EDPIA views on the European Commission proposals on the revised Payment Services Directive (PSD3/R) and Open finance

The European Digital Payments Industry Alliance (EDPIA) welcomes the European Commission's June 2023 proposals to revise the Payment Services Directive (PSD3/R) and create an Open Finance framework (FiDA) [1].

These proposals hold the promise to create a far more harmonised market in the payment sector, as well as to make Europe a leader in retail financial services beyond payments.

To make the most of this opportunity, we suggest that the following key elements are addressed:

- **Transitional provisions for licensed firms should be realistic.** Re-submitting compliance information will create a distracting burden for firms and supervisors with limited resources.
- **Safeguarding rules should address de-risking pragmatically.** It is positive that firms can rely on central banks in emergencies. This should be underpinned by clear practical mechanisms.
- **Data in scope of PSR and FiDA should be divided clearly.** The same (payment) data might fall under two overlapping rulesets, creating uncertainty. We suggest an explicit *lex specialis* rule.
- **Firms should not be made liable for things beyond their control.** To function as an incentive towards consumer protection, liability needs to focus on areas that firms can influence.
- **Non-banks should have access to infrastructure in a timely way**. The settlement finality directive amendment should ideally be adopted through the negotiations on instant payments.

Compliance assessment

The creation of distinct regulatory categories, subject to scaling requirements based on their risk-profile, has been a major legislative success for Europe's payment sector.

It is very positive to see that the text maintains the logic behind the licensing regime, including while bringing electronic money institutions and payment institutions under a single unified text.

The text requires firms established prior to the coming into force of the Directive to submit information to national competent authorities to validate their continued operation, within 24 months. We note this could be burdensome both for firms and for the authorities. Unnecessary compliance burdens could distract firms from making the most of Europe's ongoing work to unlock payments innovation.

We have not yet identified substantial problems owing to the textual merger of the EMD and PSD. Operationally, we do note that this will shorten the time that e-money firms have to safeguard customer funds from five to one day. While we understand the desire for textual elegance, we do not believe that the longer deadline for e-money firms has created any problems for the market.

EDPIA suggests:
Provide an effective grandfathering process. Ideally, firms that regularly interact with their supervisor should not need to re-submit information in a redundant manner. Firms with licences in multiple jurisdictions could also benefit from a one-stop shop. At minimum, firms that provide information within the deadline should be able to continue their operations by default if a national competent authority cannot validate them in time (which is outside the firm's control).

Align towards the longer safeguarding deadline (five days) potentially under specific criteria.

[1] See EDPIA's responses to the European Commission targeted consultation on the review of the payment services directive (PSD2) framework.

EDPIA views on the European Commission proposals on the revised Payment Services Directive (PSD3/R) and Open finance

Safeguarding

Payment firms rely on bank partnerships for several reasons, including to safeguard funds. Securing effective access to bank accounts for non-banks is practically crucial to their successful operation. The text positively introduces measures to try and prevent unnecessary de-risking by banks, including for example a formal justification and appeal process. At present it is unclear whether these measures only apply to safeguarding accounts, and it would therefore be useful to clarify that this also applies to other kinds of relationship (e.g. operational accounts).

Additionally, the text introduces the possibility for Payment Institutions (PIs) experiencing difficulties in having a payment account with credit institution to hold the funds at a central bank. EDPIA welcomes the efforts to contribute to the robustness of the payments sector.

In practice, the circumstances where a firm might turn to the central bank tend to be exceptional, for example due to the failure or termination of a banking partnership. These events can be sudden and stressful. Every day of delay can have a severe impact on a business. Relying on a discretionary assessment by a central bank in such a situation is not ideal, and different central banks might also take different approaches (creating fragmentation). While some discretionary element is probably unavoidable, given the nature of the decision, we believe that guiding mechanisms could provide market with greater clarity before such a situation emerges.

EDPIA suggests:
Clarify that measures to mitigate de-risking apply across different kinds of banking relationships.

Develop common criteria for central banks to assess payment firms when stepping in to provide safeguarding services in exceptional circumstances. An assessment should also be considered as part of the licencing process and regular supervisory activity, so that the central bank is well-prepared to react quickly in an emergency situation.

Security and fraud

EDPIA stands firmly committed to the fight against financial crime[2].

The Commission proposal notably shifts liabilities towards firms in several cases. EDPIA understands the desire to incentivize firms to combat fraud. However, it is vital that firms are given responsibilities which match their actual role down the value chain. One firm should not be forced to take on liability for something that is really controlled by a different firm. At the same time, firms choosing to outsource a specific service should remain free to agree contractually who holds the liability.

Regarding spoofing and phishing fraud (article 59), there is not much that a payment company can do to prevent a criminal from calling you and claiming that they represent the company. Indeed, in many cases the PSP cannot even be aware that is happening. It is therefore positive to see the European Commission beginning to look beyond the payment sector itself. To work as an incentive, liabilities must focus upon the actors who can genuinely do something to prevent the fraud in question. At the moment, the proposal does not provide a clear division of responsibility that matches the value chain. While telecommunications companies are required to cooperate with PSPs to counter fraud, the liability still rests with the PSP. And indeed, network operators may not themselves be the key to

[2] See EDPIA's responses to the EBA consultation on the RTS on SCA & CSC.

preventing each of these instances of fraud. More and more attacks involve mobile devices, where it may be more relevant to think about the device manufacturer than the network.

By contrast, PSPs should maintain their liability where they choose to outsource strong customer authentication (SCA) to a specific solution provider (article 58). Today, this is typically organized through commercial contracts which can have different service levels and pricing structures. Managing this liability – and the associated proof it will require – down value chains that can involve many different players will be complex. While solution providers do play an important role, it is ultimately the PSP that chooses to rely on them. Unlike spoofing and phishing issues, it is not the case that these matters are simply outside the influence of the PSP which has deliberately chosen to rely on a specific solution provider. It is not clear that this cannot simply be managed contractually as is typically the case today.

The only cases where this is not necessarily the case is where specific companies hold such a strong market presence that PSPs do not have a choice except to rely on them (and can do little to audit, control, or verify them). However, there are a wide range of technical service providers in payments today. It seems disproportionate to interfere with all actors of a specific type in order to address potential issues relating to a few specific players.

Indeed, this matter ranges beyond liability. We can see business decisions in the payments industry being increasingly influenced by decisions from a small number of players – major technology firms and card schemes – regarding the features that they choose to support and roll out. The digital markets act is a positive step in this regard, and we urge policymakers to prioritise its application to payment services.[3]

In general, EDPIA believes that strong customer authentication (SCA) has worked well. The new text noticeably allows the two factors to come from the same category (knowledge, inherence, or possession) whereas today they must come from separate categories entirely. We are concerned that this could reduce security if the independence of the two factors is not ensured effectively (as it is when they come from different categories). It is worth noting that the current requirement has not prevented the market from developing compliant solutions as it stands today.

Finally, the text introduces a requirement to support a diversity of solutions for accessibility reasons (article 88). EDPIA firmly supports the drive for digital and financial inclusion, and our members work to deliver new payment solutions suited to different situations. The current wording – which requires PSPs to cater to “all” customers – may however be impossible in a technical sense. Firms with millions of customers cannot ever really know if they have fulfilled this requirement or not. We would instead suggest requiring a “best effort” or providing a more concrete target for firms to aim towards.

[3] See EDPIA’s statement on how the DMA can boost competition in the payments ecosystem.

EDPIA suggests:
Define clear expectations for PSPs, as well as other actors, to counter the range of scams that are now in scope (including phishing and spoofing). This includes extending clear expectations and associated liability to telecommunications providers and manufacturers where relevant, and holding them liable for failing to meet their obligations. As elsewhere in the law, when firms can demonstrate that they have complied diligently with the expectations set for them, they should not be held liable. It is worth noting that this does not mean regulators should define the exact technical tools which firms should use to counter fraud, since the best practice will of course evolve over time.

Maintain PSPs liability as a rule when they outsource to technical service providers and payment scheme operators, to allow commercial negotiations to resolve these matters. In practice, the simplest solution is to delete article 58. Alternatively, only references to technical service providers could be removed given the powerful position of the card schemes in negotiations. References to gatekeepers could also be introduced in order to rebalance the negotiating position between these firms and PSPs.

Require as today that SCA factors must come from distinct categories by tweaking article 85.12.

Introduce a “best effort” approach to accessibility provisions, or clarify the expectation for firms more directly, under article 88.

Access to infrastructure

Equal access to core payments infrastructure is vital to create a level playing field between banks and non-banks. Today, non-banks are restricted by definitions set in the Settlement Finality Directive (SFD) [4].

This has important practical consequences. For example, the uptake of instant payment solutions would be supported by ensuring that non-banks can engage with them on equal terms to banks. Indeed, even after there is a legal amendment to the SFD it will take time for non-banks to apply and make use of that access.

We are hopeful that this issue can be addressed as part of the ongoing negotiations on the instant payments regulation, considering that the market is taking shape rapidly. If this proves not to be the case, then we hope that an amendment to the Settlement Finality Directive can be pursued with a short implementation timeline separate from the more complex negotiations on the PSD2 review.

EDPIA suggests:
Amend the SFD through negotiations on instant payments, with a 6-month implementation timeline after the entry into force of the Regulation.

[4] See EDPIA’s joint industry letter on amending the Settle Finality Directive (SFD) alongside the Instant Payments proposal.

EDPIA views on the European Commission proposals on the revised Payment Services Directive (PSD3/R) and Open finance

Open Banking and Open Finance

The review of PSD2 is an opportunity to reduce fragmentation. In this context, EDPIA welcomes the transfer of the relevant provisions based on EBA standards into the text of the Regulation and the efforts to specify in more detail the minimum requirements for open banking data interfaces.

In parallel, the FiDA proposal aims to expand customer's legal right to share their financial-sector data beyond the scope of open banking. This would ultimately require a wide range of financial entities to share this with authorised third-parties through standard interfaces. Considering that payments data is already covered under PSDR, we see a risk that the same data is covered by overlapping rules, and recommend clarifying this interaction.

Considering our experience with PSD2, we support the introduction of compensation in order to provide firms with a sustainable incentive to invest continuously in their user experience and functionality. While EDPIA understands that a compensation model for data holders can be a useful way to encourage ongoing investment into the data sharing ecosystem, the overarching goal of FiDA should be to empower users to share financial data not currently covered under PSD2. This means that the level of compensation for data holders should be calculated from scratch using a cost-based approach, as artificially high fees for data access would risk eroding the savings that FiDA promises to bring end-users. Ultimately the goal should be to benefit users. Regulators should engage closely with the industry through the scheme development process to monitor the standards and ensure a sustainable business model.

EDPIA generally supports the Commission's push to provide clear baseline expectations for data access interfaces, which has been a well-known pain point for PSD2 implementation. Some specific requirements could merit technical scrutiny by the co-legislators, however. Article 36.4.g requires firms to allow PISPs to verify the name of account holders before a payment is initiated, which could raise privacy concerns. Article 36.5.b requires account providers to confirm to PISPs that a payment will be executed, which should clearly by subject to any fraud prevention measures implemented by the account provider (which might rightly prevent the transaction).

In general we are in favour of the attempt to provide legal clarity, however, mechanisms to update elements that turn out to be difficult in the future would be welcome considering how granular the rules are. It will be important to make sure that each element fits other European and national law.

EDPIA suggests:
Clarify that payments data subject to the revised Payment Services Directive (PSD3/R) is *lex specialis* and not subject to FiDA.

Introduce mechanisms, including in the governance rules, to ensure that artificially high compensation levels cannot undermine FiDA's objectives.

Tweak specific requirements relating to the data access interfaces to balance access against privacy concerns and reflect the fraud management process. Mechanisms to keep these elements up to date would be welcome, while maintaining the drive for legal clarity.