KEY POINTS

- Open Finance poses huge potential for innovation in the provision and use of consumer financial products.
- There are however risks with Open Finance including cyber security and the collection and use of data. Both require planning in order to design a system for assigning liability.
- Those engaged in Open Finance should consider who is liable in the event of a cyber security breach and whether their insurance adequately covers their activities in the event of a breach.

Feature

Author Rebecca Keating

Opening innovation or opening up to risk? The potential liability framework for Open Finance

This article summarises some of the key points in the Financial Conduct Authority's recent Call for Input regarding Open Finance. Certain risks associated with Open Finance are highlighted and possible issues surrounding assigning legal liability in open finance models are addressed.

Data and technology are increasingly important to almost every facet of our lives, and the provision of financial services and banking is no different. The increasing role of data and technology in financial services and banking has led to the possibility of increasing engagement with customers, streamlining existing services and innovation. In the UK, and globally, there has been enhanced emphasis placed on Open Banking and Open Finance. Both offer the potential to have a meaningful impact on the way in which consumers engage with and use retail banking and financial services.

OPEN BANKING

Customer data is currently held largely by a relatively tight circle of established market leaders. "Open Banking", implemented by way of the revised Payment Services Directive (PSD2) and domestically by way of the Payment Services Regulations 2017 (PSRs), comprises of a series of measures which enable customers to give access to their banking transaction data to trusted third party providers (TPPs). There is also the Competition and Markets Authority's Retail Banking Market Investigation Order 2017 (RBMI Order) which applies various measures to the nine largest current account providers in the UK for the purpose of enhancing competition in retail banking. Open Banking therefore applies specifically to the banking sector, as opposed to financial products more broadly.

OPEN FINANCE

Open Finance applies a similar model to Open Banking. The Financial Conduct Authority (FCA) describes Open Finance as "where consumers and small businesses can give access to their payment account data to third party providers to get new services". The FCA goes on to note that "open finance would extend open banking principles to give consumers and businesses more control over a wider range of their financial data, such as savings, insurance, mortgages, investments, pensions and consumer credit" (Open Finance). Examples of possible use cases of Open Finance include:

- Displaying information on one platform for a customer which would explain which financial products they were using and enable a customer to better understand their financial position.
- Tools to assist consumers in managing their savings and pension investments.
- Budgeting tools.
- Aggregation of insurance policies on one platform which might enable customers to identify whether they have over or underinsured.
- The ability for third parties to reach out to consumers with more competitive deals on financial products.

On 17 December 2019 the FCA published a call for input "to explore the opportunities and risks arising from open finance" (CfI). The CfI closed on 1 October 2020.

It will naturally take some time to see the impact of Open Banking and Open Finance. In respect of Open Banking, however, there have been some promising levels of interest. The CfI notes at para 2.7 that "since the introduction of PSD2, we have registered or authorised over 135 new firms offering account information and payment initiation services". In respect of customer adoption, the FCA Sector Views report 2020 note that there are "over 1 million UK consumers using open banking services".

There are many points to consider in implementing Open Finance. For example, those who do not use technology, due to a lack of access to or a lack of training in the use of technology may be disadvantaged. However, this article focuses not on the benefits or drawbacks of Open Finance but rather the practical implementation of these measures and the possible liability framework surrounding the Open Finance initiative specifically.

A FRAMEWORK FOR LIABILITY

A key component of the ultimate adoption and success of Open Finance will be a clear framework for establishing liability. This is of importance not only to consumers but also to financial institutions and TPPs. Under PSD2, TPPs are required to hold professional indemnity insurance or a comparable guarantee against potential liability. In the event of unauthorised transactions, banks are required to refund the customer first and then to seek compensation from TPPs if those TPPs are at fault. The Open Banking Standard (OBS) has created a dispute management service which handles

enquiries, complaints and disputes. As regards Open Finance, the recourse for a customer may be slightly more difficult given that the regime and regulations will not apply, without further expansion, to all services impacted by Open Finance. In addition, the more expansive range of products and services that come within the scope of Open Finance may not be as well suited to similar provisions which govern Open Banking.

Open Finance poses two key areas of risk regarding the assignment of liability. The first area relates to potential claims arising out of issues with cyber security and the second is the collection and use of data. These issues may become particularly complex where there is no direct contractual relationship between the financial institutions, TPPs, aggregators and consumers. As noted by the Basel Committee on Banking Supervision in November 2019, TPPs themselves have no regulatory authorisation, which may further limit the possible grounds upon which liability might be attributed. Certain solutions have been adopted internationally, including data access agreements in the US. The following sections seek to explore areas of liability that might arise and potential frameworks for addressing these risks.

CYBER SECURITY

Sharing data

At the core of Open Finance is the increased sharing of data. The CfI notes at pp 3 and 4 that the FCA envisages a number of desired outcomes. Two data-related outcomes are that the FCA envisages a system whereby customers can "grant access to their data to trusted third-party providers (TPPs) and in return gain access to a wider range of financial services/products" and "have greater control over their data". This of course has to be paired with the potential risk highlighted later at para 4.3 of the CfI that there may be an increased risk of fraud if all of a consumer's data are available through one single point of entry, or are held by firms with poor system security and governance. Therefore, secure access to data is not just a key point of infrastructure but is also very important from a legal perspective.

While there are many practical steps that could be, and indeed should be, taken by financial institutions and the TPP with whom data is shared and/or by whom data is accessed, increased sharing or access can result in increased vulnerability. There are many points to consider aside from the traditional concerns regarding storage and processing by the financial institution of the data. There will also be the process by which that data is shared or accessed with an aggregator and ultimately the TPP.

The FCA addresses at paras 3.5 to 3.6 what means of access might be used. The CfI states that "in most cases this would mean TPPs could access the same information and perform the same functions as those available digitally to the customer". This would mean a TPP could do two things:

- collect a customer's financial data to present to them. The FCA refers to this as read access; or
- undertake or initiate transactions on the customer's behalf. The FCA refers to this as write access.

Both pose risk from a cyber security perspective but the latter point, write access, poses greater risks than the former.

APIs

The FCA goes on to note in the CfI that their assumption is that this access would be by way of Application Programming Interfaces (APIs). An alternative to APIs is the method of screen scraping, a process by which a consumer provides log-in details to the data aggregator. The data aggregator would then use those log-in details to access the customer's account directly. From a legal and compliance perspective, aside from the issues relating to data security and privacy, this may also constitute a breach by a customer of a provider's terms of service as such terms typically restrict the sharing of log-in details with third parties. Therefore, instead of providing access to the log-in details, APIs would involve consent being given by the customer and facilitated by the relevant financial institution for access to the data. The data aggregator then accesses a set of financial data. That data set, if collected properly, should only contain specific data which the customer has consented to sharing rather than the entirety of the data accessible to the customer directly. This method is preferable as it limits the potential for unauthorised sharing of the customer's log-in details.

Earlier in the CfI, at para 1.9, the FCA notes that certain banks and pension providers have developed their own proprietary APIs. The purpose of the APIs is to enable third parties to offer services to their customers. The FCA also notes that the Investing and Saving Alliance (TISA) has also developed APIs for open savings and investments. However, under PSD2 TPPs could also use a modified customer interface to connect directly to a bank's website with a customer's consent. The RBMI Order however required access to be provided by APIs.

The FCA states at para 3.6 of the CfI that APIs were preferable in that they reduce barriers to the market as third parties do not have to integrate via a data aggregator on a firm-by-firm basis and that this offers enhanced security. It is the latter point which is of particular importance from a legal perspective. Liability where there is a vulnerability in the API will likely rest with those responsible for the API and securing the customer's data, which will ordinarily be the financial institution. This may be a particularly acute burden where the financial institution has limited resources to implement a new API. Open-sourced APIs (publicly available applications) may alleviate this burden but will require some capital and trained staff to implement.

With screen scraping the consumer might likely be held liable for an unauthorised transaction on account of sharing the log-in details with a third party. However, where an API is used the question of liability is more complex. This again may have another layer of complexity where the breach did not occur when accessing the API but rather any subsequent extraction, processing and retention of that data.

It is not simply a case of considering whether the financial institution or TPP is responsible. While the TPP naturally receives much consideration in the CfI, the

aggregator, namely the technical service provider, receives less attention. However, these are of course a key component of Open Banking and Open Finance in that it is the aggregator that retrieves the customers' data. The role of the data aggregator should also be explored as they form a key part of possible liability arising in Open Finance.

In the event of fraud or mishandling of data, liability will likely be impacted by the following factors:

- Those responsible for the vulnerability. However, in practice this may be difficult to determine without expert input as to the cause of the vulnerability. This will depend on both where the data resided at the time of the breach and the source of the vulnerability which led to the breach. This may be a difficult technical task when one considers the combination of legacy IT systems and the need for an interface with new environments to facilitate access.
- Who is responsible for safeguarding the customer's data.
- As between the financial institution, the aggregator and the TPP there may be additional agreements in place which assign liability or risk. There may be contractual provisions and/or indemnities as between these parties which react in the event of a particular breach.

Parties should then consider whether their existing insurance policy covers them for the particular breach. Those engaged in Open Finance should therefore be considering prior to a breach whether their insurance is adequate and, in particular, whether a form of cyber insurance should be sought.

Setting aside the issue of security, and assigning liability in the event of a breach, the question also arises as to whether all APIs are to be publicly available or only available at a price. While some APIs may be launched by the financial institutions themselves, a question arises as to whether these financial institutions or banks can benefit financially from the sharing of customers' data. This is not a question considered in the CfI. Interlinked with this question are the issues of database rights and copyright. Those providing access to the data will understandably want to consider how best to protect their investments in data quality and their work invested in their databases. It may be that while institutions may not charge for basic access which is required under applicable law, they may be able to charge for an enhanced level of access that goes beyond what they are required to provide.

ISSUES WITH DATA

A framework for informed consent

Building an adequate framework for consent is of great importance to Open Finance. The CfI highlights at para 4.3 that consumers may provide consent to share their data but not be aware of how their data is ultimately used, leading to the potential for use the consumer had not contemplated or intended.

Article 6 of the General Data Protection Regulation (GDPR) requires consent for the processing of data. The GDPR also refers to "explicit consent" which has a very different meaning to Art 94 of the PSD2 which also refers to "explicit consent". The FCA's guidance on PSD2 states that the interpretation of explicit consent under the GDPR should not be read across into Art 94 of PSD2. Therefore, the GDPR requirements for "explicit consent" cannot be used as a means of avoiding an obligation to provide access to data to a TPP.

It should be kept in mind that although this definition is not the same across the GDPR and PSD2, the requirements under the GDPR regarding obtaining consent more generally continue to apply. Therefore, consent and a lawful basis for processing under the GDPR is still required where data is shared in accordance with PSD2. Any new regime governing Open Finance will therefore need to address both the meaning of consent in the context of Open Finance and parties' obligations under the GDPR.

Considering whether consent has been obtained for GDPR purposes may be complicated when paired with an industry in which consumers might find it more difficult to understand the possible use cases of their data. Providing transparent and clear information in order to enable customers to understand how their data is being used and collected will be of great importance.

The use of artificial intelligence and machine learning

On the face of it this may appear to be solely an issue of communication. However, increasingly firms are making use of artificial intelligence (AI) and machine learning (ML). Identifying at a firm level what data forms part of the underlying data set and how a customer's data is used is, in and of itself, a difficult task before one even begins the task of communicating that to the customer. Therefore, the task of obtaining informed consent relates not only to how data will be used to provide a service to that individual customer, and understanding where AI is used to provide that service, but also how that data may ultimately form part of a larger data set for AI and ML purposes at a firm level. Furthermore, with increased cross-industry data sharing care should be taken in ensuring that the information provided and consent obtained is adequate in this regard as well.

One suggestion is a granular model of consent, ie obtaining consent in relation to specific categories of data. Bundling consent poses a host of difficulties should consent be challenged later. Therefore, it is suggested that a granular model provides for adequate information to be provided and clear consent to be obtained.

Finally, consent should not be narrowly interpreted to mean initial consent. Consent of course must be revisited to consider how consumers restrict consent, revoke consent and the duration of consent. However, informed consent should also be considered in the context of transfer of data and retention of data subsequent to the initial consent to access being provided.

The role of the General Data Protection Regulation

Various issues arise under the GDPR. For the purposes of this article it is assumed that similar provisions will be adopted post-Brexit and briefly the following further issues are noted:

- The GDPR relates to identifiable personal data. This will therefore not

Biog box
Rebecca Keating is a barrister at 4 Pump Court. Email: rkeating@4pumpcourt.com

capture the variety of data that may be accessed, processed and retained under an Open Finance model. In particular the GDPR is focused on natural persons, specifically individuals, and not data relating to multiple people or groups. Therefore, the GDPR is inadequate to account for this type of data which will be used in Open Finance. This must be married with what contractual confidentiality provisions might also exist as between the financial institution and the customer. Regard should be had to:

- Who can consent on behalf of a group, business or organisation.
- Delegating consent and onward consent.
- If the above considerations differ depending on the category of data.
- The lawful basis of using data for the legitimate interests of a TPP might constitute a lawful basis for processing or sharing the data. Under the PSRs, TPPs must require the customer to re-authenticate after a 90-day period. This does offer some protection to inactive customers. However, in terms of the framework itself, there is a window in which certain aspects of a customer's data could be accessed, processed and possibly retained without a customer's consent. This would also not capture all data under an Open Finance model as the PSRs were developed specifically for Open Banking and not for financial products for example pensions and insurance.

Data portability and real time access

Another point to consider is data portability. The GDPR provides for a right of data portability. This would apply to financial institutions that would be subject to the Open Finance framework. However, this right to data portability does not equate to real time access. It only provides for access to certain kinds of data and only requires that data be provided within 30 days. As highlighted at para 4.3 of the CfI, out of date, incorrect or incomplete data may be shared with a TPP which could result in incorrect advice or recommendations. The question therefore arises as to who would be responsible in such a scenario.

As set out previously this may rest on what data was required to be shared, how often this was to be updated and any contractual provisions/indemnities as between the customer/financial institution/aggregator and TPP. In particular, exclusions and limits on liability may apply in terms of what responsibility has been taken for accuracy and quality. However, care should be taken to evaluate whether these exclusions and limits are tenable as read against applicable regulations which may apply in the future and of course where the customer concerned benefits from consumer rights legislation.

Offshore data

Finally, in relation to data, a point that is of importance from the point of view of accessing data is what happens where a customer holds offshore investments for example a Qualifying Recognised Overseas Pension Scheme (QROPS). The issue is of course not one of a technical difficulty necessarily but a legal one where a TPP is seeking to obtain access to data where jurisdictions have adopted a different vision for Open Finance or Open Banking. This requires consideration of what the rules are in the EU and globally.

Once the transition period for Brexit is over there will also need to be consideration given to harmonising regulation for those firms that wish to engage with customers in the EU. Setting aside points regarding the GDPR, or equivalent, there will be more specific regulation that may emerge which the UK will have to have in mind. On 24 September 2020, the European Commission published the Digital Finance Strategy for the EU (COM(2020) 591 final) and also published (COM(2020) 592 final) which sets out a Retail Payments Strategy for the EU. This strategy states that by mid-2022 a legislative proposal for a new Open Finance Framework will be drafted and that by 2024 a comprehensive framework will be in place. It is clear therefore that the EU, as well as the UK, are focusing on the future of digital finance. Close regard should therefore be had to not just what can be done at a domestic level but also the global requirements of the future of digital finance more broadly.

CONCLUSION

The absence of a clear framework for recourse in the event of breach and an absence of clarity as to underlying responsibility in the event of breach poses a threat to the advantages and adoption of Open Finance. Future regulation should consider a framework for liability and those engaged in Open Finance should also consider liability and insurance so that the benefits of Open Finance can be explored and not stifled. ■

Further Reading:

- Opening Pandora's Box: PSD2, consumer control and combatting fraud (2020) 1 JIBFL 48.
- In Open Banking's brave new world could using a third party to initiate payments weaken consumer protection? (2019) 1 JIBFL 25.
- LexisPSL: Banking & Finance: Practice note: One Banking – One Minute Guide.