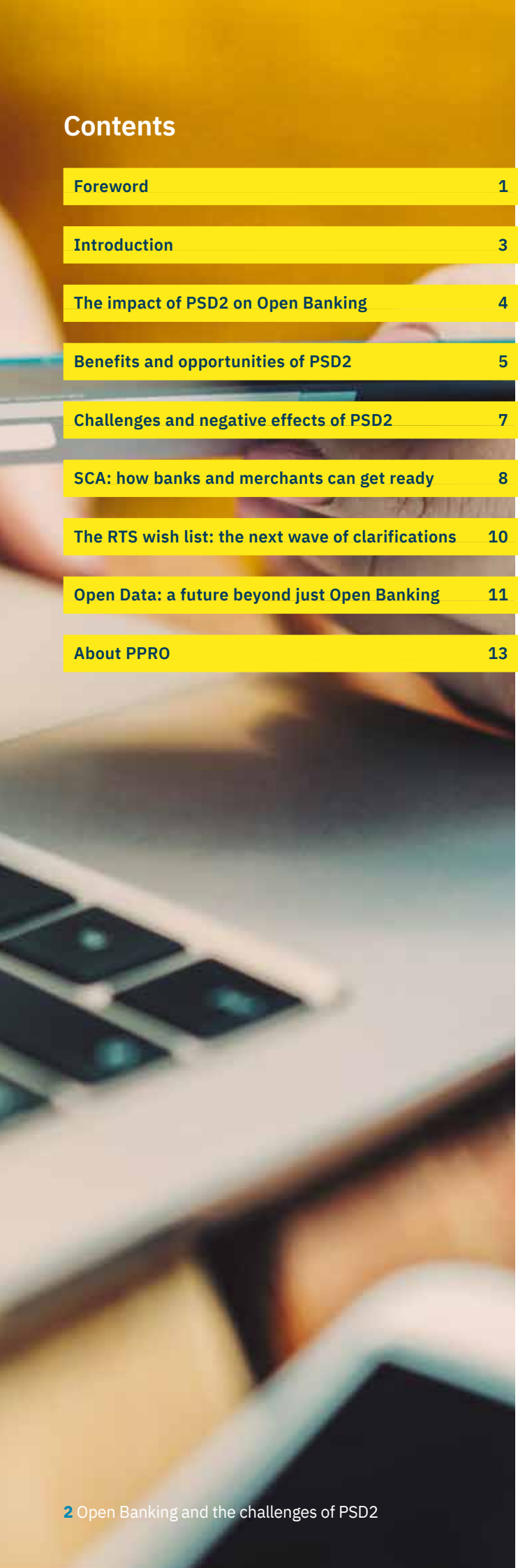
Open Banking and the challenges of PSD2

Building a frictionless European payments system

ppro

Contents



Foreword

Open Banking presents a hopeful vision for the future of the financial services sector. Thanks to the advancement of technology, we're seeing disruption to legacy banking systems, and a move towards a world of Open Data. This will enable customers across Europe to actively own their financial data and choose how they want to bank, save and pay.

With Open Banking, third-party providers (TPPs) can offer customers a wealth of new and automated services beyond their standard bank offerings, such as what products to buy or even advice on who to bank with. However, European banks and the financial sector still have work to do to reach this future.

I believe Open Banking and PSD2 will help introduce more innovative financial products and banking services than we've seen before. When implemented properly, Open Banking will foster a seamless Europe-wide payment system along with the rise of invisible banking and automated advice solutions that manage customers' money. There is so much opportunity in the fintech and Open Banking sector, now we just need to see how quickly we can get there, and what banks and TPPs can do together to move this process forward.

To help better understand this future, this whitepaper presents a detailed look at the Open Banking landscape, its benefits, challenges and the future.

Ralf Ohlhausen
Executive Advisor at PPRO and Vice-Chairman of ETPPA

Introduction

Fintech is currently the largest area for investment in Europe. According to reports, the sector receives 20% of all venture capital in Europe – that's a higher percentage than in Asia and the US. Much of this growth is driven by the increase in innovative third-party providers (TPPs) who have created digital banking experiences that allow customers to access, manage and view their money how, when and where they want to.

The goal of Open Banking is to allow customers to unlock their data and gain access to value-added financial services. Open Banking allows bank customers to use their bank account information, such as their account balance, transaction history and recurring payments, with third-parties, who may offer banking and personal finance services.

The revised Payment Services Directive (PSD2) came in to effect in January 2018. This built on many of the themes present in the earlier regulation, 2007's PSD1. Additional steps include making payments safer, increasing consumer protection and harmonising cross-border payment services throughout the EU.

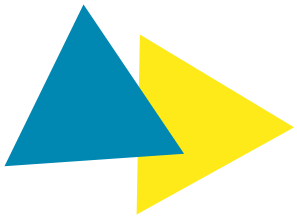
Drawing on expert advice and experiences from across the financial industry, including TPPs, payment providers and regulation specialists, this whitepaper will discuss how banks, merchants and TPPs can overcome the challenges of PSD2, prepare customers for the new world of payments and build a frictionless payment infrastructure across Europe.

Open Banking explained

About 15 years ago, we saw the first appearance of bank-independent payment initiation service providers (PISPs), which allowed customers to pay directly and in real-time from their bank accounts without needing cards or wallets. Similarly, account information service providers (AISPs) entered the scene, providing consumers and corporates with consolidated views of all their bank accounts.

To begin with, these service providers and their activities were not regulated and many banks and European governments resisted this type of competition. However, the potential to unbundle value-added services from core banking to increase competition and innovation in the banking industry was compelling. This led to PSD2 bringing PISPs and AISPs within the scope of regulation and supervision in return for mandating banks to grant access to customer data if their customers explicitly consented to this.

Open Banking applies to accessing any type of bank account. While EU payment accounts, which are the most exposed to fraud, are now specifically protected under the PSD2 regime, non-payment accounts fall under general regulations, such as GDPR.



The impact of PSD2 on Open Banking

The Open Banking movement in Europe coincided with the introduction of the revised Payments Services Directive (PSD2). This regulation aims to bring greater security and competition to the payments market.

What is PSD2?

The revised Payments Services Directive (PSD2) regulates payment competition and unites payment rules across Europe.

- **PSD2 requires EU member banks to give authorised, i.e. licensed TPPs access to customers' accounts either via APIs or their user interfaces**
- **It mandates the use of Strong Customer Authentication (SCA), which requires multiple factors of authentication from a customer, in order to initiate electronic payments and grant access to transaction data**

When does it come into effect?

- **PSD2 was passed in 2015 and came into effect in January 2018, as member states were given two years to transpose the directive into national law**
- **Several (level-2) Regulatory Technical Standards (RTS) were developed to detail the PSD2 (level-1) text. The most important of these became effective in September 2019**
- **However, the enforcement of SCA for card payments has since been delayed by 15 months to give merchants and providers longer to prepare for the roll-out**

What needs to be done to make Open Banking a more beneficial reality in Europe?

Ralf Ohlhausen
Executive Advisor at PPRO and Vice-Chairman of ETPPA

To make Open Banking a more beneficial reality in Europe we must improve the state of the API framework across the continent. The UK released its first Open Banking APIs in January 2016, 21 months before the rest of Europe, and is already using them in the market. Therefore the UK has a real head start on Europe, where hardly any APIs are being used today by the larger TPPs.

The shortcomings relate mainly to missing functionality and stability issues. TPPs have had a very hard time justifying their functional requirements as well as testing many hundreds of immature APIs. Persuading regulators to enforce access to missing functionality while also getting banks to develop sophisticated APIs is a challenging and, of course, lengthy process.

Hence, in addition to migrating all their services to APIs, most non-UK TPPs had to continue with their former practices in parallel, such as screen-scraping or reverse engineering. This meant gaining direct access via customer interfaces as opposed to going through an API, which will be much more efficient, if and when they work properly.

However, although the regulation is flawed in some ways, a harmonised regulatory framework across Europe is a big step forward and gives legal certainty to TPPs. It also reassures the end-customer as to the trustworthiness of the TPPs. These TPPs are regulated entities which, as far as payments are concerned, are now covered by the same regulation as a bank.

Benefits and opportunities of PSD2

While PSD2 was perhaps initially seen as simply a regulation exercise, it's led to the development of new, innovative technologies from many TPPs and a much-increased range of products and services for customers. Thanks to this innovation, Open Banking offers customers, banks, TPPs and retailers alike many benefits for the future of banking.

Although the introduction of the PSD2 regulation hasn't been seamless for the banking and fintech industry, it is set to offer many benefits and advantages for the end-customer, and the financial industry. Overall, the regulation will create an integrated and frictionless European payments system, that will provide the customer with more choice, control and security over their finances than ever before. The main benefits of the PSD2 regulation are:

Greater consumer protection and security

The primary goal of PSD2 is to provide greater protection against fraud for banking customers, who may have previously been open to risk through weak authentication and unregulated data-sharing practices. The new rules insist on enhanced security requirements, including the use of Strong Customer Authentication (SCA) to protect customers while making electronic payments.

Increased innovation

TPPs unencumbered by legacy technology have long been able to innovate faster than traditional banks. Now, this regulation will provide regulated and secure access to customer data, allowing them to develop products even more quickly. The new regulation promotes technology on a European level and encourages fintechs to do what they do best: innovate.

Wider choice of services for customers

This regulation increases market competition allowing customers to choose a wider range of suppliers for their banking and payment services without having to switch their bank for that. The growth and innovation in the sector will make it easier for customers to opt for the banking services that best fit their needs. It also increases the number of financial providers, services and products which customers will be able to choose from.

Increased access for third parties

PSD2 means TPPs will now benefit from a legal framework that supports their access to bank accounts if the customer wishes it. Meanwhile, banks will be prohibited from blocking access to third parties, other than for "objectively justifiable reasons".

A real-time Europe-wide payments network

In combination with Instant Payments, PSD2 will enable real-time bank transfer payment methods across all of Europe. From a customer perspective, this will allow anyone in Europe with a bank account to pay online and offline securely, by initiating the payments themselves easily without needing cards or wallets. Customers have full control of when funds are leaving their account without the need to disclose sensitive banking data. For merchants, bank transfer payments offer a very broad reach, instant confirmation, lower fees, higher security and no chargeback risk.

The balance of trust and convenience

The two main factors regulators always need to balance for greater customer adoption are trust and convenience. To illustrate this, we've highlighted two previous attempts at a version of Open Banking in the UK, which show the importance of having trust and convenience together.

In 2015, UK legislators tried to increase banking competition and trust with a project called MiData. Rolled out by the Government's Department for Business, Innovation and Skills, MiData was intended to give customers greater access to their transaction data in a portable electronic format. It was hoped this would make it easier for customers to compare current accounts and increase bank switching.

But this project relied on customers downloading their transaction data in a spreadsheet, which they could then upload into a comparison site. That's far from convenient. So, despite offering trust and flexibility, MiData didn't take off.

A few years later, UK policymakers tried again with the Competition and Markets Authority's 2017 market review into retail banking. One of the remedies suggested in this review was to mandate a data-sharing standard. This meant that instead of customers having to do the legwork and download a spreadsheet, fintechs could do the hard work and present information to customers in neat and convenient dashboards. Of course, this is convenient and flexible, but with unregulated TPPs accessing accounts, customer trust was a stumbling block.

Following these two projects, the introduction of PSD2 was a really timely measure to ensure not only trust, but also the convenience of automated data sharing, which now only happens between fully regulated and supervised entities. Therefore, PSD2 addresses both the issues of trust and convenience, making this a much more tenable proposition for end-customers.

Making the switch to Open Banking: the view from a third-party provider

Thomas Catchpole
Open Banking Lead, Account Technologies

At Account Technologies we create products that link to bank accounts and provide services that banks can't offer their customers. To operate our services, we need to present the customer with their bank balance and transaction data.

Before PSD2, we managed our customers' accounts through screen-scraping. Using the customers' online banking details — username, password and memorable information — to log in to their account on their behalf. From this data, a company can provide a number of services, for example automating mortgage applications or a safety-net overdraft. But, as you can imagine, asking a customer to give those credentials did cause quite a few people to close our application form down there and then.

But now our process is regulated. To get ready for the introduction of PSD2, we moved all our customers across to Open Banking and replaced screen-scraping with APIs. This means using a redirect model, where the customer authenticates their details with the bank during the application process. Essentially, they say, "I'm me and yes, I do give Account Technologies permission to view my data".

This transition means that the customer does not need to share their online banking login credentials with another party improving the security of the whole ecosystem.

One of the elements that the PSD2 regulators got spot on was the requirement for Account Servicing Payment Service Providers (ASPSPs) that have an app to offer an app-to-app model for authentication to TPPs. As a lot of people now bank within an app, rather than putting in a username + password + OTP, we can just send the customer to their banking app. They scan their fingerprint, select their account and they are authenticated. When banks started to roll that out, we saw a huge improvement in our conversion rates, we've almost doubled our acquisitions, from 8,000 new customers per month to 14,000 per month.

For us, the transition to Open Banking is a significant improvement to customer security and to the baseline technology that underpins our customer facing products. The services we are able to offer off the back of Open Banking in the future will improve and ultimately it provides a better customer experience and a far better interface than the tech we used before.

Challenges and negative effects of PSD2

Despite the progress of PSD2, there are still challenges to overcome to achieve widespread adoption and to meet Open Banking objectives. Two areas of the regulation that need to be improved are:

Delays to API development

One of the major factors in the UK regulator's decision to postpone the enforcement of the RTS to March 2020 was because not all the APIs were available or functional in time. These APIs are the technology that TPPs rely on to migrate their services and customer base and remain PSD2 compliant.

One of the contributing factors was that the Regulatory and Technical Standards (RTS), which apply to PSD2, left room for too many different interpretations. This ambiguity caused banks to slip behind and delay the creation of their APIs. This delay hindered European TPPs in migrating their services without losing their customer base, particularly outside the UK, where there has been no regulatory extension and where the API framework is the least advanced.

Increased customer education

Levels of awareness of the new regulations and changes to how customers access bank accounts and make online payments are very low among consumers and merchants. This leads to confusion and distrust of the authentication process in advance of the SCA roll-out. Moreover, because the majority of customers don't know about Open Banking yet, they aren't aware of the benefits. Without customer awareness and demand it may be very hard for TPPs to generate interest and uptake for their products.

Who is responsible for increasing customer education towards PSD2 and SCA?

So far there hasn't been a significant drive to raise awareness and educate the public or retailers on PSD2 and SCA. According to research from Mastercard, 75% of retailers still aren't aware of the incoming SCA process for payments.

Online searches for 'open banking' and 'data security' reveal many falsehoods and misinformation. As an end-customer, how do you know who to trust? So, whose responsibility is it to make sure consumers and merchants are aware of the new regulation and the changes they will experience in their online retail banking journeys?

The banks

Recently some regulators and banks, such as the Central Bank of Ireland, have made decent efforts to raise awareness of the changes with PSD2 campaigns. But it isn't reaching the general public. When it does, it's often because of scaremongering or fear, uncertainty and doubts around data security fuelled by incumbents to protect their business. This also isn't the right way to approach the issue as it will lead to people being more afraid, rather than aware. Instead, it is the role of payment service providers to educate their customers about Open Banking requests or opportunities, to ensure the public are aware of the changes to payment authentication procedures when SCA comes into play and are empowered to move their data.

The third-party providers

TPPs have a real vested interest in getting customers on board with Open Banking. They should build on their customer relationships to grow trust and raise levels of education around the changes.

When customers sign up for a new service, TPPs need to tell them explicitly what to expect before they have to do it, plus what explicit consent is required to access their account information in exchange for value-added services.

How will Brexit impact Open Banking for UK-based banks and fintechs?

In the immediate future, there will likely be no significant impact to Open Banking in a post-Brexit UK. The FCA has been quite clear that the PSD2 regulation, including the RTS, must still be implemented and followed after the exit from the EU. But it is possible that regulation will start to diverge thereafter. Whether the UK will adopt a Europe-wide PSD3 or an RTS2 in the same way, for example, is unknown.

Many financial institutions are now looking at owning local bases to deal with this issue in the future.
But the UK has been a leading party in the drive towards Open Banking, particularly the technology to support it.
For now, it is important that the UK and all of Europe are setting out from the same starting point in the Open Banking race.

SCA: how banks and merchants can get ready

What is SCA?

As part of PSD2, the new Strong Customer Authentication (SCA) provisions aim to reduce fraud in electronic payments. With the introduction of SCA, a customer must complete a two-step verification process before a payment can be made. This ensures that the person carrying out the payment transaction is who they claim to be.

SCA is defined as two or more of the following:

- **Something you know, such as passwords or PINs**
- **Something you have, for example a smartphone or cryptographic device key**
- **Something you are, such as biometric factors including fingerprint or iris scans, face or voice recognition**

It is important to note that some credentials are transmittable via APIs (PINs or one-time passwords), and some are not (biometrics), while some credentials are static (PINs) or dynamic (one-time passwords). To enable automated account information services without the customer present, AISPs are allowed to store customer credentials, but that can only work with transmittable and static credentials or alternatively, bank provided tokens specific to the account. PISPs are not allowed to store any credentials. A customer presence is required and banks mainly use dynamic credentials instead.

What requires SCA?

SCA is required in three situations:

1 Payments SCA

When a customer makes a payment, they will now have to authenticate using at least two of the three factors explained above. A similar process was known in the card industry as 3D-Secure, but usually circumvented by merchants voluntarily taking the transaction liability to prevent online basket abandonment. Industry participants were given an additional 15 months until the end of 2020 to adjust their processes, before SCA will apply to card purchases made online.

Conversely, PISPs were not given this extension and are therefore at a severe disadvantage during this period, because they have had to apply SCAs since September 14th.

2 Account access SCA

This provides access into a bank account for balance and transaction data. Although only legally required every 90 days, banks can request it every single time, and many do so, which is probably the biggest impact PSD2 has had so far, much to the annoyance of the wider public. The UK and France have delayed this for a few months, but it has already been implemented in all other countries since September 2019.

3 Renewal SCA (for account access)

The authorisation for account access has to be renewed at least every 90 days. Because this creates a major obstacle to the provision of automated account information services on multiple bank accounts, AISPs are of the opinion that this SCA renewal should be done by themselves rather than having to rely on the bank's credentials. The regulator's final verdict on this issue is still outstanding.

SCA exemptions

The regulation foresees various types of exemptions for lower risk use cases, where banks are allowed, but not forced, to skip the use of SCA, e.g. for payments below €30 or to trusted beneficiaries. Since SCA is seen as a conversion killer, merchants have a very strong interest to maximise the use of such exemptions, which requires a) that the criteria of the regulation is fulfilled, and b) that the bank is willing to waive the SCA option, where the latter is likely to require some 'incentivisation'.

Case Study

What TPPs and banks need to do to get ready for PSD2 and SCA

Jack Wilson
Head of Policy and Regulatory Affairs at TrueLayer
(speaking in November 2019 on PSD2 and Open Banking implementation in the UK)

The FCA's 'adjustment period'

In September 2019, the UK's Financial Conduct Authority (FCA) acted on market feedback by announcing a 6-month 'adjustment period', where it wouldn't enforce aspects of SCA for online account access. This was so banks could continue to allow third-party providers to continue accessing customer accounts via screen-scraping, to give these TPPs extra time to transition to bank APIs. But, if TPPs and banks delay this work any further, then we've got another cliff-edge post 14th March 2020.

What should TPPs and banks be doing in the adjustment period?

Banks need to complete the building of their APIs, well in advance of 14th March, so TPPs have a good chance to establish connections and complete live testing. Banks also need to be transparent about their timelines and configurations so TPPs know how to make the connections.

TPPs need to migrate to the APIs sooner rather than later. It will take time and effort to live-test the connections and then transfer customers across. TPPs also need to bear in mind that the banks will require identification via eIDAS certificates.

Making APIs work

The FCA and other regulators need empirical evidence to inform their supervisory work, and any future policy development. There is a whole framework of reporting requirements for PSD2. Firstly, banks must provide statistics on availability and performance of their dedicated interfaces to the FCA using the 'REP020' form. This will be used to assess whether banks APIs are performing as well as their online banking apps.

On the other side, TPPs are able to send a notification using the 'NOT005' form to the FCA every time there's an outage with an API relating to a specific bank. This will help the FCA build a league table of the best performers and worst offenders, so they can take action against them for not meeting PSD2 requirements.

Customer journeys and PSD2 obstacles

Good customer journeys are key to persuading consumers to start using Open Banking services. In the UK, the FCA has strongly supported 'redirection', where the customer is sent to their bank to provide credentials, rather than giving them to the TPP. Done well, this can encourage trust and take-up amongst consumers.

However, some banks interpreted PSD2 to mean that strong customer authentication would have to be obtained multiple times in any single customer redirection journey, creating major friction for consumers (which wouldn't be present in card journeys).

Thankfully, the FCA put out some specific guidance to address this potential obstacle. They advised that they see no good reason for such 'double SCA'. The UK is one of the only countries in Europe where this position has been taken. Other countries still have very prolonged SCA journeys, adding to friction and putting customers off Open Banking. So, clarification on this process needs to happen across Europe.

Jack Wilson is Head of Policy and Regulatory Affairs at TrueLayer. TrueLayer builds technology that allows third-party applications to access their users' financial data and initiate payments securely. Jack is a former policy adviser at the UK banking regulator, the FCA. There he led work to create the FCA's approach to regulating firms under the new Payment Services Directive (PSD2). Latterly Jack led the FCA's team assessing banks' readiness for Open Banking, focusing on their Open Banking interfaces (APIs) and customer journeys.

The RTS wish list: the next wave of clarifications

As this report has highlighted, not everything about PSD2 and its Regulatory Technical Standard (RTS) is perfect, and any regulation is unlikely to resolve all situations perfectly first time around.

So, what must be done to make the PSD2 regulation fit for the future? **Ralf Ohlhausen**, *Executive Advisor at PPRO and Vice-Chairman of ETPPA* and **Tom Catchpole**, *Open Banking Lead at Account Technologies* share their wish list for the elements that need to be improved and clarified.

Remove account access and renewal SCAs

SCA is a really useful requirement when significant risk is involved. Within PSD2, this applies to the authorisation of payments, both for cards and PISPs. You can argue that granting TPP access to a bank account should require SCA, similar to a direct debit mandate.

But, renewing that authentication mandate every 90 days, or needing an SCA every time you access your bank account is a major nuisance and not sufficiently justified by any risk mitigation. Had the regulator foreseen all the unintended consequences of it, I am pretty sure that the account access-related SCAs, or at least the recurring ones, would not have been stipulated.

Continuous Payment Authority integration

I completely agree with the comments Ralf made and think, for almost all AISPs, it is vital that the regulators address 90-day re-authentication, as this will be a severely limiting factor to the scalability of all AIS services.

On the payments side, I think the regulators missed a significant detail in the creation of PSD2 + RTS: Continuous Payments Authority (CPA). To make Open Banking seamless for customers across all possible digital services and a real rival to card payments, TPPs need to be able to do everything they currently do with cards via Open Banking APIs. Let's imagine that a customer issues a company permission to move payments of any amount, at any point.

That's something that we already use today via our bank cards for streaming entertainment or paying our mobile phone bills. Users authorise bank details once, then charge up services they want to buy later. The service will take payment when you purchase it, but it can also take amounts when you're not present, dependent on usage (if you go over a certain allowance, for example).

The Open Banking Implementation Entity (OBIE) is looking into sweeping type services and how a Variable Recurring Payment (VRP) offering could work and be standardised. However, if banks don't deliver VRP, it will be a real shame, as it could be a great enabler to some quite brilliant services.

A potential PSD3 needs to cover that space for TPP services.

No mandatory redirection

A dramatic impact on conversion has been observed by many TPPs due to imposed redirections, which removed their ability to design best-in-class, low-friction user experiences and also slowed down the payment flow. For TPPs that want to offer their own user experience, redirection is a severe obstacle.

Furthermore, redirection is technologically infeasible on any device other than PCs and smartphones, and therefore blocks TPPs from offering their services on all other devices such as Point-of-Sale (POS) terminals, wearables such as watches, smart speakers, etc.

Therefore, it forecloses the whole physical retail market and the whole new Internet-of-Things arena, preventing innovation and competition for creating pan-European retail payment solutions (also at physical POS).

Consequently, redirected authentication can only be optional, not mandatory, and APIs must support the so-called embedded and decoupled methods as well.

Premium APIs

As a TPP, we need live feeds of a customer's bank account activity. Currently, we just pull this account data, such as direct debits, bank transactions or balance information, several times a day. Technically, that's a waste of time.

Instead, if a bank were to share an automated feed of a person's account – for example, push us a notification when a customer's balance has changed with an option for us to fetch a new balance (all with respect to the customer's consent) – it would make the whole system so much more efficient for everyone; TPPs, ASPSPs and the products the end user gets would improve significantly.

That's not something that's legally mandated under PSD2, but if banks offered TPPs these 'premium APIs', Account Technologies would pay for them. Also, I expect a portion of the revenue this generates for the banks being put back into the premium and regulatory APIs improving the service for everyone.

In my opinion incentivising banks to start pushing beyond the regulatory minimums to deliver premium service is best for all parties and is the next stage in Open Banking's development.

> “Over the next decade, we should expect to see consumers able to actively own their data”

Open Data: a future beyond just Open Banking

The Open Banking revolution has not only transformed the European financial sector, but also set us on the road to Open Data. This incentive will empower the customer to be the owner of their own data and allow access to, and sharing of, that data with which ever third-parties or suppliers they believe offers them the best service.

If, for example, a customer decides they want to move all their emails from Gmail to, say, a BT email programme, then they should have the option to be in charge of where they keep their data. Similarly, if a customer wants to switch their car insurance, with Open Data, instead of filling in long forms on a comparison site, they could just provide their car insurance access credentials to a comparison service, who could then instantly manage the process for them.

All the data that we have buried inside tech providers across the internet should be made available on request. There are a few adaptations to our General Data Protection Regulation (GDPR) desirable to make this easier, but it already provides the legal basis for this mechanism, i.e. allowing controlled access to our big tech data. This means in the near future, there will likely be TPP services that allow that to happen.

To deliver this future in the best way, big tech organisations such as Google, Facebook, Amazon or Apple should ideally provide API access to their customers’ data. Just as with Open Banking, this will not happen overnight. In payments, thanks to PSD2, we now have a regulated environment where banks are strongly motivated to provide APIs. Outside the banking regulation, we need to incentivise tech companies to voluntarily create a similar API-based shared data framework, and the only way to grant that incentive is to allow direct access via their user interfaces as an alternative way to unlock their customers’ data. In the absence of APIs, credential sharing and direct access will be the key enabler for secure data sharing.

Thanks to Open Banking, the ability to share data securely in the retail banking sector has led to a sophisticated ecosystem where the customer is in charge of their payments and choice of banking services. Over the next decade, we should expect to see the same level of transformation in our digital services and data sharing, leading to a complete rebalance of services where customers will be able to actively own their data.

Europe is currently ahead in the race for Open Banking, so the successful implementation of PSD2 and SCA is extremely important to keep that lead and build a future with Open Finance and Open Data as well.

Local payments. Worldwide.

PPRO is the world's leading local payments platform-as-a-service, removing the complexity of domestic and cross-border payments for top-tier financial institutions, payment service providers, and their merchants.

PPRO provides partners with the ability to accept locally preferred payment methods like e-wallets, bank transfers, cash, and local cards in more than 175 countries across the globe. Through one contract and one API.

PPRO's powerful platform does it all – processing, collecting, reconciling, reporting, settling funds, and more – and we've got market experts in every region so that partners can turbocharge their speed-to-market and increase conversion in every corner of the world.

Founded in 2006, PPRO is a global financial institution with an e-money license issued by the British regulatory body FCA.

How PPRO can help you

Payment service providers

Get access to local payment methods and payment-related services under a single integration and single contract to accelerate and simplify your merchants' go-to-market strategy.

Local payment methods

Reach a global audience of local and cross-border merchants through our payment service provider partners.

Merchants

Increase your reach and revenue by offering consumers their preferred payment methods in every market, domestic and cross-border.

Contact us

www.ppro.com/contact
info@ppro.com

ppro
Local payments. Worldwide.