PAYMENTS EUROPE'S POSITION ON PSD3 AND PSR

Key takeaways

- It is of utmost importance to ensure that the PSD3 and PSR set a future-proof framework for SCA. Ensuring technological neutrality is fundamental to foster innovation and allow the market to continue developing and improving secure and user-friendly solutions.
- It is essential that the SCA framework ensures the highest level of consumer protection and fraud prevention. An SCA framework that allows and encourages PSPs to select the best combination of authentication methods and technologies is essential, as flexibility will have a positive impact on the introduction of new authentication solutions and prevent financial and digital exclusion.
- It is also very important to clarify the liability of PSPs when it comes to fraud prevention. Liability should be allocated proportionately, not least to ensure SCA exemptions are properly applied to the benefit of users.
- It is fundamental to ensure flexibility and business continuity by allowing transactions to proceed without SCA in case of no connectivity as well as supporting dynamic linking in legitimate scenarios.
- Payments Europe fully supports the ongoing efforts on the current Open Banking and upcoming Open Finance Framework, which should ensure a high level of consumer protection and foster innovation.
- It is of utmost importance that open banking (and finance) enable consumers to be in control of their data with strong and transparent measures to ensure the protection of sensitive data. This will require the establishment of transparent PSU permission dashboards and the implementation of robust authentication protocols.
- Furthermore, the responsibilities and roles of the service providers involved should be very clearly defined to ensure the highest level of service and to establish clear tools and practices whilst preventing unnecessary compliance burdens.

Payments Europe welcomes the European Commission's (EC) proposals for the review of the Payments Services Directive (PSD3) and the establishment of the Payments Services Regulation (PSR), evidence of the EC's efforts to further promote the digital transformation and eliminate fragmentation in the European payments market.

In this paper, Payments Europe shares its views on the proposed revisions, in particular in relation to rules on strong customer authentication (SCA) and open banking.

Regarding Strong Customer Authentication

Security and consumer protection are fundamental in payments, and PSD2 has been instrumental in developing a framework for the safety and reliability of payments whilst fostering competition and innovation.

PSD3 and PSR give the opportunity to ensure the SCA framework is able to respond accordingly to the rapid changes that the European payments sector is experiencing and to address any shortcomings of the existing legislation. **Technological neutrality and the development of 'future-proof regulation' should remain at the core of any legislative development, including the development of Regulatory Technical Standards, to protect innovation and develop secure and user-friendly solutions.**

On SCA delegation and outsourcing

Allowing for SCA delegation under PSR is fundamental to incentivize the emergence of new security solutions. Indeed, **relying on different SCA methods involving trusted third parties can bring about substantial benefits and have a positive effect on the introduction of new authentication solutions**, facilitating the development of new business models for payment services and improving customer convenience.

At the same time, Payments Europe is aware that requiring outsourcing agreements for all SCA methods where third parties are involved would increase their level of complexity, negatively impacting competition on the market. Indeed, this would make it increasingly difficult for smaller market players to implement outsourcing agreements, therefore making it virtually impossible for them to offer innovative SCA methods and generating competitive disadvantages.

Only authentication models in which the payer's Payment Service Provider (PSP) does not control SCA should be categorized as outsourcing. Conversely, authentication models where the payer's PSP controls SCA should not be treated as SCA delegation and should, therefore, not be subject to outsourcing requirements.

On authentication elements

There is still a wide set of static factors that are compliant with SCA requirements but are more susceptible to fraud, like knowledge-based factors such as static passwords or personal identification numbers. **Times have changed, and modern authentication requires modern means**.

Payments Europe welcomes that this has now been reflected in the EC proposal. We believe that two inherence-based factors can provide the same level of security, as long as the compromise of one factor does not imply the compromise of the other. This will allow PSPs to continue innovation and support the development of diverse and robust authentication methods.

On expanding the scope of inherence

Regarding inherence, Payments Europe welcomes the clarifications the EC proposes in the preamble of the PSR, noting that inherence should also take into account environmental and behavioral characteristics for the Transaction Monitoring Mechanisms. However, we recommend further clarifying the wording within PSR acknowledging that this behavioral and environmental characteristics could be considered as a valid SCA inherence element.

Whilst we understand that it is the EBA's task to further define SCA elements, we are convinced that environmental and behavioral characteristics should be acknowledged in the level one legislation. As technology evolves, there are increasing signs that non-physical biometrics can be equally accurate in their capacity to identify a person compared to traditional physical attributes.

On exemptions to SCA

It is essential to have an SCA framework that allows and encourages PSPs to select the best combination of authentication methods and technologies for each use case. A flexible approach to SCA will prevent financial and digital exclusion by enabling PSPs to cater to more vulnerable consumers.

Ensuring appropriate exemptions is crucial to maintaining a balance between security and user experience. Thus, it is essential to revisit the exemptions regime and refine it further, addressing any emerging concerns and taking into account the latest developments in the payments landscape. Such fine-tuning will **streamline regulatory efficacy and increase user satisfaction while maintaining a risk-aware landscape**. One example would be in flight payments which require deferred authorization.

More precisely, additional exemptions tailored for low-risk scenarios should be established, and the cap for contactless payments should be raised to €250. We would also recommend extending the current exemption for unmanned parking terminal to EV Charging points.

Moreover, **the regulator should take a proportionate approach to the issue of liability**. Whilst exemptions aim to facilitate transactions from the user's perspective, the liability rules established by Article 60, paragraph 2 of PSR inadvertently deter PSPs from relying on them, due to the potential risk of being held solely liable.

New liability provisions for impersonation fraud

The Commission proposal places significant responsibility on banks to prevent fraud. While banks indeed play a crucial role in the payment process, it is important to recognize that they cannot single-handedly prevent all instances of fraud.

Fraud is a very complex issue that often involves various entities, such as consumers, merchants, financial institutions, and telecommunication providers. Therefore, **regulation should adopt a balanced approach, ensuring shared responsibility for fraud prevention among all parties**, rather than laying the entire weight on banks.

This could entail educating consumers, mandating merchants to use secure payment systems, promoting collaboration among financial institutions for fraud detection and prevention, and fostering cooperation with mobile operators and communication platform providers. It is essential to find an equilibrium between consumer protection, equitable liability distribution, and shared responsibility across all parties involved in the payment process to avoid incentivizing complacency or lack of accountability. Financial institutions should also be proactive, investing in sophisticated security technologies and adopting rigorous security protocols.

New liability provisions for technical service providers and operators of payment schemes

The prosed PSR includes a new article outlining new liability provisions for technical service providers and operators of payment schemes for failure to provide the services that are necessary to enable the application of strong customer authentication. We believe this article is not proportional and does not reflect all the actors involved in the authentication chain posing liability only on two players that do not have control over the rest of the actors involved.

For instance, scheme operators do enable EMV 3DS Directory server that connects merchants to the relevant issuer's Access Control Server (ACS), but there are many other actors different from scheme members involved in the authentication chain that also play a part and over which scheme operators have no controls. Contracts between these parties already contain liability provisions covering cases where there might be failures during the processing of a transaction, including on the authentication.

On outages

The current wording of PSR makes it unclear whether transactions requiring SCA can continue to be authorized through the authorization network when the authentication infrastructure is down.

To ensure business continuity during technical incidents, we recommend allowing payments without SCA, exceptionally and temporarily, during technical incidents affecting the authentication infrastructure. Other appropriate safeguards should be put in place in these situations to ensure the security of payments, and Payments Europe would most welcome clear indications from the regulator as to how these should look like.

On dynamic linking

Regarding dynamic linking, Payments Europe recommends adopting a flexible approach as we observe a number of legitimate scenarios in online payments where the final transaction amount is not known, and the amount is not blocked at the time of authentication. One example is the case of online grocery shopping, where the price of weighed goods can differ from the amount estimated at authentication. As such, this poses challenges to dynamic linking as it typically involves creating a unique authentication code based on specific transaction details, including amount. Regulation should accommodate situations where final amount is uncertain or may change and ensure that legitimate transactions can still proceed securely as long as the merchant have made the customer aware that the price could vary, and the customer have agreed to such a possibility when authorizing the original indicative amount.

Definition of merchant-initiated transactions (MITs) and Mail Order Telephone Order Transactions (MOTO)

We welcome the additions in the Level one text with definitions of MIT and MOTO transactions.
With regard to MIT, in order to ensure a level playing field, we believe that for both Merchant Initiated Transactions and SEPA Direct Debits, to ensure better security for both customers and merchants, SCA should be necessary for modifying mandates, regardless of whether the payer's bank is involved in setting them up.
With regard to MOTO, Payments Europe welcomes the legal clarity on it stipulating that the obligation for SCA only applies to the initiation, and not to the execution, of a payment transaction.
Card payments and bank transfers are both 'electronic' when completed via the internet or other digital mean, whilst they are both 'not electronic' when payment details are transmitted from cardholder to merchant via non-electronic channels. This is the case even if the details captured are then sent onwards electronically for processing. Therefore, it makes sense to accept that MOTO transactions should be considered non-electronic when initiated via mail or telephone order, although they can be executed electronically afterwards.

MIT refund rights

While we are fully supportive of consumer protection, we do not favor the extension of 8-week unconditional refund rights to MITs, as these transactions already offer level strong consumer protection, and unconditional refund could lead to misuse and to increased rates of first-party fraud, and excessive burden on smaller merchants. Given the much broader range of use cases of MITs compared to SDDs, MITs are much more exposed to abuses of this unconditional refund rights than SDDs. Keeping in mind that around 30% of all e-commerce transactions are MITs, extending this unconditional right would have a very heavy impact on e-commerce merchants, particularly smaller ones, as they might find themselves obliged to refund goods or services that have already been delivered and/or consumed.

It is also worth remembering that the existing protections for card-based MIT transactions include those implemented to ensure that consumers are protected from "subscription traps".

On Open Banking

Open Banking has the potential to unlock major advancements in innovation, competition, and customer involvement in payments. To achieve this, the regulation dedicated to Open Banking should find the balance between protecting consumer and supporting innovation.

On Establishing transparent PSU permission dashboards

Transparency in financial transactions is essential to build trust between Payment Service Users (PSUs) and providers. A crucial aspect of this transparency lies in the creation of clear and comprehensive PSU permission dashboards that will empower users with a clear understanding of how their data is accessed and utilized.

By providing users with the ability to manage permissions effectively, financial institutions can enhance user confidence and satisfaction. However, when users re-establish their permissions for specific Account Information Services (AIS), they should do so in compliance with the applicable terms and procedures of the relevant service provider. With this in mind, in situations where previously withdrawn permissions need to be re-established, it will be important to ensure that this is done in accordance with the terms and procedures the AISP has in place at the time of re-establishment.

On strengthening customer authentication

The security of user data and transactions is a main concern of both users and providers. **Strengthening customer authentication mechanisms for AIS and Payment Initiation Services (PIS) is a critical step toward ensuring the protection of sensitive information.**

By implementing robust authentication protocols, financial institutions can effectively safeguard user data and prevent unauthorized access, contributing to a safer digital financial landscape.

On ensuring the presence of robust enforcement mechanisms

Regulations governing financial services require periodic review and refinement to keep up with evolving industry dynamics.

The recitals of PSR highlight the potential for Authorized Account Information Service Providers (AISPs) to transmit consolidated information to third parties for offering non-payment services, such as lending and creditworthiness assessment, with user consent. However, the definition of AIS in both texts involves collecting and consolidating payment account information for users, but not sharing them. **Clarifying this and explicitly allowing the transmission of consolidated information to allow for the provision of further services can contribute to a more comprehensive and adaptive regulatory framework** and avoid ambiguity.

To streamline processes and ensure a seamless user experience, it would also be important to clarify whether dual SCA requirements is something that the regulator supports: the shift toward AISPs conducting regular SCA during payment account access raises questions to this end, and could lead to users having to go through the SCA process twice (once with AISPs and once with Account Servicing Payment Service Providers (ASPSPs)).

On licensing processes

Payments Europe supports the EC's efforts to facilitate access to payment systems and streamline the licensing process for Payment Institutions (PIs), including Electronic Money Institutions (EMIs). The proposal currently includes a new requirement for existing PIs and EMIs to seek a new authorization under PSD3, whilst noting that Member States can provide mechanisms to automatically grant this new authorization to existing PIs and EMIs.

To avoid delays, damaging existing business models as well as to protect the level playing field, Payments Europe invites the regulator to allow existing PIs and EMIs to continue to provide their services under their existent PSD2/EMD2 licenses, without the need to seek a new PSD3 license. This approach will allow PIs to continue to provide seamless services, safeguarding operational stability.