HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 08215, 26 January 2018

Open Banking: banking but not as we know it?

By Timothy Edmonds

Contents:

Contents

Summary

2018 saw the start of two legislative initiatives that have the potential to dramatically change how people bank, or who they bank with:

- Open banking
- Payment services directive II (PSD2)

Part of the impetus behind these is a view that the retail banking personal current account (PCA) market is, from a competition and consumer perspective, not working well.

Open Banking (OB) requires firms to

- make it possible for people to share their financial transactional data far more easily with third parties online.
- allow third parties to initiate payments directly from a person's account as a bank transfer as an alternative to credit or debit card payments.
- make public and openly share their product information and importantly, their customer satisfaction scores and separately other 'service level indicators'.[1]

At OB's heart are the Application Programme Interfaces or APIs which bring disparate applications together in a functioning whole in an analogous way as, for example, Uber 'glues together' Google maps, payments and telephony to help people order and pay for taxis quickly."

The first Payment Services Directive (PSD) was implemented in the UK in 2009. It established a European-wide legal framework for payment services by setting the information requirements and the respective rights and obligations of payment service users and providers.

When reviewing the PSD in 2012, the European Commission argued that the legislation had introduced a number of benefits such as an increase in competition and choice. It was clear though that in order to remain relevant to the financial services environment it needed to change to reflect the rapid change in markets and technology in payment systems. Thus PSD2 was born.

For simplicity's sake, OB can be thought of as referring to technological solutions and opportunities for a new type of banking and PSD2 as its legislative base. In practice the two are interlinked.

The introduction of OB, following its go-live date (13 January 2018) has been rather quiet with fears over data and financial security dominating media headlines.

1 Barclays Bank; *OPEN BANKING A CONSUMER PERSPECTIVE*; January 2017

1. Introduction

Banking as a service and industry is seldom absent from the news. Much of this over the last ten years has been bad news dominated by the financial crisis, bankers' bonuses, mis-selling, poor treatment of small businesses, closure of high street branches etc. Amidst this there is, however, good news. The banks have largely recovered profitability – if not at the pre-crisis level – the November 2017 Bank of England 'Stress Test' on banks' capital adequacy found that "banks are three times stronger than they were ten years ago"[2], the Lloyds Banking Group is no longer part-owned by government and, it is an industry that has a highly engaging technological change story to tell. This Paper looks at elements of that story and, in particular, at two legislative framework initiatives that have the potential to dramatically change how people bank, or who they bank with:

- Open banking
- Payment services directive 2 (PSD2)

Part of the impetus behind these is, aside from the headline-specific problems, a view that the retail banking personal current account (PCA) market is, from a competition and consumer perspective, not working well. Put bluntly people stick with the same provider for years and years when they could (rationally) do better. They don't understand what they are paying for. They don't get the service they could. There have been many reports and reviews into this the most recent and comprehensive was that by the Competition and Markets Authority in 2016: *Making banks work harder for you*. On switching it said:

> Understandably, many customers see little to be gained from spending time thinking about whether they are on the right account or are with the right bank for them or any business they run. It is difficult for the individual customer to work out whether they are getting good value from their existing bank. As a result, only 3% of personal customers and 4% of business customers switch to a different bank in any year.[3]

The focus of reform is to get customers to be more active in the market, to persuade banks to change their approach and therefore improve competition and service in the PCA market. This is why there is so much emphasis on making switching current accounts easier, and no little official frustration that it happens so rarely given the, alleged, scale of the problem. Consumers seem to be quite happy getting a bad deal, or they simply cannot differentiate one bank from another and so think that switching is pointless. The CMA again:

> Current accounts for both personal and business customers have complicated charging structures, and the actual cost to the customer depends on how they use the account. Customers generally know very little about the charges and service quality provided by other banks. It is therefore hard for customers to know whether they could get better value and service from another bank or a different product with the same bank.
>
> Personal and business current account relationships are open-ended and do not have regular trigger points (like the annual renewal of insurance policies, for example) when customers might be prompted to ask themselves whether they could be getting a better deal elsewhere on their current account.[4]

One way out of this conundrum is to exploit new technology which can provide a much greater degree of choice of PCAs from a wider range of providers and, in parallel, encourage new 'challenger banks'. Enabling the broad adoption of new technology requires standardisation of interfaces between organisations and systems. This is 'open

2 Bank of England
3 CMA; Making banks work harder for you; August 2016
4 CMA; Making banks work harder for you; August 2016

banking'. This new freedom requires regulation, particularly controls on the transmission of personal data, which is the PSD2 strand.

The hope and expectation is that combining the two will produce a genuinely different banking experience provided by sharply different suppliers.

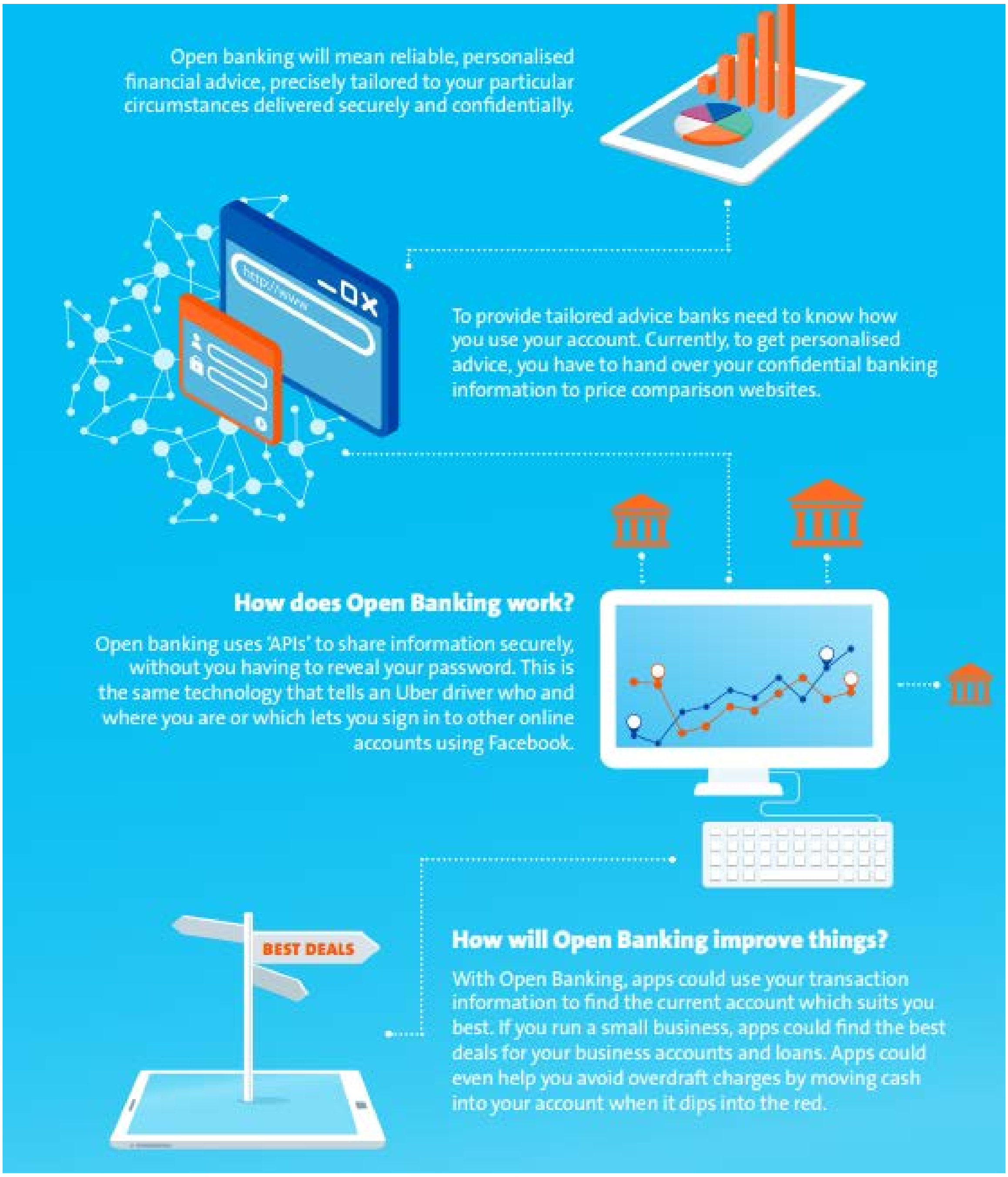
It can be reasonably argued that it is false to divide this subject into two distinct parts – open banking and PSD2 – they are part of a single initiative each part building on the other. This Paper treats, for simplicity sake, open banking as referring to technological solutions and opportunities for a new type of banking and PSD2 as its legislative base. But it acknowledges that in practice this distinction may be more imagined than real.

The Paper presents some of the ideas from recent reports into the area, in part suggested by digital banking commentator Chris Skinner.

2. Open banking (OB)

What is open banking?

Discussions of OB are blessed with many explanatory graphics. The one below is from the CMA:



A report[5] published by Barclays Bank in January 2017 defined OB as a requirement for firms to:

[5] Barclays Bank; *OPEN BANKING A CONSUMER PERSPECTIVE*; January 2017

- Make it possible for people to share their financial transactional data far more easily with third parties online.
- Allow third parties to initiate payments directly from a person's account as a bank transfer as an alternative to credit or debit card payments.
- Make public and openly share their product information and importantly, their customer satisfaction scores and separately other 'service level indicators'.[6]

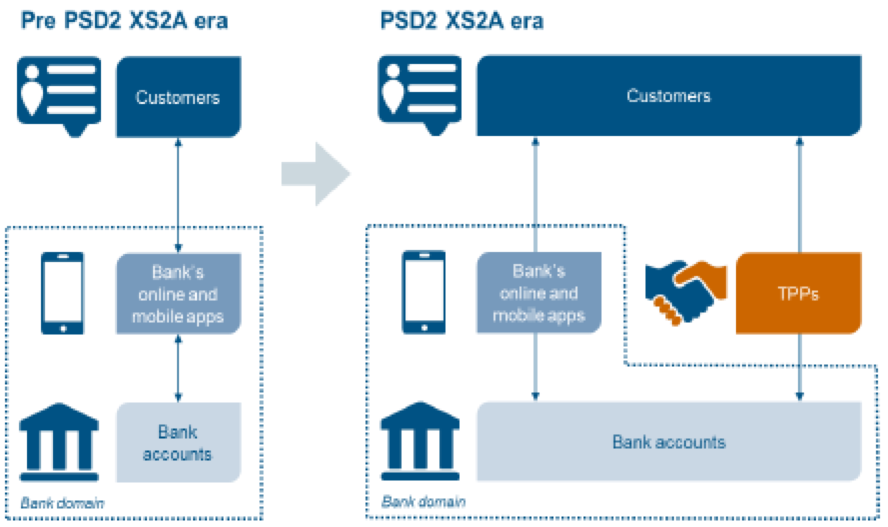
At OB's heart are the Application Programme Interfaces or APIs which bring together disparate applications in a functioning whole. As the Report points out this is not new, "Uber uses APIs to 'glue together' Google maps, payments and telephony in one useful app to help people order and pay for taxis quickly."

The driver for OB is data and lots of it. Currently the established banks and companies like the peer to peer lenders and credit reference agencies (CRAs) are the main holders of data, except in the case of the CRAs, the data is generated by a company's customers and is held (securely) by the company. The underlying 'game changer' is that under OB, data will be open to the new interface producers and it will drive the applications direct.

'Digital banking' is already well established, people use computers and mobile phones to tell their bank to pay X or to ask it for their balance. The new part of OB is that individuals will have communications with non-bank partners, both ways, to get information, receive offers, get advice or make payments, based on their own preferences and needs as evidenced by their banking data. The application of algorithms and AI to banking data will provide the basis for a more personal financial service, drawn from a wide range of sources and providers. A quote from a 'consumer expert' respondent to the Barclay's Report put it neatly:

> The interesting thing about this which is new, is it takes effectively a map of the industry, very data rich, it's got lots of products and so forth, and it also allows you to merge that with a map of the individual's either needs or actual products…and then effectively find pathways for the individual… The platforms may become the new form of adviser in a sense or at least the person you go to.

This infographic compares the existing relationship structure with the potential future on the right hand side:[7]



6 Barclays Bank; *OPEN BANKING A CONSUMER PERSPECTIVE*, January 2017
7 Nordea; *PSD2 and Open Banking;* 2017

What will it do?

One of the seductive things about OB is that the potential and possibilities currently seem limitless. Most of the actual applications to make it work or the companies that will exploit it have yet to be tested or born. As the Barclay's report notes:

> Open Banking has the power to revolutionise the way we manage our money, shop around and buy things. For SMEs, managing cashflow and receiving payments should be cheaper and easier.
>
> Technologies like Application Programme Interfaces (APIs) have the potential to create new services delivered by existing players and new intermediaries, like Personal Finance Management platforms. They have the power to bring substantial benefits to consumers, aggregating their financial products in one place; providing new insight about spending patterns; making recommendations about saving money; automating parts of the decision-making process and even offering new ways to pay.
>
> Open Banking could widen access to existing products, like credit, debt advice or financial advice. And bring new products to market from overseas or the UK, at the click of a button. Open Banking will make things simpler, quicker and more convenient.
>
> The innovation that new technologies make possible is endless and over time could create new forms of value we can't envisage today.[8]

Much work is now being carried on within the world of 'fintech' to envisage, build and test the sort of applications that would be of value for consumers. This is being carried on by both independent small firms and designers as well as by teams within the large banks. Primarily everything that will emerge will be mobile phone based. We do not know which of the current ideas will work, or be popular and there are surely things that have yet to be imagined but the sorts of things that could be developed include the following highlighted in the Barclays Report:[9]

> **Moneyhub** is a personal financial management tool which brings together in one place a customer's bank accounts, credit cards, investments, savings and borrowing, including property and pension. It gives users insight into their spending and helps them plan for the future.
>
> Users can access professional help via a direct connection to the Unbiased IFA directory. Customers can securely share their data with an adviser (if they have joined the Moneyhub network). Moneyhub allows customers to control which layers of data they wish to share or keep private through a simple consent platform.
>
> In turn, Moneyhub supports SMEs like IFAs and accountants who can use it with customers not familiar with it.
>
> **Credit Kudos** is a new type of credit reference agency. When someone with a limited credit history applies for a loan, they may find themselves rejected or offered a more expensive product. Credit Kudos allows consumers to securely share relevant information with a lender in order to get a fairer decision. Their platform instantly ascertains an individual's suitability by allowing an applicant to connect and share data directly from their online bank. It means that people who were previously excluded unnecessarily may be able to access credit. Credit Kudos aims to be quick and easy, allowing the user to choose what data to share in a secure environment without leaving a footprint.
>
> **SafetyNet Credit** is an online lending product with credit limits of up to £500 which competes with unauthorised overdrafts by offering a cheaper alternative. It uses a

---

8 Barclays Bank; *OPEN BANKING A CONSUMER PERSPECTIVE*; January 2017

9 Note these examples are representative of many others and there is no intent to endorse or otherwise the specific products or companies

> customer's current account data to carry out its affordability assessments both at the point of application and every seven days on all customers.
>
> If approved, a customer can switch on the automatic SafetyNet feature whereby in the event their bank balance breaches a level pre-set by the customer, money will be automatically deposited into their account, saving them incurring charges on an unauthorised overdraft.
>
> SafetyNet Credit automatically collects repayment from the account as soon as sufficient funds are paid into it helping the customer to reduce the charges paid in interest. It also provides its customers with a dashboard of their spending so that they can see how they are spending their money and make adjustments.
>
> **Bud** is an online and mobile platform which aggregates financial services, from traditional bank accounts to innovative fintech services. It provides a budgeting service and over time will use customer data to help them optimise their spending and use of products.
>
> Customers will be able to browse and select products and services through its app-store-style marketplace. Users can then connect these services to their Bud account creating their own bespoke 'bank' experience in one convenient platform. Bud gives exposure to new types of products, like Habito, a digital mortgage broker who have digitised the whole mortgage process.
>
> To help people connect seamlessly with other providers and buy products, Bud will offer a digital ID or 'Know your Customer' service."

Box 1: Regulatory Sandbox

For readers interested in possible upcoming financial service products based on new technology, the FCA's 'Sandbox' is the area where new ideas are tested by the regulator under strict conditions, with a view to assessing their regulatory potential. The list of the latest cohort of firms accepted by the FCA for testing can be viewed here.

As well as providing private sector benefits and goods to consumers, potentially there are 'public good' benefits too.

The first has already been mentioned, the opening up of the banking market to improve access and competition. One consultancy Report noted:

> Regulators are enabling third-party access and innovation through open strategies. While incumbent banks often feel under threat from nimble start-ups, the high cost of regulatory approval or a banking license has for a long time sheltered them from disruptive new entrants attacking their core business. Regulators around the world are using open banking as a means to remove this block, provide right of entry for innovators, promote competition, and drive better customer outcomes.[10]

In its Report into the retail banking market, the CMA proposed that if the top nine UK banks should create open banking standards it estimated that it would benefit customers by between £700 million and £1 billion.[11]

Secondly, with data spread across agencies there is potential for things like debt advice and help to be offered automatically, and at an earlier stage than it is often currently sought, and, a recovery plan based upon priority payments (rent, tax, utilities etc.) could be automatically calculated and communicated to the relevant creditors:[12]

---

10 Forrester; *The Open Banking Revolution Is Imminent*, February 2017
11 CMA; *Retail Banking Market Investigation*, August 2016
12 Barclays Bank; *OPEN BANKING A CONSUMER PERSPECTIVE*, January 2017

Following the go-live date (13 January 2018) the issue of security of data featured in several articles such as this from the Guardian - *Open banking? I think I'll be keeping my door shut*. Open Banking the CMA body set up to oversee the project states in its customers section of its website that:

> How can I use Open Banking securely?
>
> Open Banking is safe and secure. You have control of your data: you decide if you want to share it, you decide what data you want to share and you decide what it can be used for.
>
> Your data is encrypted and shared securely. All usage of your information is tracked and you should be able to withdraw your consent at any time.
>
> Every provider who uses Open Banking to access data must be regulated by the FCA in the UK, or the national competent authority in other European countries.

The Tech website 'WIRED UK' acknowledged the security issue but went on to say:

> From a technical point of view, Open Banking is at least as safe as online banking. APIs – the technology used to move the data – are trusted and the law requires account providers to use strong customer authentication, a procedure which allows the payment service provider to verify the identity of both the user and the service.
>
> Only startups that have been approved by the Financial Services Authority (FSA) will be allowed to use the system. However, just like online banking, increased movement of data does offer opportunities for scammers, who might try and trick people into sending over their data.
>
> The key thing to remember: anyone using an Open Banking service will not need to share their banking login or password with anyone but the bank. This is actually an improvement on existing services, which sometimes require this as a workaround for existing incompatibility.

> If something does go wrong with a payment, your bank should be able to help you get a refund. If someone misuses your data, then the case is subject to data protection laws and you will be able to complain to the Information commissioner.[13]

Fintech commentator Chris Skinner, in his blog - *The disappointing arrival of Open Banking … and the optimistic future* picked up on the negativity with which OB was initially greeted:

> "nearly all of the mainstream media greeted the launch of Open Banking with fear and scaremongering. These three headlines illustrate it well:
>
> Open banking? I think I'll be keeping my door shut, The Guardian
>
> Fraud fears over 'open banking' revolution, The Times
>
> Customers who sign up to 'open banking' revolution where they share details in the hope of better deals 'could be put at risk from fraudsters', Daily Mail
>
> Even *The Financial Times* jumped on the bandwagon:
>
>> Will you let a stranger look deep into your bank account?
>>
>> *Be afraid … be moderately afraid. Open Banking arrives on January 13, allowing "third-party service providers" to access data from your bank accounts online, if you give permission. It sounds terrifying, doesn't it?*
>
> Although after that opening line, the article does a good job of explaining that it is safe and secure and a good thing potentially. However, it started with such a negative tone and, with the ADD world we live in, that is likely to be all the reader remembers. In fact, the problem is that nearly every article I've read has greeted the development with a negative headline, even if the mainstream content is more balanced. As a result, no consumer is going to think Open Banking is a good thing and, with two-thirds of UK bank customers avoiding mobile banking and a third even running scared of internet banking, as they think it is insecure, I really cannot see how consumers are going to adapt to and accept the benefits of Open Banking.[14]

It is certainly the case that OB started with more of a whimper than a bang. However, there is a large and innovative Fin Tech industry which has received £billions in investment and this is its opportunity. Chris Skinner feels that they will not be quiet forever, but that things may not develop exactly as people first thought:

> the most likely outcome of Open Banking and Open APIs is that the big players will try to leverage more against their competition through data and the internet giants will gradually step in, with possible partnerships with the niche FinTech community, to create that compelling switch reason.
>
> For example, if Facebook is savvy enough, they would pickup with Stripe, TransferWise, Zopa and others to look for ways to make it easy for you to respond to their in-app advertisers, games and purchases and make it easy to get anything you want with a swipe. Add on to this that it's social and sharing, then I should be able to donate to friends' causes or pay my mates with messenger.
>
> Amazon and Alibaba are the two most likely global players who will get this first, not forgetting the other guys: PayPal, Tencent and more. It is these heavyweights working with niche lightweights that will change the game through Open Banking and, in the meantime, the ill-informed carping journalists can continue to kiss the banks' backsides.[15]

13 WIRED UK
14 Chris Skinner Blog 21 January 2018
15 Chris Skinner Blog 21 January 2018

The Project

Much of the project to introduce OB has been taken forward by the *Open Banking Working Group* which was established at the request of HM Treasury, in September 2015. Its focus has been to draw up the Open Banking Standard which sets common standards for the development of API based utilities.

There is another central OB body the *Open Banking Implementation Entity* (OBIE) which was set up by the CMA to further the goals expressed in the Review of PCAs through OB implementation. Its role is to

- Design the specifications for the Application Programme Interfaces (APIs) that banks and building societies use to securely provide Open Banking
- Support regulated third party providers and banks and building societies to use the Open Banking standards
- Create security and messaging standards
- Manage the Open Banking Directory which allows regulated participants like banks, building societies and third party providers to enrol in Open Banking
- Produce guidelines for participants in the Open Banking ecosystem
- Set out the process for managing disputes and complaints

It has produced technical information on specifications for API and OB standards here.

OB will apply to the following financial institutions: HSBC, Barclays, RBS, Santander, Bank of Ireland, Allied Irish Bank, Danske, Lloyds and Nationwide.

3. Payments Services Directive 2

To give it its full name the *Directive on payment services in the internal market (Dir 2015/2366)* is one of a long line of EU directives and measures which arguably go back to the EU's Financial Services Action Plan of 1999. It was transposed into UK law by *The Payment Services Regulations* 2017 (SI2017/752). It came into force 13 January 2018.

PaymentsUK, the eponymous industry body, says:

> the revised **Payment Services Directive (PSD2)**, requires all payment account providers across the EU to provide third party access. While this does not require an open standard, PSD2 does provide the legal framework within which the CMA requirements will have to operate, and the CMA mandate will need to be delivered in a way that is PSD2-compliant. It will keep customers safe and secure, enhancing the opportunities for enhancing customer propositions.

There is a standalone briefing on PSD2 by Payments UK and a joint Treasury/FCA publication *Expectations for the third party access provisions in Payment Services Directive II*.

The issue for the public is that they should be able to see real improvements in the range of service because of the joint PSD2 – open banking initiatives, without worries about the misuse of data. PaymentsUK says:

> New Payment Initiation and Account Information Services: PSD2 is expected to lead to a major change in terms of the accessibility of customer data to authorised third parties **when the customer has given their explicit consent**. Customers will be able to use payment initiation services and account information services where their payment accounts are accessible online, making internet and mobile payments easier and helping customers to manage their accounts and make better comparisons of deals.
>
> In addition, Payments UK anticipates that these changes will result in the development of products and services that allow customers to optimise the use of their account and transaction data. The value-added services which could result could easily go beyond payment and financial services and e-commerce. PSD2 could help open up new markets and encourage new market entrants, some of whom will offer services that will assist people who are currently financially excluded. There are a whole host of opportunities that it may not be possible to fully anticipate which could hugely benefit customers.
>
> PSD2 builds heavily upon existing consumer protection rules to help protect consumers against fraud, possible abuses and payment incidents through enhanced security requirements, including the use of strong customer authentication for electronic payments.

The two new regulated activities (see below) that will run OB are Account Information Services (AIS) and Payment Initiation Services (PIA) described below by the Financial Conduct Authority (FCA).[16]

Account Information Services

Under PSD2 an 'account information service' is an online service which provides consolidated information to a payment service user on one or more payment accounts held by that payment service user with other payment service providers. These services already exist in the UK.

Payment Initiation Services

[16] FCA website February 2017

Under PSD2, a 'payment initiation service' is an online service to initiate a payment order at the request of a payment service user from a payment account held at another payment service provider with the user's consent and authentication.

The new rules bring payment initiation services within the scope of regulation. They ensure that PISPs receive access to payment accounts and place requirements on them to ensure security for users. PSD2 will:

- bring PISPs within the scope of regulation
- ensure that AISPs can receive access to payment accounts
- place requirements on PISPs to ensure security for users

PSD2 also includes a ban on payment card surcharges – the frequent +2.5% paid by credit card users when they buy something online. It is estimated that surcharging cost British consumers £166 million in 2015.[17] There will be a public revenue cost to this measure in that the government has had to pass legislation to remove such charges from certain of its online services such as car tax.

[17] Gov.UK Press Release 13 January 2018

4. Regulation

The chief financial services regulator in the UK is the Financial Conduct Authority (FCA). Its role is to authorise and register, along with other European regulators, companies that wish to provide the basic services on which OB depends. These are the Account Information Services (AIS) or Payment Initiation Services (PIS) (see above).

The FCA and other European Regulators will add AIS and PIS providers to the registers they keep of all authorised businesses. These registers are publicly available.

The FCA's AIS and PIS webpage outlines the regulatory framework:

> **Our role in regulating AIS and PIS providers**
>
> We are responsible for ensuring AISPs and PISPs are registered or authorised. For businesses that only carry on account information services, there is an option to become a 'registered account information service provider'. These providers have no capital requirements and need to meet fewer conditions than authorised firms. Businesses that provide payment initiation services must be authorised and must have a minimum of €50,000 in initial capital (or higher if they provide certain other payment services). Both AISPs and PISPs have to hold professional indemnity insurance (PII).
>
> **Providing access to customers' payment accounts for providers of AIS and PIS**
>
> Businesses that provide 'payment accounts' that are accessible online to their customers will have to give AISPs and PISPs access to these accounts, with the user's consent and authentication. Under PSD2, providers of payment accounts are referred to as 'account servicing payment service providers' (ASPSPs).
>
> **Expectations for the third party access provisions in PSD2**
>
> The European Banking Authority has developed regulatory technical standards that introduce standards for common and secure communications between ASPSPs and AISPs or PISPs. These technical standards are expected to take effect from September 2019. We issued a joint communication with the Treasury which sets out our expectations of firms in the pre-RTS period.
>
> The joint communication also reflects our views around the use of application programming interfaces (APIs) standards, such as those being developed by the Open Banking Implementation Entity, as the basis on which secure access to payment accounts could be provided in future.

Aware of the likely public concerns over data security and yet wanting the public to be able to take advantage of OB, the FCA on its main OB webpage has the following advice and reassurance for individuals:

> **Giving consent for access to account data**
>
> When you sign up with a company for account information services, the AIS provider should give you enough information to understand the nature of the service being provided and how it will use your data, including whether it will share your data with anyone else.
>
> **Sharing security details**
>
> Currently, businesses that provide AIS and PIS often ask you to share your bank security details with them, such as your login and passwords.
>
> Under existing data protection law, these businesses must protect your data and PSD2 will require these businesses to put further measures in place to keep your credentials safe and secure.

Your banking terms and conditions should not prevent you from sharing your credentials with regulated AIS or PIS providers. Your bank cannot hold you responsible for unauthorised transactions just because you have shared your credentials with regulated AIS and PIS providers.

Unauthorised payments

If you notice a payment out of your account that you did not authorise, you should contact your bank as soon as possible. If you did not authorise it you can claim a refund. You should contact your bank to claim a refund even if you think a PIS was used to make the payment.

Making a complaint

You have the right to complain to an AIS or PIS provider if you have a problem with the service they are providing. They must respond to your complaint within 15 days unless there are exceptional circumstances.

If you are not happy with the firm's response, they reject your complaint or you do not hear from them, you have the right to take your complaint to the Financial Ombudsman Service.

If your complaint is about something your bank has done, for example if a bank has refused to refund an unauthorised payment, you should contact the bank to make a complaint. You have the same right to take your complaint to the Financial Ombudsman Service.

How to protect yourself

We want consumers to enjoy the full benefits that these changes can bring, however there are some important things you should be aware of.

– **Be alert -** you should be vigilant to fraud when using online payment initiation or account information services. If you don't know who you are talking to, or there is reason to suspect that the provider is not who they claim to be, don't disclose your banking security credentials, or other personal or financial information.

– **Read the details -** always read the terms and conditions of a provider of financial services carefully before signing up, this includes the terms and conditions of AIS and PIS providers.

– **Be data savvy -** make sure you understand and agree with what access you are granting to your account, how the account information will be used and who it may be passed to.

– **Check your statements -** keep an eye on your bank statements and get in touch with your bank if you don't recognise a payment.

Data protection

Companies that access your data need to comply with data protection law. Banks, building societies and other payment services providers, including AIS providers, will be subject to data protection law as well as the requirements of PSD2.

If you have a concern about a breach of data protection law, you can contact the Information Commissioner's Office.

Before you use one of these services be alert, and make sure you are confident that any organisations you share your information with are who they say they are. You should make sure that you understand the service and that you are happy with who will be providing it to you.

BRIEFING PAPER
Number 08215
26 January 2018

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.