directive solutions in a vacuum and meant that they then had to seek to revise the details once the RTS were published.

In the UK, this was further complicated by the need to comply also with the Order, which sets out very detailed remedies to specific market issues that the CMA noted in the report and which came into force sooner than the 2015 Directive.

One of the greatest challenges for practitioners is therefore to reconcile the two regimes. For example, while the 2015 Directive is technology-neutral, the Order requires access to be provided by APIs. Conversely, while the Order is prescriptive about the means of access, the RTS under the 2015 Directive are permissive but contain a very broad requirement that ASPSPs choosing to offer a dedicated interface for access by third parties must ensure that there are no obstacles to access. There is, however, no guidance on what might constitute an obstacle, which has led to lengthy discussions on what this might mean in practice.

### What to expect in 2019

In the UK, the CMA9 have been complying with the OBIE standards since early 2018. Compliance is mandatory for the CMA9 but voluntary for all other market participants.

According to the OBIE open banking roadmap, which sets out the high-level implementation plan, 2019 will be a busy year, with the rollout of new functionality to help extend the scope of access from that required by the Order to the full range of access needed to comply with the 2015 Directive (*www.openbanking.org.uk/wp-content/uploads/Open-Banking-Revised-Roadmap-July-2018.pdf*). In particular, 2019 will see access to corporate accounts, batch and bulk payment initiation, and future-dated payments (*see box "Upcoming functionality"*).

### The second Payment Services Directive

The Directive on payment services in the internal market (*2015/2366/EU*) (2015 Directive), also known as the second Payment Services Directive or PSD2, sets out an EU-wide legal framework for payment services, and it replaces and updates the Payment Services Directive (*2007/64/EC*).

The aims of the 2015 Directive are: to improve payment security and consumer protection; and to integrate the payments market across the EU. The introduction of two new payment services, account information services and payment initiation services, broadens the range of services and products that can be provided to customers. One of the key goals of the 2015 Directive is to ensure a level playing field for different payment service providers.

The 2015 Directive's connection with open banking is that it grants registered or authorised third parties the right to access customer payment accounts, which includes current accounts, credit card accounts and e-money accounts. However, the 2015 Directive does not prescribe the means of access that must be offered.

While the start of 2019 has seen a slew of articles in the media looking at the impact of open banking one year on, it is important to remember that, at this stage, the project is only halfway there. Judgment should perhaps be reserved until the full scope has been implemented, and RTS compliance achieved, later in 2019.

## REGULATORY SUPERVISION

The new services that have been introduced in the 2015 Directive (account information services (AIS) and payment initiation services (PIS)) have brought with them a new chain of market participants. Unlike traditional banking relationships, which have only two parties, the bank and the customer, these new services are often provided through a much more complicated chain of service providers. The issue of which entities need to be supervised is therefore crucial and often difficult.

This question is important not just because carrying on regulated activities without Financial Conduct Authority (FCA) permission is a criminal offence in the UK under regulation 138 of the 2017 Regulations but also because account providers are obliged by the 2015 Directive to provide access only to TPPs that are authorised (in the case of a PISP) or registered (in the case of an AISP) as applicable. A TPP that is not authorised or registered does not have access rights in its own right and it would therefore be unable to require an account provider to provide access.

The following example illustrates the difficulties that can arise. An entity, Y, has a customer-facing relationship but relies on a third party, Z, to provide the account aggregation engine that drives the service. The FCA Handbook provides that whether a service is an account information service depends on whether there has been access to payment accounts (*Perimeter Guidance manual (PERG) 15.3*). Y would therefore not require permission in the UK because it does not access the customer's accounts. As a result, however, Y also has no right to access accounts.

This means that Y's service provider, Z, must be authorised. PERG goes on to state, however, that where more than one business is involved in providing an account information service, the business that requires authorisation or registration is the one that provides consolidated account information to the payment service user. Consequently, it is possible to create a chain of providers that may not strictly include a single person carrying on the regulated activity. As a result, none of the providers in the chain will have a right to access payment accounts for the provision of TPP services. Merely obtaining and processing data but not providing them to the user appears to lead the FCA to categorise a firm as a technical service provider meaning that the firm does not need to be regulated.

There may, of course, be advantages for Y to fall into the technical service provider exemption because, as an unregulated entity, it will not have to comply directly with the 2015 Directive or the FCA's rules. However, there is a big potential drawback because not having access rights in its own right may create a problem for Y's business proposition.

### Agency relationship

The law does not currently allow appointed representatives for AISPs or PISPs as payment services do not fall within the Financial Services and Markets Act 2000 regime. Therefore, AISPs and PISPs cannot use the FCA's appointed representative regime to enable another firm to make use of the principal's access rights through its role as an appointed representative. In practice, therefore, a company wishing to use another entity to obtain the data is likely to need to use a more traditional agency relationship, in order that the principal is treated as both accessing accounts and providing the data to the user. This brings its own considerations from a commercial and liability perspective.

## KEY ISSUES

Anyone working with financial technology businesses or account providers may be involved in advising on issues connected to open access. The basic issues that all commercial and corporate lawyers should be aware of are discussed below.

### Regulated activity alert

As mentioned above, the provision of payment services is a regulated activity under the 2017 Regulations and requires authorisation from the FCA (*see "Regulatory supervision" above*). It can be difficult to work out when an entity is providing payment services, however, since it covers such a broad range of activities and, despite the name, may not necessarily involve a payment (AIS, for example). Carrying on a regulated activity without permission is a criminal offence. Although there are certain exceptions that could apply, particularly for services that do not involve a payment service user, they are not all easy to apply in practice.

In particular, the role of players within a chain linked to the provision of payment services is unclear. While, generally, the entity that deals with the end user is likely to need authorisation, it is difficult to be certain whether entities providing services further up the chain are carrying on a regulated activity.

### The Retail Banking Market Investigation Order

The Retail Banking Market Investigation Order 2017 (the Order) is a piece of UK legislation that implements the Competition and Markets Authority's (CMA) final report of its market investigation into the supply of retail banking services (the report) (*see "Competition" in the main text*) (*https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf*).

The report focused on the lack of competition within the retail banking market, in particular, in the personal and business current accounts markets. The CMA required several remedies to address its competition concerns. One of the key remedies was the introduction of open banking for the nine largest current account providers in the UK (the CMA9).

Under the Order, the CMA9 were required to establish and fund the Open Banking Implementation Entity (OBIE), and to work together with OBIE to develop open application program interface (API) standards for read and write access, that is, both account information and payment initiation access (API standards). The API standards are compulsory for the CMA9 but optional for other market participants.

### Contracts

One way that the 2015 Directive challenges traditional approaches to co-operation between businesses is by stipulating that the provision of third-party services will not depend on the existence of a contractual relationship between the TPP and the ASPSP (*Articles 66(5) and 67(4)*). This means that banks and other account providers not only have to allow access to their customers' data but must do so without restriction or discrimination, and without being able to charge for those data. In a world where data are increasingly valuable, that is a game-changer.

The law does not, however, prohibit an ASPSP from having a contract with a TPP. This opens the door for account providers to offer two levels of service:

- The basic access required by the 2015 Directive.
- An enhanced level of access, which could include, for example, additional data, or product or account types, but for which the TPP would have to enter into a contract allowing allocation of liability on commercial terms and providing for payment for access.

### Liability

Arguably one of the least satisfactory parts of the legislative framework, and potentially the most contentious in future, is the question of liability in the absence of a contract, particularly in the context of unauthorised (that is, fraudulent) payments or incorrectly executed payments made through a PISP. The 2015 Directive requires the ASPSP to:

- Refund the account holder within one business day if an unauthorised payment is made, including where the payment was made through a PIS. The caveat to this is that where the PISP is liable, the PISP must immediately compensate the ASPSP. With no guidance or direction given on when the PISP would be liable, and no contract in place to allocate liability, this looks like fertile ground for disputes.
- Compensate the customer where a payment is incorrectly executed. The PISP is required to prove that, within its sphere of competence, the transaction was authenticated, accurately recorded and not affected by a technical deficiency linked to the incorrect execution. If the PISP is liable, it must compensate the ASPSP immediately. Again, while this may look workable on the surface, it is debatable to what extent this mechanism will work in practice. After all, it is never easy to prove a negative.

## Upcoming functionality

New functionality to be made available through the Open Banking Implementation Entity in 2019 includes the ability for a third-party provider to:

- Access corporate accounts (that is, more complex accounts for corporate customers that often involve higher levels of access security and multiple user authorisation levels).
- Initiate batch payments (that is, a single file of payments to be made to multiple payees from multiple accounts) and bulk payments (that is, a single file of payments from a single account to multiple payees). These will facilitate the use of payment initiation services for payroll and other corporate use cases.
- Initiate and schedule future-dated payments, whereas currently only immediate payments are supported.

## OPEN BANKING GLOBALLY

While open banking is, for the largest players at least, being delivered in a particular way in the UK, driven largely by the requirements of the CMA, there is no standard vision of how to put the concept into practice elsewhere. Interpretations of open banking globally vary widely, resulting in many different permutations of it in other jurisdictions, as each local solution will be shaped by different regulatory and contractual considerations.

While the implementation of open banking is driven by a number of fundamental common goals and principles, different jurisdictions will place a different emphasis on each of these. In jurisdictions such as the UK, for example, open banking is focused on improving customer choice and promoting competition while in other countries, notably in Central and South America, Africa and parts of Asia, the primary objective may be to improve the financial inclusion of the unbanked or underbanked. People who are unbanked or underbanked typically rely heavily on non-traditional forms of finance and micro-finance such as payday lenders, loan sharks and pawnbrokers.

Given the relatively advanced state of the UK open banking system, there is much that other jurisdictions can learn from the UK experience but, at the same time, market participants that operate in other jurisdictions will need to bear in mind that the UK model is not necessarily a blueprint for success. The needs of the market and regulators will vary and may be better or more quickly met through alternative choices in some areas.

### Global initiatives

Open banking initiatives are springing up across the globe as more jurisdictions embrace the benefits of opening up access to financial data. Open banking in the UK, with its dual foundation based on the Order and the 2015 Directive, is one of the leading initiatives in the world and it offers other jurisdictions a good framework for setting up their own open banking system. However, given how broad the concept of open banking is, it is not surprising that open banking has been implemented in different ways with different scopes and to serve different goals.

An important point to remember is that compliance with the 2015 Directive or with open banking in the UK does not guarantee compliance with any other open banking projects across the globe. For example, while the OBIE has been developing a set of API standards in the UK, the Berlin Group in Germany and Stet in France have been working on their own approaches to implementing the open banking aspects of the 2015 Directive. These groups have reached different conclusions in relation to some of the challenges brought to light by the generality of the 2015 Directive requirements. Other EU jurisdictions, in particular, Poland and Slovakia, may also implement more detailed specifications to support the 2015 Directive requirements.

In general, three main issues can affect the shape of an open banking initiative, and there is a spectrum of options within each issue:

- Open banking initiatives can be led centrally by a regulator or legislator, or can be market-led. Market-led initiatives tend to be voluntary while government-led initiatives tend to be mandatory, although there are examples of government-developed initiatives that are voluntary. Some systems, such as open banking in the UK, are a mix of mandatory and voluntary.

- Depending on how it has been introduced to the market, open banking can be a rather broad and high-level concept, such as the requirements introduced in the 2015 Directive, or it can set out very specific and specialised rules and standards that need to be adopted.

- Open banking initiatives can focus on read-only functionality (that is, accessing data from accounts) or both read and write functionality (that is, both accessing data and also being able to give instructions). Different limitations can be placed on either or both types of functionality to suit different market needs.

Given the numerous paths that an open banking initiative can take, it is no wonder that the projects around the world are taking different forms and shapes. The initiatives are also being driven by different concerns: in some jurisdictions, the focus may be on improving access to banking services for the unbanked or underbanked; in others, the focus may be on improving competition in a stagnant market or to drive innovation. Many of the global open banking initiatives are still in their early stages so it remains unclear what any future obligations may look like in those jurisdictions.

One thing is clear, however. The days of banks having a monopoly over banking data are well and truly over.

*James Black is Counsel at Hogan Lovells.*

## Related information

This article is at practicallaw.com/w-018-8842

**Other links from uk.practicallaw.com/**

**Topics**

| | |
|---|---|
| Authorisation | topic/7-201-5204 |
| Banking | topic/7-385-1287 |
| Data sharing | topic/2-616-6187 |
| Fintech | topic/w-012-0924 |
| GDPR and data protection reform | topic/7-616-6199 |
| Information technology | topic/5-103-2074 |
| Payment services | topic/9-103-2034 |
| Regulated activities | topic/2-201-5211 |

**Practice notes**

| | |
|---|---|
| A guide to Practical Law's materials on regulated activities | 6-505-5843 |
| Fintech jargon buster | w-010-9893 |
| Fintech: UK financial services regulatory developments | w-014-6806 |
| Overview of GDPR: UK perspective | w-013-3757 |
| Overview of PSD2 | 4-629-7314 |
| UK implementation of PSD2 | w-007-1613 |

**Previous articles**

| | |
|---|---|
| Data use: protecting a critical resource (2018) | w-012-5424 |
| Fintech: key issues for operating fintech businesses (2017) | 9-639-9305 |
| Challenger banks: risks and rewards for new entrants (2016) | 0-630-1959 |
| General Data Protection Regulation: a game-changer (2016) | 2-632-5285 |
| New payment services regime: preparing for a revised landscape (2016) | 8-630-5425 |
| Big data: protecting rights and extracting value (2015) | 1-595-7246 |

*For subscription enquiries to Practical Law web materials please call +44 0345 600 9355*