OneSpan

PSD3 in focus: The evolution of SCA and APP fraud prevention requirements

Update on proposed regulatory changes

WHITE PAPER JANUARY 2025

Contents

Introduction

Digital banking and payment services regulation in the European Union is currently undergoing a major overhaul. New types of banking and payment fraud are rapidly increasing and have driven European regulators to review and adapt PSD2, the payment services directive that currently applies.

In this paper, we discuss the current state of this regulatory overhaul, focusing on upcoming legislative changes in the areas of strong customer authentication (SCA) for digital banking and payments on the one hand and prevention of authorised push payment (APP) fraud on the other.

What happened so far

On 28 June 2023, the Directorate-General for Financial Services (DG FISMA) of the European Commission published its long-awaited draft proposals for a Directive on Payment Services and Electronic Money Services (PSD3) and a Regulation on Payment Services (PSR), the long-awaited successors of the revised Payment Services Directive (PSD2).

Subsequently, the review process by the European Parliament and Council kicked off. In November 2023, the European Parliament's Economic and Monetary Affairs Committee (ECON) published draft reports on the proposals with recommendations for amendments. On 14 February 2024, ECON voted to adopt both texts. Finally, on 23 April 2024 the European Parliament voted to adopt both texts in plenary, closing the first reading.

A few days later, on 29 April 2024 the European Banking Authority (EBA) published its Opinion on new types of payment fraud and possible mitigations. In this Opinion, the EBA notes that fraudsters are shifting fraud techniques toward APP fraud. It also comments on the draft proposal of the European Commission and proposes various additional security countermeasures to increase protection against APP fraud.

The European Parliament has adopted PSD3 and PSR, introducing enhanced measures for strong customer authentication and combating authorised push payment fraud.

Strong customer authentication

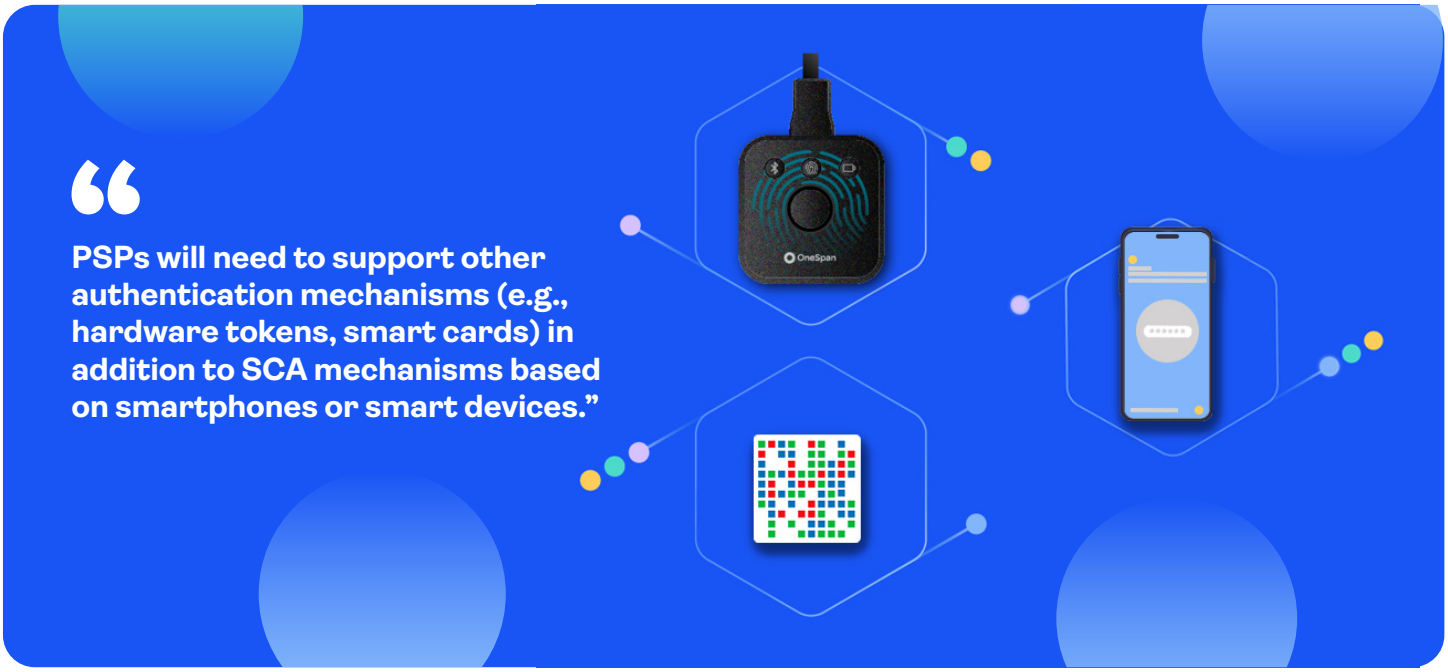
The requirements related to strong customer authentication are present in Articles 85-89 of the current draft of the PSR from the European Parliament. In what follows, we review the main changes in the Parliament's draft compared to the Commission's original draft proposal. We also discuss the EBA's comments where relevant.

Definition of SCA

The main change to the definition of SCA in the draft proposal of the European Commission in June 2023 was that the authentication elements that make up the SCA mechanism do not necessarily need to belong to different categories, as long as their independence is preserved. The European Parliament has maintained this change under item 12 of Article 85. As a consequence, the current draft proposal allows creating an SCA mechanism from two knowledge elements, two possession elements, or two inherence elements, for example, as long as they are independent. The EBA, on the other hand, requests in item 29 of its Opinion that the definition of SCA from PSD2 be reinstated, so that the authentication elements need to belong to at least two different categories. The EBA says allowing authentication elements from the same category could make SCA more subject to fraud.

SCA mechanisms constructed from two elements in the same category currently do not really exist in practice. It is also not clear how an SCA mechanism based on two knowledge elements or two inherence elements could be practically constructed, as these SCA mechanisms would lack the possession factor that usually stores the cryptographic key used to generate the authentication code. Hence, the practical advantages of allowing two elements from the same category are not immediately clear.

Also it is remarkable that the definition of SCA in the PSR remains very basic, and does not refer to more advanced properties of authentication mechanisms such as "phishing resistance" and "verifier compromise resistance", which have become common in recent years. The EBA's Opinion also does not mention these properties. Hopefully the upcoming Regulatory Technical Standards (RTS) will develop the definition of SCA in more detail.



SCA by account information service providers (AISPs)

The draft proposal of the European Commission proposed a significant change to the usage of SCA in the context of open banking: It allowed AISPs to perform SCA themselves, without having to rely on the SCA mechanism of the account servicing payment service provider (ASPSP, typically the bank). This was a change requested and welcomed by AISPs, as it allowed them to simplify the SCA experience of their users.

However, the draft proposal of the European Parliament has removed this possibility: Articles 85 and 86 do not allow AISPs to use their own SCA anymore. The EBA's Opinion does not discuss this topic. The European Parliament probably listened to concerns of ASPSPs, which did not like the prospect of not fully controlling the SCA mechanisms used to access bank accounts.

Accessibility requirements for SCA mechanisms

Article 88 requires PSPs to ensure that all users can perform SCA, including persons with disabilities, older persons, people with low digital skills, and those who do not have access to digital channels or payment instruments. This has remained unchanged in the European Parliament's review and will require PSPs to support various forms of SCA mechanisms to cater for the specific situation and needs of all their users.

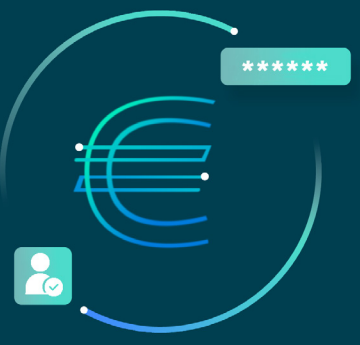
No mobile-only approach to SCA

In addition, Article 88 says PSPs must not use a single SCA mechanism, such as a mechanism based on smartphones, but instead support various authentication mechanisms. The European Parliament maintains this position, and strengthens it by emphasizing that PSPs must support more than one SCA mechanism in order to cater to the needs of their entire customer base and in particular to the needs of customers with disabilities, limited digital skills, older persons, and people who do not have access to digital channels.

Many PSPs currently adopt a *mobile-first* approach to SCA. The above requirements imply that PSPs cannot adopt a *mobile-only* approach. PSPs will need to support other authentication mechanisms (e.g., hardware tokens, smart cards) in addition to SCA mechanisms based on smartphones or smart devices.

Furthermore, the European Parliament added the requirement to Article 88 that PSPs must provide SCA mechanisms free of charge. In other words, they are not allowed to charge their customers for SCA mechanisms. This is an important addition, as it is not uncommon for PSPs to charge.

"The European Parliament added the requirement to Article 88 that PSPs must provide SCA mechanisms free of charge. In other words, they are not allowed to charge their customers for SCA mechanisms. This is worth noting, as it is not uncommon for PSPs to charge."



Authorised push payment (APP) fraud prevention

One of the main goals of the PSR is to curb APP fraud. APP fraud occurs when a fraudster tricks a victim into authorizing a payment to a fraudulent account. This is often done through sophisticated social engineering techniques, such as phishing emails, phone calls, or text messages. The fraudster may impersonate a trusted individual or organization, such as a bank, the police, or a government agency. They may create a sense of urgency, claiming that the victim needs to act quickly to avoid a negative consequence. Once the victim is convinced, they are instructed to transfer money to a specific bank account controlled by the fraudster.

The draft proposal of the European Commission listed various countermeasures against this type of scam in Articles 81-84. In what follows, we'll discuss how the Parliament's draft is different from the Commission's original draft proposal.

IBAN/name matching service

Article 50 of the draft proposal of the European Commission stipulates that the PSP of a payer, who initiates a credit transfer, can request the PSP of the payee to verify whether the name and IBAN of the payee, as provided by the payer, match. If they don't match, the payer's PSP must inform the payer about the discrepancy and the degree of the discrepancy, and this within a few seconds after entry of the payee information by the payer. The payer remains free to decide whether or not to authorise the credit transfer, even if a discrepancy was detected. The service must be provided free of charge.

The European Parliament has retained this article unchanged in its draft proposal. An IBAN/name matching service can indeed be very helpful to address social engineering fraud, as fraudsters sometimes try to convince victims that a certain IBAN belongs to a trusted beneficiary, while in reality if belongs to a money mule. The matching service is not a silver bullet as it relies on the ability of the payer to correctly interpret the notification and take appropriate action, and fraudsters might convince the victim to ignore the notification. But it's certainly a good countermeasure, and is already in widespread use in various countries (e.g., UK, Netherlands) and also part of anti-scam initiatives in other countries (e.g., UK, Australia).

Liability for fraud

Article 59, entitled "impersonation fraud", discusses liability for fraud whereby the victim is manipulated by a fraudster impersonating another entity. The European Parliament made significant changes to this article. In the European Commission's original proposal from June 2023, impersonation fraud only covered fraud cases whereby the fraudster is impersonating the victim's PSP, and not other types of entities. In the Parliament's draft, impersonation fraud covers cases whereby the fraudster pretends to be an employee of the victim's PSP or any other entity (e.g., the police). Hence, the scope of impersonation fraud has significantly expanded.

This expansion is a welcome change for consumers, as in many APP scam cases the fraudster impersonates an entity different from the PSP. On the other hand, PSPs might not be in favour of this change as they fear becoming "fraud compensation funds". In order to soothe the pain, PSPs will be able to shift liability to other parties under certain conditions, as we will discuss further below. In any case this topic will most likely be heavily debated in the upcoming trilogue negotiations among the Commission, Parliament, and Council.

The PSP is liable for impersonation fraud if the fraudster, who pretends to be an employee of a certain entity, manipulates the victim using the name, email address, or telephone number of that entity and that manipulation gives rise to fraudulent payments authorised by the victim, under the condition that the victim reported the fraud to the police and notified their PSP. In such a scenario the victim's PSP has to refund the victim the full amount of the fraudulent authorised payment transaction. Note that the draft PSR does not define a maximum liability amount. This is different from the situation in the UK, where banks are currently liable for APP scams up to £85 000.

The PSP is not liable if the victim acted fraudulently or acted with gross negligence. However, the burden to prove that the victim acted fraudulently or with gross negligence resides with the victim's PSP.

In addition, under the Parliament's draft proposal, the PSP could

transfer liability to the electronic communications provider used by the fraudster to communicate with the victim, if the PSP informs this provider about the fraud case and if this provider does not remove fraudulent content related to the fraud case.

The PSR defines an *electronic communications provider* as a company subject to the European Electronic Communications Code (ECCC) or the European Digital Services Act. These companies are traditional telecommunications providers, such as mobile network operators, fixed-line operators, and Internet service providers, but also social media platforms, messaging apps, online marketplaces, content sharing platforms, online travel and accommodation platforms, etc.

PSPs in many European countries have long argued that they should not be solely liable for impersonation fraud, as the fraud very often originates outside banking or payment applications. The Parliament has listened to this concern and its draft proposal puts more responsibility on electronic communications providers, similar to the liability schemes in the UK, Singapore, and Australia. Nevertheless it is still the PSP that needs to refund the victim, after which the PSP can attempt to obtain a refund from the electronic communications provider. Trying to obtain a refund can still put a significant burden on PSPs.

Electronic communications service providers are also required to educate and alert their customers about new forms of scams, explain which precautions they can take to avoid falling victim, and inform them how they can report fraudulent content.

Finally, the draft proposal of the Parliament states that all providers involved in the fraud chain have to put organisational and technical measures in place to prevent and mitigate payment fraud. It is not specified which measures are meant. This will most likely be developed further in the Regulatory Technical Standards (RTS) accompanying the PSR.

In summary, the Parliament intends to provide consumers with broader protection against impersonation scams and wants not only PSPs but also electronic communications and digital services providers to do their part in the battle against impersonation scams.

Transaction monitoring

Article 83 of the PSR basically contains the same requirements related to transaction monitoring as those already present in the RTS on SCA of PSD2. It requires PSPs to have transaction monitoring mechanisms in place to support the implementation of SCA and its exemptions, and to detect and prevent potentially fraudulent payment transactions.

The latest review of the European Parliament states that when transaction monitoring mechanisms provide strong evidence for suspecting a fraudulent transaction, payment service providers have the right to block the execution of the payment. In addition, when the PSP of the beneficiary of an incoming transaction suspects that the transaction is fraudulent, the PSP might refuse to make the funds available immediately to the beneficiary. The beneficiary's PSP can further analyse the transaction, and either make the funds available to the beneficiary or return them to the payer's account servicing payment service provider. These possibilities will require transaction monitoring mechanisms to have low degrees of false positives, in order to avoid unpleasant conversations with consumers.

In its Opinion, the EBA proposes various enhancements to the Commission's proposal in the context of transaction monitoring. In particular, the EBA proposes in item 29 to complement the transaction monitoring performed by PSPs initiating transactions with the screening of received transactions by the beneficiary's PSP, aimed at detecting suspicious fraud patterns based on the amount, origin, frequency of transactions, possible deviation of the payee's name in transactions against the payee's name, etc. This proposal indeed makes sense and is already implemented in the UK's Contingent Reimbursement Model Code since 2019.

Fraud data sharing

In order to improve the protection of payers against fraud in credit transfers, PSPs should be able to perform transaction monitoring based on information as comprehensive and up to date as possible, namely by collectively using information concerning IBANs of payees, manipulation techniques, and other circumstances associated with fraudulent credit transfers identified by PSPs. Article 83 therefore provides a legal basis for PSPs to share fraud-related information between themselves in respect of GDPR.

The Parliament's draft proposal goes into more detail and specifies that PSPs have to exchange identifiers (e.g., names, personal identification numbers, organisation numbers), the fraudster's modus operandi, and other transaction information about payees who are believed to be recipients of a fraudulent payment with other PSPs when the PSP has sufficient evidence to assume that there was a fraudulent payment transaction. It can be assumed that sufficient evidence is available when at least two customers of the same PSP have informed that a unique identifier of a payee was used to make a fraudulent credit transfer.

User Education

Article 84 introduces an obligation for PSPs to carry out education actions to increase awareness of payments fraud among their customers and staff. Specifically, PSPs must give their customers clear indications on how to identify fraudulent attempts and how to avoid falling victim to fraudulent actions targeting them. Payment service providers have to inform their customers of where they can report fraudulent actions and obtain fraud-related information.

In the Parliament's draft proposal, this article additionally requires European Member States to allocate substantial means to investing in education on payment-related fraud, for example via media campaigns or schools. Payment service providers and electronic communications service providers have to cooperate free of charge with the Member States in those educational activities.

European Member States will be reuiqred to allocate substantial means to investing in education on payment-related fraud, for example via media campaigns or schools.

What comes next

As mentioned above, the European Parliament adopted draft texts for the PSR on 23 April 2024, closing its first reading.

The legislative process now continues with a review by the European Council and trilogue negotiations among the Commission, Parliament, and Council, which are expected to conclude in the first half of 2025.

Once the trilogue negotiations have been concluded, the final text of the PSR will be published in the Official Journal of the European Union. The PSR enters into force 20 days after this publication and enters into application 18 months thereafter. If the final proposal of the PSR were published in April 2025, for example, the PSR would enter into application in October 2026.

Once the PSR is available, the European Banking Authority (EBA) will start with the development of more detailed Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS).

Conclusion

The European Parliament has made various significant changes to the European Commission's original draft proposal for the PSR in the areas of strong customer authentication and fraud prevention.

In the context of SCA, PSPs have to make sure they support multiple SCA mechanisms to cater to the needs of their entire customer base. It is not enough for PSPs to wait until customers ask for another SCA mechanism – they need to proactively support multiple authentication mechanisms. In addition, PSPs are not allowed anymore to charge their customers for SCA mechanisms. It is also noteworthy that, under the Parliament's draft proposal, AISPs are no longer able to perform SCA themselves and have to keep using the ASPSP's SCA mechanisms.

The most prominent new elements in the area of APP fraud prevention are the broader definition of impersonation fraud and the responsibilities of electronic communications providers and digital service providers. In the Parliament's proposal, banks would not only be liable for bank impersonation fraud, but for impersonation fraud relating to any third party. PSPs could transfer liability to electronic communications providers if the latter fail to remove fraudulent content that is used by fraudsters to commit impersonation fraud.

The discussion will continue in the trilogue negotiations among the Commission, Parliament, and Council. Once the PSR itself is final, the SCA and APP fraud prevention mechanisms will be further detailed in the new or revised RTS.

For more information or to discuss regulatory developments and compliance in more detail for your business, contact a OneSpan representative.

About the author

Frederik Mennes is Director of Product Management & Business Strategy at OneSpan. In this role, he is responsible for defining and implementing OneSpan's business strategy for specific industry verticals, and to determine how OneSpan responds to security and regulatory market trends. Previously, Frederik led OneSpan's Security Competence Center, where he was responsible for the security aspects of OneSpan's products and infrastructure. He has an in-depth knowledge of authentication, identity management, and security technology in general.

For more information or to discuss regulatory developments and compliance in more detail for your business, contact the author at frederik.mennes@onespan.com.

About OneSpan

OneSpan helps organizations accelerate digital transformations by enabling secure, compliant, and refreshingly easy customer agreements and transaction experiences. Organizations requiring high assurance security, including the integrity of end-users and the fidelity of transaction records behind every agreement, choose OneSpan to simplify and secure business processes with their partners and customers. Trusted by global blue-chip enterprises, including more than 60% of the world's largest 100 banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

Learn more at
OneSpan.com

Contact us at
OneSpan.com/contact-us

OneSpan