Brussels, 31 October 2023

European Commission's Proposal for Payment Services Regulation and Payment Services Directive 3

EACB position

The **European Association of Co-operative Banks** (EACB) is the voice of the cooperative banks in Europe. It represents, promotes and defends the common interests of its 26 member institutions and of cooperative banks in general. Cooperative banks form decentralised networks which are subject to banking as well as cooperative legislation. Democracy, transparency and proximity are the three key characteristics of the cooperative banks' business model. With 2,700 locally operating banks and 40,000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 227 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 89 million members and 720,000 employees and have a total average market share of about 20%.

For further details, please visit www.eacb.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eacb.coop • e-mail : secretariat@eacb.coop

1 Introduction

On June 28, 2023, the European Commission released a package of legislative proposals on financial data access and payments[1]. As part of the package, the Commission proposes to amend the current Payment Services Directive (PSD2), which would be replaced by Payment Services Directive 3 (PSD3) and Payment Services Regulation (PSR). PSD3 will regulate the licensing and supervisory requirements for payment institutions, while PSR covers conduct rules and operational requirements for payment and electronic money service providers. The draft PSR is of a particular importance to EACB members since cooperative banks offer a wide range of payment services to their customers.

The EACB actively contributed to the PSD2 review process with our input reflecting the views of cooperative banks across the EU[2]. We believe that PSD2 has brought benefits for payment users by making payments safer and more secure through the implementation of strong customer authentication, although new kinds of fraud have developed, and the methods used by fraudsters changed after the implementation of PSD2. Besides that, PSD2 has created a market for third-party providers (TPPs), created more trust with consumers in sharing customer data, and has proliferated APIs. The EACB considers that retail payments sector is well regulated by a broad range of EU legislative acts and further regulatory intervention is not warranted.

The proposal for a draft PSR contains a number of positive provisions with regard to the open banking, e.g. access to customers' payment accounts by TPPs would only be possible via dedicated interfaces (API); no new EU API standard would be imposed on market actors; orientation of APIs towards international industry standards, such as the Berlin Group interface; small banks that have very limited or no data traffic through API would be allowed to ask national competent authorities an authorisation not to offer APIs and any other interface. We also welcome the proposal to enable merchants to offer cash withdrawal service up to EUR 50 (even in the absence of any purchase of goods or services) without the need to obtain a payment institution license (Art. 37 PSD3). Cash in shop would be an alternative option for users to access cash and complement current possibilities.

Notwithstanding the above positive developments, we have strong concerns regarding a sizeable negative effect and unintended consequences that other proposals under the draft PSR could have for the functioning of the EU payments market. Contrary to the Commission's announcement that its regulatory proposals represent an evolution not a revolution of the EU payments framework, our initial assessment is that there are surprisingly many detailed changes compared to the previous regulatory texts. An extensive revision of PSD2 will leads to high complexity and involves potentially unintended interactions. Second, one of the key lessons learned from PSD2 was that open banking cannot work properly without a sustainable business model, i.e. a fair distribution of value and risk among market actors is needed. However, the Commission's proposal would maintain the existing status quo with a free of charge access to bank customers' payment account data by TPPs. Third, by shifting liability for authorized fraudulent transactions to payment services providers PSR would undermine the current balance between liability of payment service users and PSPs in case of fraud and would have negative consequences for market actors without tackling the source of the problem (e.g. social engineering fraud).

In the following sections we have set out the EACB comments and proposals for changes to the draft PSR, and, to a lesser extent, to the draft PSD3.

[1] Financial data access and payments package, 28.06.2023: https://finance.ec.europa.eu/publications/financial-data-access-and-payments-package_en

[2] EACB response to the Commission's targeted consultation on the review of PSD2, 19.07.2022: https://www.eacb.coop/en/payment-systems/position-papers/eacb-response-to-the-targeted-consultation-on-the-review-of-the-revised-payment-services-directive-psd2.html

2 Open banking

Articles 35-48 of the draft PSR cover the provisions related to open banking.

Business model: PSD2 has not ensured equal treatment of the interests of Account Servicing Payment Service Providers (ASPSPs), in particular credit institutions, and other providers, and has in effect established an uneven playing field. Regardless of their respective clients' needs and whether they use the services of Third-Party Providers (TPPs), ASPSPs were forced to establish an expensive infrastructure without the possibility of recovering the costs incurred. At the same time, the full economic opportunities have been to the sole benefit of the TPP.

We strongly advocate that PSR redresses this situation and lays the foundations for a sustainable business model for open banking instead of preserving the current status quo. TPPs should not be able to continue accessing payment accounts data free of charge, while ASPSPs pay the costs of the infrastructure. A sustainable business model is all the more important since the draft PSR imposes further investment costs on ASPSPs, such as minimum API performance criteria, introduction of additional API functionalities for the benefit of TPPs (Art. 36), the imposition of several methods of customer authentication (Art. 44.1.(k)) and an obligation to set up a dashboard allowing consumers to better manage access to their data by third-parties. Future level 2 texts (RTS) should avoid disproportionate costs on ASPSPs due to new requirements.

It is worth noting that the Commission proposal for a Financial Data Access Framework (FIDA) is more market-oriented as it would allow ASPSPs charging financial information service providers for the provision of data. PSR should adopt similar approach.

Contingency measures for an unavailable dedicated interface: We welcome the Commission's intention to ban screen scraping. However, while Art. 35 PSR puts an end to permanent fallback interface, Art. 38 requires ASPSPs to offer an effective fallback solution in case of API's unavailability, i.e. ASPSPs will de facto be obliged to maintain the fallback interface, including those ASPSPs that are currently exempted from the fallback. Art. 38 waters down the Commission's intention to ban screen scraping, plus imposes additional costs on ASPSPs. Consequently, the wording of PSR should be amended to make sure that TPPs can only access customers' payment accounts via dedicated interfaces that are reliable and robust. No fallback options should be possible, similar to the approach adopted in FIDA.

Consumer dashboard: The Commission has proposed the implementation of dashboards with the aim to give payment service users greater control over their data (Art. 43 PSR). That said, we suggest the following adjustments to the draft proposal. First, the PSU should be able to know and manage the consent not only as given to the TPP but also as if it was given to the ultimate recipient of the data, since the PSU may be familiar with the ultimate recipient of the data and not with the TPP (in case of license-as-a-service). Second, the implementation and maintenance of the dashboards will impose additional costs on ASPSPs, which need to be taken into account in the fees that ASPSPs should be allowed to charge TPPs for data access. Finally, it is important to ensure that the requirements for dashboards are harmonized between PSR and FIDA: a single dashboard should be set up to serve both purposes of PSR and FIDA.

Introduction of additional functionalities for APIs: Banks will be forced to develop free functionalities for TPPs, that TPPs will be able to monetize. For example:

- Art. 36.2 (d): see, prior to initiation of the payment in the case of payment initiation service providers, the unique identifier of the account, the associated names of the account holder and the currencies as available to the payment service user.

- Art. 36.4 (g): verify the name of the account holder before the payment is initiated and regardless of whether the name of the account holder is available via the direct interface.
- Art. 36.5 (a): the immediate confirmation, upon request, in a simple 'yes' or 'no' format, of whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer.
- Art. 36.5 (b): the confirmation from the account servicing payment service provider that the payment will be executed on the basis of the information available to the account servicing payment service provider, taking into account any pre-existing payment orders that might affect the full execution of the payment order being placed.
- Art. 36.5 requires banks to provide PISPs with services that they do not offer their own customers.

Imposing several methods for customer authentication: Banks will have to offer several authentication solutions to TPPs, which again entail development and maintenance costs (Art. 44.1.(k)). Banks should remain free to choose their own security mechanisms, given the risks they incur. As long as TPPs are not exposed to the risk, they should not be allowed to impose their operating methods.

Changes to API specifications: The requirement to make available any change to the technical specifications of APIs to PISPs, AISPs and PSPs at least 3 months before a change is implemented is unbalanced and will slow down innovation in the market (Art. 35.4 PSR). The wording should be adapted as follows: *"…as soon as possible, at least two weeks before the change is implemented".*

3 Fraud prevention, processing and exchanging information

Banks put in place significant resources to fight fraud and protect their customers' funds. Therefore, we welcome the initiatives that contribute to that goal.

IBAN-Name check: The Commission proposes to extend the IBAN-Name check, also called confirmation of payee, to all credit transfers (Art. 50 and 57 PSR). We wanted to point out that the full introduction of an IBAN-Name check involves significant costs and legal and operational challenges, besides raising serious doubts about its effectiveness in reducing fraud, e.g. as those using social engineering.

But if the co-legislators, despite all concerns, decide to introduce the above-mentioned obligation for PSPs, a full consistency in terms of functionality and liability rules with the parallel requirements for instant credit transfers (amended SEPA Regulation) should be ensured.

The interaction with the other proposed anti-fraud regulations should be clarified by law. For example, it would be desirable that discrepancies resulting from IBAN-Name check can be used for data exchange between PSPs under Art. 83 PSR. The payer's bank should also be enabled to use the findings from the IBAN-Name check for its own fraud prevention processes. If it turns out that certain IBANs are being used by payees for fraudulent purposes, the payer's bank should be granted the right under Art. 65 PSR to reject further payment transactions in favour of such a fraudulent IBAN altogether.

Likewise, it should be clarified that due diligence obligations for PSUs may arise from the offering of the IBAN-Name check service, which may have an impact on liability rules (in particular Art. 59 PSR).

The liability in Article 57 PSR, which also includes consequential damages, should be able to be designed and limited by the national legislators in analogy to the provisions in Article 56.6 PSR.

Whether a credit institution should be liable for any consequential damages is a question of attribution. A credit institution would only be able to assess this question if it were to inquire about the "loss potential" of each credit transfer. However, this is not possible in the mass business of payment transactions. The credit institutions would therefore have to insure themselves against such risks, which would increase costs and ultimately be to the disadvantage of the customer. This disadvantage can only be avoided by the possibility of limiting liability for consequential damages, as has been codified in respective national legislations.

When it comes to pricing, we believe that PSPs should be allowed to charge users for IBAN-Name check service since it will involve significant implementation costs.

Fraud data sharing: We welcome the possibility to share suspicious customer identifiers between PSPs in line with data protection rules (Art. 83 PSR). In our opinion, in addition to the multilateral platform solution proposed by the Commission, bilateral exchanges between PSPs should also be possible.

Art 83.3 provides that *"Sufficient evidence for sharing unique identifiers shall be assumed when at least two different payment services users who are customers of the same payment service provider have informed that a unique identifier of a payee was used to make a fraudulent credit transfer".* This provision seems excessive when the objective is to stop fraudulent payments without delay. It is unclear why there needs to be the precondition that the two PSUs must be customers of the same PSP. It should be enough that the PSP's internal controls and fraud prevention methods identify the bank account to be used fraudulently. This would enable sharing and blocking suspicious account identifiers even before any fraudulent transactions occur.

Besides, only sharing information on fraudulent identifiers is insufficient – where there is sufficiently clear evidence that an IBAN has been used to commit fraud, it should be blocked.

Besides sharing customer identifier, TPPs, acquirers and merchants should be obliged to exchange extended information on location data, environmental and behavioural data.

Finally, PSPs should be able to block incoming payments in the event of suspected fraud.

Strong Customer Authentication: We welcome that the Commission recognizes the success achieved in combating fraud with the use of SCA and confirms that SCA requirements will remain (Art. 85-89 PSR). At the same time, our view is that SCA provisions in draft PSR require some improvements:

If both elements of SCA belong to the same category (e.g. "what we know"), SCA quality might be undermined (Art. 85.12 PSR). Therefore, we would argue against this provision.

There should not be a binding obligation on ASPSPs to allow AISPs to conduct their own SCA (Art. 86.4 PSR). Otherwise, the security of payments might be compromised. In our opinion, the possibility for AISPs to use their own SCA could be bilaterally agreed between ASPSPs and AISPs.

Accessibility requirements (Art 88): Solutions for vulnerable users are ensured by the European Accessibility Act, thus we see no added value in Art. 88. In case PSR mandates the provision of alternative (non-smartphone-based) SCA methods, maximum one such alternative method per PSP should be mandated by law, leaving it up to PSPs to possibly offer more options, and market-based pricing of alternative SCA methods should be possible.

4 Liability in case of fraud and scam

PSD2 already contains a balanced liability regime that comprehensively protects users in case of unauthorized transactions.

The fight against scams is a priority, both for PSPs and for regulators and supervisors. In the fight against authorised push payment (APP) scams in particular, the emphasis should be on preventing the scam and identifying the criminals. All parties in the scam chain must be part of the fight against scams.

Liability for scam losses: By contrast, extending liability for authorized payments through social engineering (Art. 59 PSR – PSPs liability for impersonation fraud) is unbalanced and would make credit institutions responsible with risks that in actual fact lie outside their of control. In the case described in Art. 59, the bank is also victim of spoofing and would be doubly penalized: its identity is usurped, and it must reimburse the fraud.

Furthermore, it is unclear how such a liability shift would effectively prevent fraud. On the contrary, we see a risk that fraudsters will exploit these provisions and the related losses could increase and also exacerbate other risks, e.g. in the area of money laundering[3]. Such a liability shift would create false incentives for clients to be less diligent, as they would have the impression that the credit institution is always liable (full coverage mentality). This is also extremely problematic in view of the envisaged distribution of the burden of proof. We strongly advocate against changing the current liability regime in case of scam (authorized fraud). The focus should rather be on preventing fraud and scam in close cooperation among all relevant actors.

Electronic communication services providers: In principle, we welcome the proposal to involve electronic communications services providers in fraud prevention (Art. 59.5 PSR). The following amendments should be made in that respect:

- Provide a definition for "electronic communication service providers'' and include telecommunications companies and mobile phone operating system developers in the definition.
- In the event of a failure that can be attributed to an electronic communications service provider, the latter should be liable and bear all losses incurred by the payer.

Gross negligence: We advocate for limiting liability of the ASPSP to exclude cases of gross negligence or intent of the PSU. Art. 59.3 PSR stipulates *"… shall not apply if the consumer has acted fraudulently or with gross negligence"*. We believe this principle should be extended to every Article related to liability in order to prevent moral hazard and "careless behaviour" of PSUs.

Furthermore, the term "gross negligence" should be defined in an article, and not only described in recital 82. Providing a list of criteria would bring further clarity to the term and proper liability allocation between the PSP and the PSU. For example, the following criteria could be used:

- A fraud victim who has been made aware of the risks of fraud could be considered as acting negligently.

[3] Referring to the experience of the Dutch payment service providers, a liability shift does not reduce bank-employee impersonation scams. In 2020, Dutch banks decided to compensate damages caused by 'bank-employee impersonation scam' out of leniency. But the number of scams has not decreased. The Dutch example shows that placing liability on banks does not decrease bank-employee impersonation fraud.

PSUs forwarding sensitive payment data to third-parties despite the recurring information that the bank will never ask for credentials/sensitive data on the phone or via mail could be considered as acting negligently.

5 Payments involving third countries

Given that the application of EU payment services legislation is limited to EU Member States, provisions for payments involving third countries remain exceptional. Expanding the information requirements for PSPs concerning execution times and currency conversions for credit transfers to third countries is not appropriate (Art. 13 and 20 PSR). Due to the limited reach of the EU payment services legislation on a global scale, a PSP cannot provide information on certain aspects beyond its direct control. Moreover, providing this supplementary information might potentially confuse customers and burden existing customer information with additional content.

6 Access to payment systems

The draft PSD3 amends the Settlement Finality Directive (SFD) by adding payment institutions to the list of PSPs that may be direct participants in payment systems.

In general, we are not in favour of amending SFD to allow payment institutions (PIs) and electronic money institutions (EMI) direct access to payment systems, including those designated by Member States. The different supervisory requirements for credit institutions versus PIs and EMIs beyond the scope of payments services legislation can result in different risk profiles with corresponding effects on payment systems and their participants.

However, should PIs and EMIs be provided with direct access to payment systems, they should be subject to the same obligations as credit institutions and only be admitted after an appropriate risk assessment.

7 Sanctions

In our view, the range of penalties stipulated in Art. 97.2(a)(i) and (ii) PSR (maximum administrative fine of at least 10% of its total annual turnover for legal persons or EUR 5.000.000,- for natural persons) is disproportionate to the severity and impact of any violations of the provisions listed in Art. 97.1 PSR.

It must be borne in mind that the current legal framework stipulates "only" administrative fines up to EUR 60.000,- in case of an infringement of the PSD2 framework.

We consider that administrative sanctions and other administrative measures for specific infringements should be scaled back to a level which is proportionate to the severity and impact of an infringement of provisions listed in Art. 97.1 PSR.

8 Implementation timelines

In the past few years banks and other PSPs have invested huge financial and human resources to comply with numerous pieces of EU legislation such as SEPA Regulation, Interchange Fee Regulation, Payment Accounts Directive, PSD2, AML/CTF directives, without necessarily being offset by new or additional revenues. Furthermore, new legislative acts such as the Digital Euro Regulation and Regulation on legal tender of cash are currently being scrutinized by the co-legislators.

It is important to take into account the combined effects of relevant legislation and allow appropriate implementation timelines to market actors. Based on the experience gained from the

implementation of PSD2, we believe that the implementation timeline for various provisions of PSR and PSD3 should be at least 24 months.

Supplementary implementations with IT related effects, such as the proposed requirements under Art. 50 and 57 PSR (IBAN-Name check) would require an implementation period of 36 months.

In addition, based on the experiences with PSD2, early planning for the implementation of level 2 measures (e.g. RTS) is important – divergent implementation deadlines for regulatory areas that involve dependencies with regard to their technical or customer-contractual implementation must be avoided in order to enable efficient implementation for the benefit of the institutions and their customers.

Contact:

The EACB trusts that its comments will be taken into account.

For further information or questions on this paper, please contact:

- Ms Marieke van Berkel, Head of Department (m.vanberkel@eacb.coop)
- Mr Farid Aliyev, Senior Adviser, Payment Systems (farid.aliyev@eacb.coop)