

How banks can build trust in a PSD2 world

White Paper

The catalyst for change

Ten years after the introduction of the Payments Services Directive, (PSD) the European payments ecosystem is taking the next step in its regulatory evolution in the form of PSD2 - and it is set to disrupt the payments landscape in a far more radical way than its predecessor.

The second iteration of the Directive is motivated by the same ambitions as the first – to drive payments innovation and data security by reducing competitive barriers, mandating new security processes and encouraging standardized technology. The rapid technological advancements and

digitization of payments in the last decade have driven the need for updated standards – to bring more payment types, methods and players into scope to reduce fragmentation, address rising ecommerce fraud rates and prepare for the digitally transformed future.

There is no doubt that PSD2 will create significant benefits for consumers, as well as interesting prospects for merchants and FinTech companies, who will be able to explore new revenue streams and customer interaction opportunities. At the same time, the Directive also presents a range of challenges for banks who must now address not only the new compliance standards, but also find their place in the new world - evolving to ensure they

retain a strong connection to their own customers.

With more and more sensitive information being shared between consumers and businesses - and the increasingly digital nature of these customer relationships - it is no surprise that data access security and customer authentication are big features of PSD2.

In this paper, we will focus on one of the biggest issues for banks – the new regulations around Strong Customer Authentication (SCA). We will highlight the challenges posed and explore how banks can go beyond simple compliance to build trust and create a smooth experience for all users.

Our Specialists

Christophe Brunet, Global Product Manager

Christophe Brunet has worked as a Product Manager since June 2015. Previously he was the technical manager responsible for trust and security products, such as electronic signatures, secure archiving, and PKIs. And in this role, on several occasions he supported national and international certification processes (CSPN, RGS, Common Criteria, ETSI, PCI). He also worked on the online payment solution by Worldline: Sips.

Julien Gabillet, Global Product Manager & Intl. Business Development

Julien is responsible for Product management of Innovative payment and Strong Authentication solutions. He also drives international business development related to his product portfolio.

Sylvie Calsacy, Head of Payments Strategy

Sylvie joined Worldline in 2012 where she had several positions being responsible for the SEPA product line and development of new business areas in relation with Online Banking. Before joining Worldline, she worked for Groupe Crédit Agricole, initially in investment banking then she got a position as liquidity manager and global treasurer for insurance companies. She holds a Master in Financials at the ESCE French business school and holds a graduation in financial analysis at the SFAF.

Michael Salmony

Michael is Executive Adviser at Worldline SE, Europe's largest payment provider, which processes over 17 trillion Euro per year. He is an internationally recognized leader on business innovations especially in the digital and financial services space. He is board-level advisor to major international banks, industry associations and European bodies. Previously he was IBM's Director of Market Development Media and Communications Technologies and studied at Cambridge University, UK.



PSD2 RTS on SCA for ASPSPs

Deciphering the acronyms

PSD2 will introduce a host of new roles for different organizations to play in the payments process. The most important part of the Directive is the introduction of two new roles as Third Party Providers (TPPs) in the banking ecosystem: Payment Initiation Service Providers (PISP) and Account Information Service Providers (AISP).

Both roles are open to current and new players - and banks, or Account Servicing Payment Service Providers, (ASPSPs) will be required to support these new service providers if their customers want to grant them access to their account (either for information purposes or to initiate a payment). This is commonly referred to as 'Access to Account' or XS2A.

The Regulatory Technical Standards (RTS)¹ on Strong Customer Authentication are designed to standardize data security policies and improve adoption of strong customer authentication processes to ensure that whatever the customer payment journey, their information is protected and the risk of fraud is minimized at every point.

Under PSD2 (article 97), SCA applies to a wide range of payment transactions where the payer:

- accesses their payment account online;
- initiates an electronic payment transaction; or
- carries out any action through a remote channel which

implies a risk of payment fraud.

This also applies to any transactions or account access which is initiated via a TPP.

In the context of PSD2, SCA means that a payer must authorize his payment transaction using two out of three independent authentication 'elements' which, in turn, generate a one-time authorization code which is dynamically linked to the transaction.

The three authorization elements consist of:

- knowledge (i.e. something only the payer knows, such as a password or PIN);
- possession (i.e. something only the payer possesses, such as a token or smart device); or
- inherence (i.e. something that is inherent to the payer, such as biometric characteristics).

These elements must be independent from each other, so that a security breach of one will not compromise another.

With the responsibility sitting firmly with ASPSPs to provide these authentication methods, offer robust XS2A and support comprehensive monitoring and reporting processes, banks certainly have their work cut out to meet the new standards - with a host of considerations to factor in to their approach.

Addressing authentication challenges

What the RTS means in practice

One of the biggest challenges around the RTS for SCA is the broad scope of use cases which it covers – both in terms of the variety of transaction type and the breadth of different users who will now be involved in accessing bank accounts.

Supporting XS2A

The access to account requirement is disruptive in several ways: it imposes operational risks and costs on the banks, since they are responsible for finding secure and efficient ways to provide access for a potentially huge number of diverse TPPs. Banks will also continue to be liable for all transactions, including those initiated by a TPP – making it even more important to manage the authentication process effectively.

The explicit requirement in the RTS is that banks must offer a dedicated interface that manages account access for TPPs based on common and secure communication standards. For some, this will involve creating a new interface which is separate from their direct customer channel. Others may consider opening up their customer portal to TPPs. There are, however, a number of factors to consider in this process. For instance, banks who already have a functioning SCA setup need to evaluate whether their solution can handle the significant increase in transactions generated through potentially thousands of new TPPs – especially since this volume will be very unpredictable to begin with.

Underpinning the user experience

Under the new rules, banks must be able to provide compliant authentication processes that meet the needs of 100% of their customers – whatever their journey and whatever

method of access or payment they choose. This, of course, means that banks need to evaluate what types of SCA they offer and consider extending that range to support more flexible authentication strategies and better user experiences.

The challenge here is two-fold. Firstly, banks must be able to easily integrate highly secure, relevant, user-friendly authentication methods for their customer groups (including for TPP access). They must also find a way to efficiently manage a global SCA strategy and processes at the back end, while remaining flexible enough to change these strategies and authentication methods as market trends and technology evolve.

Reducing friction

There are also a number of other complexities that banks need to manage effectively to ensure that friction is minimized and that authentication processes run smoothly.

Firstly, there are a number of exemptions to the rules on SCA. For example, transactions such as low value contactless payments, fees paid at unattended transport or parking terminals and payments to 'trusted beneficiaries' do not have to go through SCA processes. There is also an opportunity to apply exemptions to payments identified as low risk based on a bank's real-time risk analysis and transaction monitoring solution. This exemption will only apply if the payment amount does not exceed a value between €100 and €500, depending on the payment service provider's reference fraud rate.

To promote a frictionless payments flow, it is therefore vital for banks to easily manage the full range of exemptions. They have to deploy highly accurate fraud scoring tools and lower their fraud rate to be eligible to RBA and allow more transactions to bypass the SCA process.

Lastly, there is a requirement for banks to ensure their authentication services are fully resilient, and to provide a back-up user interface for TPPs, to prevent any downtime and the resulting impact on customers.

Of course, the biggest challenge of all is that banks must consider what all of this means for their resources, costs, customer experience and brand reputation – and to weigh up all the options to achieve compliance whilst protecting relationships.

Balancing security, cost and customer experience

Worldline has extensive experience delivering comprehensive payments, authentication and risk management solutions to players across the payments ecosystem. It is from this experience that we understand the huge challenges involved in balancing security and customer experience with cost.

We believe that the key to achieving this balance in the context of SCA for PSD2 is to deploy an adaptive approach to authentication using Risk-Based Authentication (RBA) of transactions. By utilizing RBA, banks can help to keep their fraud rates in check to minimize losses and avoid penalties. But, by using sophisticated fraud scoring and data profiling tools, banks will be also able to support a higher volume of frictionless transactions - helping to deliver a good customer experience and reduce the costs of authentication by only deploying SCA processes for higher risk transactions.

Lastly, by utilizing RBA as a core part of their new approach to authentication, banks can position themselves well for future developments, such as the pending introduction of 3D Secure 2.0 which also supports a strong RBA approach.



Building trust

Taking authentication beyond compliance

At Worldline, we understand that building trust is critical for banks. But we also believe that trust is about more than payments security. It is about the ability to support secure transactions that are also fast, simple and consistent - creating a seamless digital banking experience that shows customers you are an organization they can rely on.

This kind of trust is what helps to build relationships and brand reputation, keeping customers loyal and encouraging growth. To achieve this in today's consumer-driven world, banks need to utilize solutions that are robust, work in real-time, across multiple channels, using recognizable processes and transparent communications. These principles are ones which banks must keep top of mind as they make any changes to services and systems.

The tenets of PSD2 will naturally encourage increased transaction and data security, as well as providing more payment and account access options for consumers. But, what it won't achieve through pure compliance alone, is to guarantee the convenient, fuss-free, fast, consistent payments and banking experiences that today's digital savvy consumers demand.

In developing their approach to SCA, there are several elements which we believe banks must address to ensure that they can protect their relationships by providing a trusted experience.



Managing the authentication process

From working closely with clients in the banking sector, our experience is that a common platform that can centralize authentication strategies is a valuable asset to banks who need to provide smart, consistent authentication processes across a variety of use cases, customer types, authentication methods and exemption cases.

Given the complexity of all the variables presented by PSD2, having a single platform with built-in workflow management will help banks to have greater control, flexibility and visibility over these processes, enabling them to be consistent across all user interactions and agile enough to respond to change.

It will also be vital for banks to ensure that their authentication platform is built using secure and robust infrastructure, including the ability to manage the growth of new authentication requests generated by the influx of new TPPs. Resilience is, of course, a requirement of the Directive, but it is also necessary to protect customer relationships – whether transactions are conducted directly or via a TPP. Banks need to make sure they have built in fail-safes and a robust, resilient first line solution for all their interactions to ensure that they maintain that consistent experience.

Choosing the right authentication methods

Banks must consider which authentication methods will provide the best user experience based on a variety of factors, including customer familiarity and convenience, as well as how they can be delivered in line with the requirements of the RTS.

We strongly believe that mobile can and should play a central role in customer authentication strategies. With smartphone usage playing an increasingly important role in the day-to-day lives of consumers around the world, mobile can offer a convenient, cost-effective and familiar route to support a variety of authentication options.

Biometry is set to take an important part in the future of payments and data security – it is also a method of identification which consumers trust and are becoming more and more comfortable with. Biometrics also address the third element of authentication – inherence – and are currently difficult for fraudsters to compromise, making these measures a strong choice for banks to invest in.

Whichever authentication methods banks choose to deploy, it will be vital to maintain a strong roadmap of development and to ensure that authentication platforms have the scalability and adaptability to respond to new innovations and deploy new authentication methods with ease, as technology, consumer preference and fraudster strategy changes.



Milan, Italy

Worldline support to deliver *a trusted user experience*

Building on our longstanding experience in security and certification processes, Worldline have worked closely with players across the industry to develop a range of complementary solutions which can help banks meet their PSD2 SCA

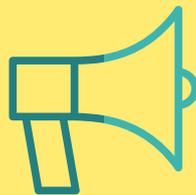
obligations cost-effectively while keeping customer experience top of mind.

In 2017 Worldline secured almost half a billion transactions for millions of consumers across 20 countries, via the following key solutions:

WL Access Control Server: supporting 3D-Secure regulation, including 3D-S 2.0

WL Authentication Process Management: providing effective management of different authentication processes – including RBA - and their related authentication methods, in full compliance with PSD2 requirements.

WL Trusted Authentication: powering authentication of any kind of digital service or software-based solution, including biometric recognition.



Closing Remarks

By opening the access to the account data, PSD2 should foster creativity and considerably expand the range of digital services on offer to customer from banks and non-bank players. This will naturally increase the need for Strong Customer Authentication.

As a digital service provider, you will need to find the most appropriate way to address this PSD2 challenge for your business. In doing so, there is a good opportunity to improve and rationalize your customer authentication strategy.

Built on 45 years of experience in securing electronic transactions, Worldline's comprehensive range of solutions can help you address your PSD2 challenges, whatever your specific needs.

About Worldline

Worldline [Euronext: WLN] is the European leader in the payments and transactional services industry and #4 player worldwide. With its global reach and its commitment to innovation, Worldline is the technology partner of choice for merchants, banks and third-party acquirers as well as public transport operators, government agencies and industrial companies in all sectors. Powered by over 20,000 employees in more than 50 countries, Worldline provides its clients with sustainable, trusted and secure solutions across the payment value chain, fostering their business growth wherever they are. Services offered by Worldline in the areas of Merchant Services; Terminals, Solutions & Services; Financial Services and Mobility & e-Transactional Services include domestic and cross-border commercial acquiring, both in-store and online, highly-secure payment transaction processing, a broad portfolio of payment terminals as well as e-ticketing and digital services in the industrial environment. In 2020 Worldline generated a proforma revenue of 4.8 billion euros.

worldline.com



For further information
sales-fs@worldline.com



Worldline is a registered trademark of Worldline SA. September 2021
© 2021 Worldline.