

From PSD2 to PSD3 and PSR – European Parliament sets out its vision on the future of payments

24 April 2024

The payments landscape has undergone significant changes over the past decade, changes driven by fast-paced technological advancements and evolving consumer behaviours. In response to this dynamic evolution (rather than revolution), the European Commission proposed to revamp the Payment Services Directive (**PSD2**) regime with a new regulatory framework proposed in June 2023 (Payment Services Regulation (**PSR**) and Payment Services Directive (**PSD3**). In our previous [blogpost](#) we examined what the proposed changes were, and how they could potentially impact the sector.

Fast forward 10 months and discussions by the co-legislators (the Council and the European Parliament) have advanced quickly. In fact, on 23 April 2024 the Parliament gave the green light of its plenary to the Economic and Monetary Affairs Committee (ECON) position. Indeed, the corridors of the European Parliament have been buzzing with both political and technical negotiations on amendments to the Commission's proposals, whether by adding more stringent transparency requirements on elements such as currency exchange rates or adding new robust consumer protection safeguards.

In parallel, Member State attachés have been engaging in their own discussions and should come to a position by the end of June 2024.

To be able to understand the next step of the process, let's delve into what's expected for the "trilogue process". Trilogues, or inter-institutional negotiations, will bring together the Council of the EU, the European Commission, and the European Parliament to reach an agreement on the new set of rules and obligations. As the only co-legislator with a finalised position right now, let's see what change MEPs have made in more detail.

The Parliament's position on PSD3 and PSR - what you need to know

a) Licensing requirements and authorisation

PSD3 covers authorisation and supervision of payment institutions. One of the novelties in the PSD2 revision is that payment institutions now encompass the provision of electronic money services, as PSD3 merges with the Electronic Money Directive.

Regarding licensing, the Parliament maintains most of the Commission's drafting, specifying that Member States must require companies applying for authorization to offer payment services to have professional indemnity insurance or a similar liability guarantee for the areas they operate in. However, the Parliament adds that undertakings may also have a minimum starting capital of EUR 50,000, but only during the initial authorization period.

The Parliament's position also requires the Commission to set up a dedicated website containing all registration information for each Member State. Additionally, it mandates the European Banking Authority (**EBA**) to organize an annual collaboration forum among National Competent Authorities (**NCA**s) to enhance harmonization in implementing PSD3's provisions.

The Parliament maintains the Commission's proposal to provide for the option that payment institutions may open safeguarding accounts with central banks, as payment institutions have frequently faced the challenge that credit institutions refused their requests. However, the Parliament goes one step further and suggests that central banks (similar to credit institutions) also must provide a clear explanation when they refuse access to safeguarding accounts or terminate the payment institution's existing account. While the Commission suggested a similar obligation, the Parliament has clarified further how this justification should be provided.

b) Open banking

As proposed by the Commission, account servicing payment service providers (**ASPSP**) would be obliged to provide at least one dedicated interface for open banking data access (see our [blogpost](#)). Moreover, ASPSPs will need to provide payment initiation service providers (**PISP**) with the necessary transaction information when initiated directly by the user for execution.

The Parliament's proposal would require ASPSPs not only to provide the information after receiving the payment order but also any updates, like payment status, via a dedicated interface in real-time until the payment is completed or rejected. MEPs also suggest that the EBA should be tasked with developing guidelines on third-party data access.

The Parliament position aligns with the Commission in that it indicates that ASPSPs should not be required to offer an alternative interface where the dedicated interface is unavailable other than the interface that the account servicing payment service provider uses for authentication and communication with its users to access payment account data.

To enable payment services users (**PSU**) to manage their open banking permissions in a convenient way, ASPSPs would be required under both the Parliament and Commission's proposal to offer a "dashboard", that is integrated in the user interface, allowing the PSU to withdraw the data access to any given open banking provider. However, the Parliament's position goes one step further and suggests the EBA develops draft regulatory technical standards setting out a standardised list of categories of information to be disclosed in such a dashboard.

c) Fraud provisions and liability

Given the rise of new fraud types, MEPs have spent significant time discussing how to enhance consumer protection measures and raising awareness about these emerging threats.

The Parliament's position on fraud prevention empowers payment service providers (**PSPs**) to block payment orders or funds if their monitoring or a police report indicates fraud, prioritizing transaction security. The Parliament also suggests clarifying that if the PSP had reason to block a unique identifier but did not, the PSU will not face any financial consequences. Additionally, MEPs aim to enhance consumer awareness by mandating Member States to invest in anti-fraud education, supported by

payment and communication providers, who shall also cooperate with Member States free of charge in this respect.

In cases of fraud, the PSR proposal places the burden on the PSP to prove that the consumer acted fraudulently or with gross negligence and that the PSP should be held liable where a consumer has been manipulated by a third party under certain conditions (see our [blogpost](#)). The Parliament extends fraud reimbursement rights to a broader scope of electronic communications service providers, which the Parliament defines as any providers covered by the Digital Services Act or the European electronic communications code. If such providers fail to remove fraudulent or illegal content after being informed thereof, in cases of impersonation fraud they must refund consumers for the relevant fraudulently authorised transactions, provided that the consumer reported the fraud to the police and their PSP promptly. Additionally, the Parliament position would oblige electronic communications and digital platform service providers to employ fraud prevention techniques to combat different types of fraud, such as unauthorized and authorized push payment fraud.

d) Strong Customer Authentication (SCA)

SCA is a vital fraud prevention tool, adding extra layers of authentication for secure online payments (see our [blogpost](#)). Under PSD2, customers were required to provide two out of three authentication factors: knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is), to access their accounts. While the Commission's proposal indicated that these two or more elements do not necessarily need to belong to the same category, the Parliament's position additionally clarifies that the independence of the elements shall be preserved at all times. It also states that the "inherence" element of SCA can include things such as environmental and behavioural characteristics, for example where the transaction is happening.

e) Enforcement

The Parliament position maintains the Commission's proposal to set out expanded sanction powers of the NCAs including comprehensive investigation rights, the right to impose periodic penalty payments on PSPs and members of their management body, and a requirement to publish decisions on sanctions and administrative measures ("naming and shaming").

What's next?

The European Parliament [adopted](#) its position ([link](#)) on PSD3/PSR on 23 April 2024. Member States in the Council will now need to adopt their position for trilogue negotiations to start. The Belgian Presidency is optimistic that Member States will manage to finalize their position by June 2024.

Trilogues will only begin once the new Parliament is formed, following European elections from 6 to 9 June – potentially around September 2024.

According to the current Commission proposal, PSD3 shall be transposed into national law within 18 months, and PSR shall apply from the date 18 months, after its respective entry into force. The Parliament has kept the same timeline as suggested by the Commission for PSD3 but suggests that PSR shall only apply 21 months after its entry into force.

"(...) With this file we do not only protect consumers, from various types of fraud, oblige payment service providers to deliver higher transparency levels for ATM withdrawals or give consumers better control over who has access to their data." Marek Belka, Socialist Polish MEP and lead drafts-person on the PSR

 www.europarl.europa.eu/...