PSD3: European Parliament adopts amended PSD3 and PSR texts at first reading

08 May 2024

On 23 April 2024, the European Parliament announced its adoption at first reading of amended texts of the European Commission's June 2023 legislative proposals for a Directive on payment services and electronic money services (PSD3) and a Regulation on payment services in the EU (PSR). This was followed on 29 April by the European Banking Authority's (EBA) publication of an Opinion on new types of payment fraud, setting out additional measures for consideration by the EU co-legislators and the Commission in the negotiation of the PSD3/PSR proposals. The Council has not yet published its proposals on the Commission's draft legislation, although we are expecting to have a general approach before the end of the Belgian Presidency on 30 June 2024. After that - and once the new Parliament is in place following the European elections on 6-9 June 2024 - trilogues (inter-institutional negotiations) will begin.

What's the story so far?

The European Commission published its anticipated PSD3 and PSR proposals to improve the functioning of PSD2 in June 2023. Those texts are now subject to review and amendment by the European Parliament and Council of the EU as well as inter-institutional negotiations (trilogues) with the Commission.

In November 2023, ECON published draft reports on the proposals with recommendations for amendments (see 'PSD3: Putting citizens at the heart of EU payments'). ECON voted to adopt the texts in February 2024 (see 'PSD3: European Parliament's ECON Committee adopts draft reports on PSR and PSD3'). The Parliament has now voted to adopt both texts in plenary, closing the first reading.

For an overview of the whole June 2023 legislative package, take a look at our article 'Evolution not revolution: European Commission publishes financial data access and payments package' which also links to a full form briefing.

EBA Opinion on new types of payment fraud and possible mitigants

As part of the EBA's objective to 'contribute to enhancing customer protection' and 'play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union' (see Regulation (EU) No 1093/2010 establishing the EBA), it has issued an Opinion aimed at helping to further strengthen the forthcoming legislative framework under PSD3 and the PSR in relation to anti-fraud requirements for retail payments.

The Opinion follows on from the EBA's June 2022 Opinion on the PSD2 review and its recommendations are made in light of (among other things):

- its recent assessment of fraud data for 2022, which found that:
    - instant payments - which with the application of the Regulation on instant credit transfers in euro ((EU) 2024/886) (Instant Payments Regulation) are expected to be increasingly used by customers in the EU - show markedly higher fraud rates than traditional credit transfers;
    - fraud rates for cross-border transactions are much higher than for domestic ones across all payment instruments included in the PSD2 payment fraud reporting framework (applying to both cross-border transactions among countries in the Economic European Area (EEA) and cross-border transactions between an EEA country and an extra-EEA country);
    - the distribution of liability for fraud losses in the EEA between the payment service user (PSU) and the PSP or other entities varies considerably across payment instruments (eg in 2022 for card payments the losses were approximately equally split between PSUs and PSPs plus other entities, but for credit transfers the share of losses borne by the PSU was 79%), and the share of losses borne by the PSU also varies significantly across the EEA; and
- its observation of emerging types of payment fraud, notably more sophisticated forms which employ social engineering to circumvent the protection afforded by strong customer authentication (SCA).

The EBA welcomes the new security provisions included in the Commission's PSD3 and PSR proposals and in the Instant Payments Regulation and acknowledges the additional provisions to mitigate fraud that have been proposed in the amended texts adopted by the European Parliament. However, it is of the view that the additional security measures set out in its Opinion could support a '*comprehensive, uniform and future-proof framework for the mitigation and control of payment fraud in the EU*'.

Parliament's position on PSD3/PSR and EBA's Opinion: What are some of the key points to be aware of?

PSD3 proposal

Authorisation: Existing payments and e-money firms

- There is clarification that PIs already authorised under the current Payment Services Directive ((EU) 2015/2366) (PSD2) will not have to go through a full authorisation process. Instead, they will only have to provide their competent authority with the extra elements required under the updated rules (eg a winding-up plan), following which the competent authority will make a decision on the continued authorisation of the PI. Similar changes are proposed in relation to EMIs already authorised under the second Electronic Money Directive (2009/110/EC) (EMD).
- The proposed provisions allowing for automatic authorisation under PSD3 where the competent authorities have evidence that an existing PI or EMI already complies with PSD3 have been amended to make such automatic authorisation a requirement for Member States. There is also revised wording obliging competent authorities to inform the PI or EMI concerned of any obstacle to authorisation and to proceed, without undue delay, to the removal of that obstacle.
- There is a new provision allowing competent authorities to extend the period before existing PIs and EMIs are prohibited from providing services when those PIs or EMIs have provided the required additional information but the competent authority has not been able to process it within the applicable deadline.

Authorisation: PISPs and AISPs

- The Commission's proposal contains a new provision allowing account information service providers (AISPs) to choose to hold initial capital of EUR 50,000 as an alternative to professional indemnity insurance or some other comparable guarantee at the registration stage only, to be replaced by professional indemnity insurance without undue delay after registration has been obtained. The Parliament replicates this for payment initiation service providers (PISPs).

Authorisation: Optional exemption for MiCA

- The Parliament proposes the addition of a new optional exemption where, for payment transactions used for the execution of trading and settlement services using e-money tokens as defined in Article 3(1), point (7) of MiCA (Regulation (EU) 2023/1114), the PSP has already been authorised as a cryptoasset service provider (CASP) in a Member State for those services under Title V of MiCA.

Streamlining central contact points

- Under PSD2, Member States were given the option to request that PIs established in another Member State set up central contact point(s) (CCPs) in the host Member State in order to report periodically to the host Member State on activities within that Member State for information or statistical purposes.
- However, there have been divergent applications of this provision across the Single Market and the draft ECON report queried whether CCPs should be done away with. The suggested first step – which has remained in the Parliament's final adopted text - is to streamline the provisions to ensure that PIs send all relevant information to just one contact point, which would then communicate the relevant information to the national competent authority of the Member State.

Emphasising the importance of access to cash and fee transparency

- The Parliament proposes increasing the amount that retailers are permitted to give customers in the form of cashback without a purchase from EUR 50 to EUR 100 (or the equivalent amount in the currency of the Member State concerned). There is also an additional condition that the withdrawal is non-anonymised and requires use of customer authentication.
- There is a new provision requiring ATM deployers to comply with the requirements on transparency of fees and charges in Article 7 of the proposed PSR, with a particular obligation to ensure the display of those fees and charges at the very beginning of the transaction. (See also 'Enhancing transparency measures' under 'PSR proposal' below.)

Opening of accounts by payment institutions

- The Parliament has included a new Recital which provides that, where a credit institution refuses to open, or decides to terminate, a PI's account, the credit institution should be required to provide the PI with a 'duly justified response and reasoning'. This is to protect the objective of diversification of risk for PIs.
- Likewise, with the Commission's proposal for an option for PIs to open safeguarding accounts at central banks the Parliament further proposes that any rejection of a PI's request by a central bank

should be ‘duly justified’.

Granting of credit relating to payment services

- The maximum duration for credit of 12 months has been removed. Instead, this point is left to the discretion of national competent authorities, creating a risk of divergence across Member States.

Access of PIs to designated payment systems: removal of proposed Settlement Finality Directive changes

- The Commission's June text proposed amending the Settlement Finality Directive (98/26/EC) (SFD) to include PIs as possible participants in designated payment systems, helping to level the playing field with credit institutions.
- The draft ECON report had highlighted that this amendment had also been proposed under the Regulation on instant credit transfers in euro ((EU) 2024/886), which at the time was still being finalised but has subsequently entered into force (although subject to phased implementation deadlines). It is presumably for this reason that the Parliament’s final adopted text does not contain the previously proposed SFD changes.

PSR proposal

Ensuring better anti-fraud protection for consumers

- The Commission’s proposed anti-fraud provisions include an obligation on electronic communications services providers (ECSPs) - such as mobile network operators and internet platforms and defined as any provider within the scope of the European electronic communications code (Directive (EU) 2018/1972) or the Digital Services Act (Regulation (EU) 2022/2065) - to cooperate with payment service providers (which includes the newly expanded definition of PIs as well as banks) (PSPs) in the fight against fraud. The Parliament has gone a step further by proposing explicit Recital references to:
    - joint responsibility of the PSP and the ECSP in the event of fraud where the latter fails to cooperate;
    - liability of ECSPs in relation to preventing further occurrences of so-called “spoofing” or impersonation fraud;
    - liability of online platforms (without prejudice to their obligations under the Digital Services Act) where fraud has arisen as a direct result of fraudsters using their platform to defraud consumers, if they were informed about fraudulent content on their platform and did not remove it.

In addition, the Parliament extends the scope of the provisions on impersonation fraud to include ECSPs and online platforms.

- On impersonation fraud in more detail:
    - A customer’s right to a refund in APP fraud “spoofing” cases has been expanded by the Parliament so that it covers not just situations where fraudsters pretend to be from the customer’s bank but from ‘any other relevant entity of a public or private nature’ too.

    - There is additional wording providing that ECSPs who do not remove fraudulent or illegal content after being informed must refund the PSP the amount of the fraudulent transaction, provided that the consumer has reported the fraud to the police and notified its PSP without any delay.
    - The Parliament proposes to require ECSPs to have in place all necessary educational measures for their customers, including alerts about new forms of online scams and how to report fraud, taking into account the needs of their most vulnerable customers.
    - There is a further proposed provision requiring PSPs, ECSPs and digital platform service providers to have in place fraud prevention and mitigation techniques to fight fraud in all its configurations, including non-authorised and authorised push payment fraud.
- The EBA's Opinion contains a number of proposals to amend the liability rules in the PSR proposal, including:
    - Clarifying the delineation between authorised and unauthorised transactions in case of disputes about a suspected fraud between the PSU and the PSP. Specifically, the EBA suggests:
        - specifying that, where a payer denies having authorised a transaction, the use of SCA should not in itself be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently;
        - specifying that, in the case of payer-initiated transactions (eg credit transfers), a transaction denied by the payer cannot be considered as authorised where the payment order was initiated by a fraudster, even if it was subsequently authenticated by the PSU;
        - clarifying that, without prejudice to the liability provisions relating to the verification of payee service introduced under the Instant Payments Regulation, a transaction denied by the payer cannot be considered as authorised where the payer was not made aware of a mismatch between the IBAN and the name of the beneficiary including, for example, because the fraudster has intercepted the notification from the payer's PSP referred to in the process for the verification of payee service as set out in the Instant Payments Regulation.
    - Clarifying the concept of gross negligence by amending the Recitals to the PSR to include:
        - that where a PSU falls victim to social engineering fraud, account should be taken of all relevant factors when assessing whether they acted with gross negligence, including but not limited to the complexity of the fraud, the PSU's personal circumstances, whether they had reasonable grounds for believing they were making a payment to a legitimate payee, and whether the PSP could have taken additional steps to help prevent the fraud taking place;
        - a non-exhaustive list of circumstances that could be taken into account when assessing gross negligence, such as:
            - the PSU has made a payment to a fraudster without having any reasonable grounds for believing that the payee is legitimate;
            - the PSU has made their personal security credentials including, where applicable, the devices or elements used for the second factor of authentication, openly and easily available to the fraudsters;
            - the PSU has already been a victim of the same type of fraud;

        - the PSU has disregarded warnings relating to the specific fraud type which were recently addressed to the PSU by the PSP following the outcome of transaction monitoring and/or related investigations;
        - the PSU has not notified the fraud to the PSP in a timely manner once aware of it.
    - Specifying that PSPs are liable for fraud, among other things, when:
        - they have failed to fulfil their obligations to provide the PSU with customer assistance with regards to security, as articulated in paragraph 29(d) above, in relation to the fraud experienced;
        - prior to the fraud, the fraudster has accessed the PSU's personal or account information following a data breach at the PSP, including of the kind set out in Article 9(3)(c) of DORA (which requires that financial entities' ICT solutions and processes must prevent lack of availability, impairment of authenticity and integrity, breaches of confidentiality and the loss of data).
- In relation to transaction monitoring mechanisms and fraud data sharing, among other things:
    - It is proposed that exchange of information on fraudulent unique identifiers should become an obligation rather than just an option.
    - A new provision requiring the EBA to set up a dedicated IT platform to allow PSPs to exchange information on fraudulent unique identifiers with other PSPs is inserted.
    - A new provision is added stating that where a PSP fails to block a unique identifier which was reported to it as fraudulent or involved in fraudulent transactions, the PSU won't bear any resulting financial losses.
    - There is the inclusion of a provision which states that where monitoring mechanisms provide strong evidence of a fraudulent transaction, the PSP shall have the right to block the transaction.
    - The Parliament proposes that where payment fraud results from the publication of fraudulent content online, PSPs must promptly inform providers of hosting services following the procedure laid down in Article 16 of the Digital Services Act (Regulation (EU) 2022/2065).
    - The EBA's Opinion suggests a number of further measures to strengthen the transaction monitoring provisions. These include requiring all PSPs to share fraud related data, to include not only unique identifiers/IBANs of the payee but also items such as information identifying suspected fraudsters (including names, IP addresses and phone numbers used) and information on their modus operandi. In addition and in order to fully reap the benefits of its proposed enhanced fraud transaction monitoring and data sharing measures, the EBA suggests a requirement to have a single EU-wide fraud data sharing platform, to be maintained and run by PSPs.
- The Parliament also proposes new provisions on fraud education which would require Member States to allocate 'substantial means' to invest in education on payment-related fraud, either in the form of a media campaign or lessons at schools. PSPs and ECSPs would be required to co-operate in those educational activities free of charge.
- The EBA's Opinion suggests a requirement for PSPs to provide customer assistance in relation to any security aspects of the payment service and notification of anomalies and suspected fraud, including ensuring that the PSU is able to quickly contact trained staff and that the relevant case is followed up by the PSP in a timely manner, as needed. The EBA proposes that this service should

cover at least the operating hours of the relevant payment service (ie the time span when the payment service is available to the PSU). It makes it clear that this is without prejudice to PSPs' existing obligation in relation to notifications by PSUs of the loss, theft, misappropriation or unauthorised use of payment instruments or PSUs' requests for the unblocking of payment instruments under Article 70(1)(c) of PSD2.

- In its Opinion, the EBA advises the Commission, Parliament and Council to set out requirements for a fraud risk management framework to be put in place by PSPs as part of the existing broader framework on risk management policies under PSD2 and the Regulation on digital operational resilience for the financial sector ((EU) 2022/2554) (DORA). The framework could provide for periodical fraud risk assessment based, among other things, on the fraud data collected under the PSR and could include:
    - a fraud risk statement by PSPs setting out their fraud control objectives, to be regularly revised;
    - regular monitoring by PSPs of their own fraud levels, both on the payer's PSP side and the payee's PSP side;
    - regular updating of the security measures implemented to mitigate the risk of fraud, based on the detected fraud rate and an assessment of the relevant risk faced.
- There are also EBA proposals on strengthening and harmonising the supervision of fraud management, drawing on supervisory best practices in some Member States as well as the fraud data collected under the PSD2 reporting framework.

Strong customer authentication (SCA)

- There is a proposal to remove the requirement for AISPs to apply their own SCA when the payment services user accesses the payment account information retrieved by that AISP at least 180 days after SCA was last applied.
- The Parliament provides that the "inherence" element of SCA may include environmental and behavioural characteristics such as those related to the location of the PSU, the time when the transaction occurs or the device being used.
- In its Opinion, the EBA suggests clarifying that the two SCA factors should belong to at least two different categories. It also suggests adding a requirement for PSPs to offer PSUs the possibility of setting daily or per payment limits, below or above default values set by the PSP for each payment instrument.

Open Banking

- According to the Commission's legislative proposal, ASPSPs are required to provide at least one dedicated interface for third party data access. ASPSPs must also provide PISPs with the information necessary for the initiation and execution of the payment transaction provided or made available to the PSU when the transaction is initiated directly by the PSU. Under the Parliament's proposed amendment, ASPSPs would not only have to provide the information after receiving the payment order but also any update to that information, including to the payment status, via the dedicated interface in real-time until the payment is either executed or rejected.
- The Parliament inserts a provision requiring the EBA to develop guidelines on data access for third parties.

- There is also an amendment that would require the EBA to develop draft RTS setting out a standardised list of data categories of information to be disclosed on the dashboard that banks and other ASPSPs will be required to offer to their Open Banking customers (see further 'Strengthening the EBA's role' below).

Surcharging

- There is new Recitals wording that refers explicitly to the enactment of a complete ban on surcharging across the European Union.

Enhancing transparency measures

- With regard to credit transfers and money remittances from the EU to a non-EU country, the Commission's proposal introduced an obligation for PSPs to provide PSUs with certain information, in particular: (i) the estimated time for the funds to be received by the PSP of the payee located outside the EU and (ii) (in an effective extension of the revised Cross-Border Payments Regulation to this type of transaction) the estimated currency conversion charges must be expressed, for comparability purposes, as a percentage mark-up over the latest available ECB euro foreign exchange reference rates. Here, the Parliament proposes further changes aimed at providing better information, for example to stipulate that estimated currency conversion charges should be disclosed transparently and expressed as a percentage mark-up over a foreign exchange benchmark rate which complies with the Benchmark Regulation ((EU) 2016/1011) as well as in real monetary value in the payer's currency. There is also a new stipulation that those charges shall be displayed no later than the moment when the payer authorises the payment transaction.

Strengthening the EBA's role

- The Parliament suggests mandating the EBA to develop various additional RTS or guidelines including:
    - in relation to the new anti-fraud provisions, guidelines on how the concept of 'gross negligence' is to be interpreted for the purpose of the PSR, taking into account that the term is interpreted in very different ways across the EU;
    - draft RTS setting out a standardised list of data categories of information to be disclosed on the dashboard that banks and other account servicing payment service providers will be required to offer to their Open Banking customers to allow them to see at a glance what data access rights they have granted and to whom and to cancel TPP access to their data (this is also relevant to enhancing transparency); and
    - draft RTS setting out an exhaustive list of the methods that can be used as a unique identifier (taking into account relevant market practices), which will be relevant to the proposed new IBAN/name verification service to tackle payments fraud. The Parliament proposes that the verification carried out by PSPs should not focus solely on the IBAN number but also encompass other proxies defined by the EBA. Again, these proposed amendments are also relevant to enhancing transparency.

Next steps

The Council has not yet published its proposals on the Commission's draft legislation, although we are expecting to have a general approach before the end of the Belgian Presidency on 30 June 2024. After that - and once the new Parliament is in place following the European elections on 6-9 June 2024 - trilogues (inter-institutional negotiations) will begin. The aim of these negotiations will be to reach a compromise between the texts of the three institutions.

There is added complexity to this given the European elections, which not only delay the ability to enter into trilogues but should the key personnel (rapporteurs and ECON chair) not be re-elected, our past experience suggests there could be some deviation in the negotiations if a new rapporteur takes over. Therefore while it is good news that we have the Parliament's position before the elections (thereby removing the risk of the payments proposals becoming somewhat of a political orphan), there is still some uncertainty about whether there will be any future change of course. We have seen this in the past with some files in ECON.

Also of note is that, ordinarily, the Council would have decided on its general approach on the files before the Parliament had voted through its position, which often results in the Parliament baking in room for negotiation on divergent positions. The impending elections have resulted in a reversal of the usual running order so again it's unclear how this might affect the final position on the texts.

In light of the European elections and the European Commission having to be sworn in before the trilogues can start, our current view is that the PSR could take effect in H2 2026, with PSD3 taking full effect in early 2027.

The Commission's June 2023 legislative package also included a proposal to create a financial data access (FIDA) framework. ECON published a draft report on the FIDA proposal in December 2023 and it voted to adopt the final report on 18 April 2024. Work on the first reading in the Parliament will take place in the next mandate, ie after the June elections.

If you have any questions arising from this article, please get in touch with any of the listed people or your usual Hogan Lovells contact.

Authored by Eimear O'Brien, Virginia Montgomery and Lavan Thasarathakumar.

Hogan Lovells (Luxembourg) LLP is registered with the Luxembourg bar.