Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Payment Services Regulation

Comments on EP and Council mandates with a view on the upcoming trilogue

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:

Wulf Hartmann
Director
+49 30 1663-3140
wulf.hartmann@bdb.de

Albrecht Wallraf
Associate Director
Telephone: +49 30 1663-2312
albrecht.wallraf@bdb.de

Berlin, 28 August 2025

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public banks, the Deutscher Sparkassen- und Giroverband (DSGV),
for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks. Collectively, they represent approximately 1,700 banks.

Coordinator:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin | Germany
Telephone: +49 30 1663-0
www.die-deutsche-kreditwirtschaft.de
www.german-banking-industry.org

Content

I. Introductory Remarks

This document aims to contribute to the co-legislators' efforts during the upcoming trilogue for the Payment Services Regulation (PSR)[1] under consideration of the EP mandate[2] and Council mandate[3], respectively.

It addresses the following **regulatory areas** of the PSR:

- Fraud prevention and liability
- Transparency on fees
- Third-party providers
- Strong customer authentication
- Relation to MiCAR
- Implementation feasibility and unintended consequences

II. Fraud prevention and liability

1. General remarks

If the PSR is to reasonably contribute to reducing fraudulent attacks on payment service users and the losses resulting from fraudulent attempts, it is crucial to ensure a fair balance between instruments for fraud prevention and the liability regime in fraud cases.

To place the subsequent observations on individual provisions in context, we assess the starting position for the trilogue as follows:

- We are very pleased to see that the EP mandate and the Council mandate, respectively, further improve provisions on instruments for fraud prevention (in particular Articles 51, 65, 69, 83). However, we still see considerable need from improvement to facilitate their effectiveness.
- We continue to view the unilateral transfer of liability for impersonation fraud to the payer's PSP in Article 59 in a very critical light. This is because it places risks on PSPs that they cannot control. The EP mandate's proposed extension of the scope of application of Article 59 PSR would tip the balance even further into an unsustainable situation: banks would then become liable in cases where the underlying fraud takes place outside the bank's spheres of influence and detectability. Such a regime would not reduce fraud but merely shift its economic impact, disadvantaging payment products and all customers over time. Furthermore, fraudsters would exploit such chain of effects and in fact intensify fraudulent attacks on consumers with adverse implications far beyond payments.

[1] Proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (COM(2023) 367 final)

[2] European Parliament, Legislative resolution of 23 April 2024 on the proposal for a regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 (COM(2023)0367 – C9-0217/2023 – 2023/0210(COD))

[3] Council of the European Union, Payment Services Regulation (PSR) - Mandate for negotiations with the European Parliament of 18 June 2025 (10268/25)

- The interplay between individual instruments for fraud prevention and liability in fraud cases should always follow principles of proportionality and accountability: effective and unambiguous provisions help banks to fulfil their obligations as well as to derive due diligence obligations of payment services users.

2. Authorisation (Article 49)

We welcome the fact that that the co-legislators maintain a high degree of consistency in the concept and definition of "authorisation" compared to PSD2. To increase legal clarity, we suggest adopting the Council's wording, i.e. choose "give consent" instead of "give permission".

3. Discrepancies between the name and unique identifier of a payee in case of credit transfers and related liability rules (Articles 50 and 57)

The inclusion of any "verification of the payee" obligations in the PSR should be taken as an opportunity to correct weaknesses in the related provision in Article 5c of the SEPA regulation[4].

In light of this, both Council and EP mandates are still missing the following aspects:

- The right of payers who are non-consumers to opt out from receiving the service is currently too narrowly defined, i.e. only in the case of bulk payments. Non-consumers should have a general and unconditional opt out right to avoid unnecessary verification procedures that impede their payment processing.
- Article 57 must exclude the payer's PSP's refund obligation in cases of fraud or gross negligence on the part of its customer. This is necessary to account for specific mechanisms of "verification of the payee"-services and the customer's ongoing due diligence obligations. The Council's proposal to delete paragraph 5 should therefore be reversed.

Furthermore, it is crucial to limit the geographical scope of Article 50 to intra-EEA credit transfers, as rightly provided for in the addition to Article 2(5) in the Council Mandate. An additional clarification in Article 50 regarding the geographical scope could further increase clarity.

To ensure regulatory clarity, co-legislators should consider withdrawing Article 5c of the SEPA regulation and regulate the verification of the payee issue completely and exclusively in the PSR.

4. Limits and blocking of the use of the payment instrument (Article 51)

Limits on and the option to block payment instruments are a key factor for preventing losses as a result of fraud. Therefore, we welcome the valuable considerations of the co-legislators

[4] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro

designed to further strengthen Article 51. In particular, the amendments proposed by the Council Mandate should be pursued, including the intended extension to "means of payments".

However, the following aspects should be reconsidered:

- Any increase of spending limits on the use of the payment instrument by the payment service user has to rely on the consent of the bank. This enables the PSP to continue managing its risks. In each such case, the principle of agreement between the PSU and the bank must not be undermined.
- While a regulatory minimum delay period may be justified, the suggested maximum duration of 12 hours should be deleted (paragraphs 1 and 5 in accordance with the Council Mandate). 12 hours is not sufficient for maintaining the intended protective function in all cases. Furthermore, fraudsters could exploit a strict and uniform maximum duration in their interaction with victims.
- The unilateral possibility for PSUs to opt out of the application of a delay period contradicts the intended protective function and must be deleted ("*The payment service user shall have the right to adjust or opt out of the application of such a delay period.*", see paragraphs 1a and 5 according to the Council Mandate).
- The suggested strict separation of channels for the activation of mobile devices would severely impact customer convenience, in particular in the context of "mobile first" account packages addressed to digitally savvy PSUs. The respective clause should be deleted ("*[…] and the use of different communication channels to activate the mobile application on a new device […]*", see paragraph 5 in accordance with the Council Mandate).
- Given the comprehensive scope of Article 51 in the version of the Council Mandate, Article 5a paragraph 6 SEPA regulation should be deleted to prevent inconsistencies.

5. Obligations of the payment service provider in relation to payment instruments (Article 53)

Article 53 paragraph 1 correctly stipulates that PSUs must be enabled to submit notifications leading to the blocking of payment instruments quickly and easily. However, the EP Mandate's provision that a *"[…] communication channel allowing for human support […]"* shall be present at all times is unduly strict and should be discarded: it underestimates the effectiveness of digital forms of interaction, including AI-supported phone services, and would represent a disproportionate burden for many PSPs with no clear countervailing benefit for PSUs.

6. Evidence on authorisation and execution of payment transactions (Article 55)

In order to ensure legal certainty, we welcome the fact that the co-legislators maintain a high degree of consistency as compared to PSD2. The amendments included in the Council Mandate appear suitable both to further increase clarity and to rectify those ambiguities in the Commission proposal that could have potentially detrimental effects (e.g. restoration of the term *"necessarily"* in paragraph 2 to facilitate consistency with jurisprudence regarding prima facie evidence).

7. Payment service provider's liability for unauthorised payment transactions (Article 56)

We are strongly in favour of the co-legislators' proposal to extend the period defined in paragraph 2 to 15 business days: this correctly reflects that the analysis of complex circumstances requires a reasonable timeframe in order to reach conclusions that do justice to the interests of both the customer and the PSP.

8. Payment service provider's liability for impersonation fraud (Article 59)

Following on from the explanations under "General Remarks", we continue to view the unilateral transfer of liability for impersonation fraud to the payer's PSP in Article 59 in a highly critical light. This is because it places risks on PSPs that they cannot control. It creates false incentives for clients to be less diligent, as they then have the impression that the credit institution is always liable ("all-risks-insured mentality").

Extending the scope to include all kinds of impersonation fraud as suggested by the EP mandate, in particular, must be rejected. Any assumption of liability for fraud cases outside the PSP's sphere of influence inevitably leads to adverse effects on customers, banks and the overall target of fraud reduction.

Against this backdrop, we welcome that the Council at least aims at limiting such liability to the case of "bank employee impersonation fraud". The following additional aspects must be considered if outcomes are to be satisfactory:

- In order for this rule to work as a guiding mechanism and, ideally, reduce fraud, the PSP must be able to establish a concrete link to its own behaviour. In that regard, the Council's proposed wording under paragraph 1 on the lines of communication allows for a better alignment with the PSP's concrete processes and how these could be improved: The suggested wording *"[…] communication channels attributed to the consumer's PSP […]"* should therefore be adopted, whereas the more arbitrary listing *"[…] the name or e-mail address or telephone number […]"* should be dismissed.
- We welcome the EP's amendment to exclude refund rights for the payer in the event that the payer refuses to support the PSP's investigation (Article 59 paragraph 3).
- Credit institutions cannot bear unlimited liability risks outside their sphere of influence, especially since these are not insurable. Therefore, the total reimbursement claim under Article 59 PSR must be capped.
- If the customer is comprehensively informed by their credit institution regarding precautionary measures to prevent fraud in accordance with Article 84, this must also find expression in the civil law relationship. If the customer violates their contractual duty of care in that regard, this should be able to be classified as gross negligence and reflected in Article 59 PSR accordingly.
- We welcome the Council's suggested extension of the period mentioned in paragraph 2 to 15 business days which is also in line with the proposed amendments to Article 56.
- The Commission proposal and the co-legislators' mandates correctly reflect that only consumers should be covered by the protective purpose of dedicated liability rules, if at all. However, any intended consumer protection considerations should not lead to regulations that weaken consumers' individual responsibility and vigilance: an adequate

liability cap is therefore essential, both to avoid excessive risks for account servicing PSPs and to ensure alignment with the legislation's intended regulatory purpose.

Please note the following section in regard to the inclusion of Electronic Communication Service Providers (ECSPs) in the proposed provisions.

9. Cross-sectoral cooperation for the purpose of fraud prevention and detection (Articles 59 and 59a within the Council mandate)

We welcome the approach to extend fraud prevention responsibilities to other sectors such as telecommunications and platform providers (electronic communications service providers - ECSPs).

The different approaches for addressing ECSPs, as suggested by the Commission, the EP and the Council, are a testament to the shared insight that effective fraud prevention cannot be limited to banks' efforts. Fraud originating the digital sphere is not limited to payments and its societal risks in terms of economic losses and impaired trust extend far beyond payments. However, we doubt that these approaches – and the scope of the PSR in general – will achieve a sufficiently comprehensive outcome in this respect.

For an effective implementation, however, sector-specific regulation needs to be adapted to clearly define the relevant obligations, ideally on the basis of harmonised European rules. Such provisions must include more comprehensive prohibitions on, inter alia, caller ID spoofing, the explicit authorisation to deploy SMS content firewalls, and the ability to exchange fraud-related information to detect and stop fraudulent transactions.

We therefore urge legislators to

- … formulate obligations in the PSR specifically for ECSPs which are precise and uniformly applicable across the Union and directly aimed at raising customer awareness and their interaction with banks (e.g. dedicated communication channels and obligations resulting from the notification of fraudulent attempts). Here, complementing ECSPs' obligations with dedicated liability rules as suggested by the EP may be appropriate if the provisions allow for a meaningful attribution to fraud-induced losses.
- … formulate provisions in the PSR addressed at ECSPs which clarify that the prevention of fraudulent attempts resulting in "push payment fraud" are inherently part of their general obligations to prevent misuse of their services – as well as possible liability implications.
- … assess legislative action and other suitable measures aimed at strengthening resilience against fraud across all relevant industries, public sectors and citizens (see our comments below regarding Article 83b of the Council mandate).

10. Blocking of suspicious payments by the payer's or payee's PSP (Articles 65 and 69)

We strongly welcome the fact that both the EP and Council have included provisions that increase legal certainty when blocking the execution or crediting of suspicious payments. This

is a logical and beneficial complement to the provisions on blocking payment instruments according to Article 51. Furthermore, establishing a reference to the provisions on the transaction monitoring (Article 83) further strengthens the latter instrument's effectiveness. Lastly, the intended definition of subsequent steps to resolve a suspected case make it possible to outline a plausible mechanism of action.

We urge the co-legislators to assess, on the basis of the comprehensive version in the Council mandate, whether Articles 65 and 69 require further improvement in conjunction with Article 83 in order to achieve the intended goals and to avoid conflicting provisions.

In that regard, the version of the Council mandate should be adopted and supplemented by the following amendments:

- The last sentence of Article 65 paragraph 1 should be dismissed, as its meaning is ambiguous and could thus contradict PSPs' efforts (*"For the purpose of this Regulation, the fact that a payment order is unusual shall not by itself constitute reasonable grounds to suspect fraud."*).
- Article 65 and the related Article 110c commendably provide for the special circumstances of instant credit transfers from the perspective of a payer's bank. By contrast, Article 69 still lacks equivalent provisions for the payee's bank: Article 69 paragraph 2a should be extended to clarify that in the case of instant credit transfers the incoming payment shall be rejected by the payee's bank. This avoids conflicts with the provision of the SEPA regulation and the premises of SEPA instant credit transfers in general.
- It is unclear why Article 69 paragraph 2a presumes that the payee's bank *"may"* postpone making the funds available in cases of suspected fraud: in accordance with the analogous provision in Article 65, the suspension of making funds available should be formulated as an obligation (i.e. *"shall"* instead of *"may"*).

11. Transaction monitoring mechanisms and fraud data sharing (Articles 83 and 83a)

<u>Remarks on provisions for transaction monitoring (Article 83):</u>

The PSR will significantly strengthen the role of the transaction monitoring for fraud prevention, not least in conjunction with the provisions on stopping suspicious payment flows (see previous section on Articles 65 and 69).

In light of this, we particularly appreciate the Council Mandate's intention to further specify the parameters applicable for the payer's bank and payee's bank, respectively. Nevertheless, the following improvements should be considered:

- *Liability and payer's refund right (paragraph 1a of the Council mandate):*
  Neither the EU Commission nor the EP has deemed separate liability regulations necessary. The goal of Article 83 is to regulate the purpose and scope of transaction monitoring as a fraud prevention measure in a uniform manner across the EU and to create legal certainty. A separate liability regime is not necessary for this purpose. It carries the risk of giving rise to more legal disputes between PSUs and PSPs. The existing liability regime for unauthorized payments already provides sufficient protection

for PSUs. In addition, the burden of proof in liability cases proposed by the Council for PSPs would mean that in legal disputes PSPs would have to disclose the details of how their transaction monitoring mechanisms work. Such disclosure would be counterproductive. Effective fraud prevention depends largely on the confidentiality of the procedures used. Details should only have to be disclosed to banking supervisors and data protection authorities for supervisory purposes.

If, however, legislators were to follow the Council's proposal to include a dedicated liability provision, the exclusion of the bank's liability may not be limited to cases of fraud on the part of its own customer. It must also include instances of gross negligence by the PSU. This is necessary to account for their ongoing due diligence obligations, which cannot be substituted by the banks' transaction monitoring. Furthermore, an appropriate time limit for the refund is essential yet still lacking: an alignment with the time limit specified in Article 54 could be appropriate here.

- *Data relevant for transaction monitoring of the payer's bank (paragraph 2 of the Council mandate):*
  The Commission, EP, and Council want to exhaustively regulate and limit the types of data for transaction monitoring in paragraph 2, sentence 2 (Commission/Council = "limit", EP = "include"). Based on the experience credit institutions have in current fraud prevention today, we know that this approach is not flexible enough. Fraud models can change, particularly due to technological progress. PSPs must be able to respond appropriately to such developments when monitoring transactions. Consequently, the provision must be flexible. The list of data types cannot, therefore, be exhaustive. Greater emphasis should also be placed on the fact that the purpose of fraud prevention is crucial in determining which types of data may be processed. Consideration should also be given to how the expert knowledge gathered in the "Platform on combating fraud" (Art. 83b Council proposal) can be used to decide which data may be used in transaction monitoring.
  Furthermore, the provision should recognise that not all data elements listed may be available for every payment situation (in particular "environmental and behavioural characteristics" according to lit. (e)).
  Both aspects could be mitigated by the following clarification in sentence 2:

  "Processing by the payment service provider of the payer ***may include the non-exhaustive list of*** *the following data, insofar as* ***available to the payment service provider and*** *necessary to achieve the purposes referred to in paragraph 1"*.

- *Data relevant for transaction monitoring of the payee's bank (paragraph 2 of the Council mandate):*
  The above change should also be made in the sentence preceding the list of data elements applicable by the payee's bank. Furthermore, as regards lit (c), (d) and (e), it must be clearly specified that these data shall refer to the payee and not to the payer: the payee's bank does not (and should not) possess such information on the payer, as a general rule. One exception to this constitutes the name of the payer which can be known to the payee's bank in certain circumstances.

Remarks on provisions for fraud data sharing (Article 83 and Article 83a of the Council mandate, respectively):

As with transaction monitoring, adequate provisions on fraud data sharing have the potential to significantly increase the effectiveness of fraud prevention efforts. However, when contrasting the Commission's proposal with the mandates of the Council and EP, it is questionable whether a sufficient degree of maturity has already been achieved.

We strongly urge the trilogue partners to assess the following aspects:

- *Data exchange as an obligation or a right?*
  From the perspective of the banking industry, it makes a lot of sense to create a uniform EU legal basis for the exchange of personal data for the purpose of combating fraud, This would create greater legal certainty, particularly with regard to data protection. However, it is sufficient to authorise PSPs to exchange personal data and to regulate the scope of data transfer. It is not necessary to oblige all PSPs to exchange fraud-related personal data. This would represent an excessive infringement of companies' freedom of action, especially in connection with the obligation to conclude an "information sharing agreement" with other PSPs. An obligation to exchange personal data is also too far-reaching with a view on data protection. In addition, the scope of the provision should be limited to the exchange of personal data. This is because a legal basis under data protection law is necessary solely for reasons of data protection and banking secrecy. The exchange of non-personal data (e.g., anonymised data, information on fraud methods) is not subject to the restrictions of data protection law, meaning that there is no need for regulation. In order to express that PSPs may (but are not required to) exchange certain personal data, Article 83a(1) sentence 1 of the Council's version could be worded as follows:

  "*Payment service providers **are allowed** to exchange **personal** data with other...*".

  However, if the legislators were instead to *oblige* all PSPs to exchange data, the approach favoured by the Commission and the Council so far is likely to be difficult to implement in the foreseeable timeframe due to its high complexity. In that case, consideration should be given to centralising the framework conditions for data exchange and the operation of the data exchange platform at the EBA, as already proposed by the EP.

- *Purpose of fraud data sharing and resulting obligations:*
  Article 83a paragraph 1 of the Council mandate lacks clarity as regards to the intended addressees of fraud cases submitted by a payer's bank via a fraud data sharing arrangement. We assume that it should be understood two-fold: the payee's bank servicing a suspicious payment account should receive such information (to examine the suspicious behaviour of its own customer), as should the other payers' banks (to possibly prevent other payers falling victim to a fraudulent scheme and making payments to suspicious accounts). Both these intentions and the subsequent obligations of the involved banks must be clearly stated to avoid operational and legal uncertainties. A sole reference to the provisions on transaction monitoring in Article 83 is insufficient.

- *Data relevant for fraud data sharing:*
  An unambiguous specification of data elements is key to balance the effectiveness of fraud data sharing with the accompanying data protection considerations. A mere reference to the data elements mentioned in Article 83 (transaction monitoring), as suggested by the Council mandate, is insufficient to strike this balance, as its scope of data is too extensive. Data elements for the purpose of fraud data sharing should focus on relevant information pointing to the suspected fraudster (payee) but may not include personal data of the alleged victims (payer). Here, limiting the information to the unique identifier of the payee's payment account, as proposed by the Commission, may be too restrictive. It should be extended to include the payee's name and the underlying modus operandi, as suggested by the EP mandate. In regard to the modus operandi, the submission of data on the specific device from which the transaction was initiated could be helpful in cases where the payer's bank has reasonable grounds to suspect that the initiation has been performed by a fraudster with this specific tool. Pure device data without additional information about individuals should be classified as anonymous data and therefore be exchangeable without restrictions under data protection law.

- *Barriers to the establishment of fraud data sharing arrangements:*
  According to the PSR, the basis for multilateral data exchange shall be an agreement between PSPs. For such an agreement to be successfully established, the framework conditions must not be too complicated or complex. As in the example of the model clauses for third-country data transfers in the GDPR, model contracts published by the EU Commission could be a useful aid here. It is important that such an agreement is supported by the competent supervisory authorities for payment services *and* those for data protection if this is to be successful. Coordination between supervisory authorities is of crucial importance. Given the tight implementation deadlines, the dependencies on the requested data protection assessments (for example in accordance with Article 83a paragraph 3 of the Council mandate) must be respected. The PSR should clarify that the obligation to participate in such arrangements and the related legal and liability consequences only arise once this process is complete.

12. Platform on combatting fraud (Article 83b of the Council mandate)

We are strongly in favour of the Council's proposal to establish a dedicated platform on combatting fraud. This is testament to the shared insight that effective fraud prevention cannot be limited to the payments sector and its regulatory provisions. However, the Article should be extended to ensure

- the inclusion of the ECSP industry and its relevant regulatory bodies and
- that the platform's scope is, inter alia, aimed at facilitating legislative proposals to improve fraud prevention measures of all affected industries and the public sector.

III. Transparency on fees

1. Information requirements applicable to cash withdrawal services (Article 7)

The Council mandate's proposed extension of Article 7 to include making information available on a durable medium contradicts the political goal of simplification: in many member states, ATMs do not have a printer function, and replacement or retrofitting of existing ATMs would lead to high costs whilst lacking added value for the customer. This is exacerbated in the light of the fact that the recent implementation of requirements from the European Accessibility Act already imposed significant costs on ATM providers. Experience shows that receipts are often forgotten by customers, posing a risk that criminals will use forgotten receipts to select their next victim based on the amount withdrawn. Further, an additional mandatory printout would also counteract interests of sustainability. Not only that, customers are already informed in advance about possible ATM fees and receive additional information on their card or account statement after the transaction has been processed.

Thus, the obligation to make any charges available to the payer on a durable medium should be dismissed. However, if legislators were to uphold this proposal, a significantly longer implementation period than outlined in Article 112 would be necessary.

2. Charges for currency conversion (Articles 5, 13, 20 and 110a)

The suggested provisions lead to a disproportionately complex implementation needs, especially given the already high degree of transparency provided by the current PSD2 and by Regulation (EU) 2021/1230[5].

Therefore, the provisions should either be discarded or at least mitigated according to the following parameters:

- Information on the monetary amount for credit transfers shall only be necessary where the payer initiates these *"online directly, using the website or the mobile banking application of the payment service provider"* (consistency with the provisions in Regulation (EU) 2021/1230). This requires clarification in Articles 13 and 20.
- The provisions regarding the estimation of conversion charges, based on a recent aggregated mid-market exchange rate, are far too rigid. The envisaged maximum delay of ten minutes would require substantial changes to IT systems, and it remains unclear whether this ambitious condition can even be met by relevant market administrators and for all currencies or currency pairs. We suggest instead following the current logic of Regulation (EU) 2021/1230, which does not impose such tight time limits.
- A limitation to transactions made in a currency of a member state is necessary, not least to overcome the issue that the term *"the latest available applicable foreign exchange reference rate issued by the relevant central bank"* as reference value is not specific enough (especially in the case of rather illiquid currencies or currency pairs). This requires respective amendments to Article 2 paragraphs 4 and 5 which define the geographical scope of, inter alia, Title II.

[5] Regulation (EU) 2021/1230 of the European Parliament and of the Council of 14 July 2021 on cross-border payments in the Union

IV. Third-party providers

1. Requirements regarding dedicated data access interfaces (Article 36)

We support the addition of the Council's mandate of Article 36 paragraph 4 lit. (e), which correctly limits the mentioned interface functionality to instances where this functionality is already available to the account holder via the ASPSP's own interface – a basic principle established through PSD2. Consequently, the addition should be added to the previous functionalities as well (especially lit. (d) since this is not a regularly available standard feature in online banking). We also support the proposed deletion of the term "direct debit" in lit. (a). The regulator should clearly highlight that credit institutions must retain the freedom to decide which products to offer to which customer segments, based on demand and risk considerations. A legal obligation to implement a fixed set of functions would force banks to build and maintain functions that customers neither need nor use. This creates unnecessary costs which would ultimately be passed on to all customers, regardless of whether they benefit from the service.

2. Data access management by payment service users (Article 43)

The implementation of "reactivation functionality" would be highly demanding for the ASPSP and PIS alike, both from a technical and legal perspective.

If the payment services user allows a Third-Party Provider (TPP) to access the data interface, they enter into a contractual relationship with the respective TTP – not just with the ASPSP. In turn, the ASPSP has no insight into whether the terms governing data access or payment initiation agreed between the TPP and the payment service user are still in place once permissions are withdrawn. If a user withdraws permission, e.g. via the dashboard, any subsequent re-establishment must take place directly via the TPP. Banks cannot be responsible for managing access to services they do not control (e.g., if the TPP's conditions may have changed in the meantime).

Therefore, we strongly support the EP's mandate to delete lit. (c) of paragraph 2.

V. Strong customer authentication

1. General provisions on strong customer authentication (Articles 85, 85a and 86)

We support strong customer authentication (SCA) as a tool to reduce fraud, but the current rules need to be both more practical and more future-proof. In essence, it should be the decision of the issuing bank to apply SCA based on the actual risk of a transaction, not as a one-size-fits-all rule.

We are concerned about the new rule in Article 86 that shifts responsibility for re-authentication after 180 days to third-party providers such as Account Information Service Providers (AISPs). This change creates legal uncertainty and could confuse consumers. AISPs should follow the same rules and standards as banks when performing SCA. Finally, the regulation should better distinguish between consumer and business use cases, so that innovation in areas like machine-to-machine payments is not held back by rigid rules.

We believe that Article 85a as proposed by the Council's mandate introduces a superfluous regulatory layer that goes beyond what is required to ensure secure and efficient payment processes. The existing rules under Article 85 already provide sufficient flexibility to support innovative payment models while maintaining high security standards. The proposed addition represents a niche business model, and the decision to apply this model must lie within the scope of each individual business. Embedding this formalised process into the regulatory framework risks overstepping the role of regulation by prescribing commercial models and operational practices that should remain within the discretion of market participants. Thus, Article 85a should be deleted.

2. Outsourcing agreements for the application of strong customer authentication (Article 87)

We fully support the EP's mandate to entirely delete the proposed outsourcing requirement under Article 87 of the PSR. The provision risks obliging PSPs to enter into extensive outsourcing agreements with device manufacturers and other third parties, regardless of actual risk or relevance. This approach is disproportionate, given that PSPs already assess the security of authentication technologies based on international standards. Imposing blanket contractual obligations would create legal uncertainty, hinder innovation, and raise barriers for smaller market participants. Regulation should enable proportionate, risk-based decisions – not mandate formal outsourcing where there is no operational justification for doing so.

3. Accessibility requirements regarding strong customer authentication (Article 88)

We acknowledge the intention of Article 88 to ensure inclusive access to strong customer authentication (SCA) for all payment service users. However, the related provisions require a proportionate approach to ensure their intended targeted effect:

- We welcome the Council's proposal to exempt payment account packages or business models catering to digitally savvy customer segments from the obligations in (2).
- A strict prohibition of fees would contradict the causation principle, which would disadvantage other customers: banks should be allowed to charge fees on a strictly cost-based basis for the provision of dedicated hardware-based solutions (e.g. TAN generators).

4. Relation PSR to eIDAS

We are concerned about the unclear relation between the PSR and the European Digital Identity Wallet (EUDIW) implemented under Regulation (EU) No 910/2014. This jeopardises the acceptance of the EUDIW and its potential for European digital sovereignty.

In general, the payment service provider must decide which payment instruments and products they will integrate into the EUDIW (no mandatory usage).

Where payment service providers accept the EUDIW for the purpose of payments, the relation to the relevant PSR provisions has not yet been adequately defined. The acceptance of EUDIW in accordance with Art. 5f paragraph 2 of Regulation (EU) No 910/2014 poses an incalculable risk for payment service providers in cases of unauthorised transactions or malfunctions within the sphere of the EUDIW provider. The following key aspects must be regulated by the PSR:

- Clarification that no contractual arrangements or outsourcing agreement towards the EUDI wallet operator are needed.
- Clear definition and distinction between obligations for EUDIW providers and payment service providers, e.g. in conjunction with Articles 51, 55 and 56 (as regards payment instruments and strong customer authentication), and Article 83 (transaction monitoring).
- In particular, the authorization of a payment transaction shall be rebuttably presumed, if the payer has used the EUDIW for the purpose of authentication.
- Furthermore, regulatory provisions need to be clear on how banks can reject a particular EUDIW if security vulnerabilities are known. This requires, among other things, that the technical parameters and the provider of the EUDIW used by the payment services user can be identified by the bank at all times.
- Clear allocation of liability for EUDIW providers (in cases of unauthorised payments or where legitimate payments cannot be executed due to malfunctioning of the EUDIW).
- Access to relevant evidence that PSPs may require in civil liability proceedings.

VI. Relation PSR to MiCAR

We deem the PSR generally not the most appropriate framework for regulating crypto-assets, namely electronic money tokens (EMTs). Their technical characteristics, market function, and risk profile are fundamentally different from traditional payment instruments and are already comprehensively addressed under MiCAR[6]. EMT-specific regulation should therefore remain within MiCAR's scope.

Nonetheless we welcome the fact that the ongoing discussions for the PSR have placed greater emphasis on the interplay between EMTs and MiCAR and on which EBA has already elaborated on.[7] In this context, we consider the European Parliament's approach more suitable for ensuring a clear, proportionate, and technically coherent framework. This leads to an corresponding delineation. The targeted exclusion in Article 2 for "*payment transactions used*

[6] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets

[7] cf. EBA Opinion of 10 June 2025 on the interplay of PSD and MiCAR in relation to CASPs that transact electronic money tokens, EBA/Op/2005/08

for the execution of trading and settlement services using EMTs where the payment service provider has already been authorised as a crypto-asset service provider in a Member State for those services under Title V of MiCAR" is a practical and effective tool to avoid duplicate regulations in areas already covered by MiCAR. By explicitly distinguishing between EMTs used for investment/trading purposes and those used for payments, the Parliament's proposal correctly reflects the significant operational and technical differences between EMTs and traditional funds.

By contrast, the Council mandate amendments—although recognising EMTs in the PSR and acknowledging their specific characteristics—limits the exclusion in Article 2 to a narrower set of crypto-asset-services. In addition, its wording is – in our view - ambiguously and not very clear which may lead to questions as regards its scope. This approach risks subjecting a wide range of EMT transactions, which MiCAR is designed to regulate, to unnecessary and duplicate PSR obligations.

We therefore urge co-legislators to ensure a clear and strict separation of regulatory responsibilities. We believe that a clearly separated regulatory scope is a more suitable option. EMTs used solely for investment or trading purposes should be regulated exclusively under MiCAR, while PSD3/PSR should apply only to EMT transfers intended as payments—such as those for goods and services.

Finally, we want to highlight the importance of ensuring that custodial wallets are not conflated with payment accounts. Payment accounts involve reciprocal claims between the provider and the client, recorded on the account and balanced at regular intervals. Custodial wallets, by contrast, primarily serve as secure storage for crypto-assets or the keys granting access to them. They are part of a tripartite relationship in which the token issuer is a separate counterparty for redemption claims. As long as a custodial wallet cannot – either by contractual provisions or technical design – be used for payment transactions, it should not be classified as a payment account. Highlighting this distinction is important to ensure legal certainty and avoid any unintended extension of the PSR's scope.

VII. Implementation feasibility and unintended consequences

1. Conditional refund for payment transactions (Articles 61 to 63)

We welcome the clarification provided by the PSR which states that SCA is not required for transactions initiated 'by the payee only'. However, we are of the opinion that an unconditional ('no questions asked') refund right should not apply to merchant-initiated transactions (MIT), as these already ensure a very high level of consumer protection. Currently, consumers and merchants both profit from the existing, strict mechanisms of scheme rules which are enacted to effectively settle disputes. A static legal requirement goes against the political goal of simplification, undermines existing flexible products and would most likely lead to an increase in fraudulent behaviour.

2. Administrative sanctions and administrative measures (Article 96)

The proposed introduction of personal liability provisions for employees under Article 96(3) of the PSR should be dismissed entirely. The provision implies the necessity of establishing personal liability for employees. However, this approach is disproportionate and unwarranted, given the existence of effective supervisory and sanctioning mechanisms already applicable to payment service providers.

Moreover, in light of the ongoing shortage of qualified professionals in the financial sector, extending liability to employees without executive functions would send the wrong signal to the labour market and ultimately undermine both legislative objectives and sound business practice.

3. Provisions addressing the issuing of IBANs (Article 50a of the EP mandate and Articles 32a, 108 of the Council mandate)

Regulatory, infrastructure and market practice factors influence and constrain the issuing of IBANs and comparable account identifiers. Any legal provisions affecting this relationship must be carefully examined for against unintended consequences.

As regards the problem of "IBAN discrimination", Article 50a as proposed by the EP mandate should be discarded: it is redundant given the intended effects of established provisions (e.g. Article 9 SEPA regulation). Furthermore, it could lead to unintended consequences in light of the presumably contradictory relationship to the IBAN definition by ISO.

By contrast, Article 32a and Article 108 paragraph 1a as proposed by the Council mandate addressing so-called "virtual IBANs" seems appropriate, as its goal is to gain a better understanding of business practices in the light of regulatory considerations.

4. Provision by credit institutions of payment accounts to payment institutions (Article 32)

Adequate rules for the provisions of payment accounts to payment institutions are crucial to balance market access and financial risk considerations. The EP mandate and Council mandate, respectively, risk violating this balance by excessive tightening of the exclusion criteria in paragraph 2 as proposed by the Commission:

- The exclusion criteria in lit. (d) and (e) are necessary to ensure that CRR institutions may accept or decline opening said accounts according to their own compliance capacities.
- This is not only crucial for CRR institutions, allowing them to avoid excessive risk exposures. It is also key to ensuring that credit institutions may effectively fulfil their critical role as "gatekeepers" of payment systems, thereby preventing risks for all of the latter's participants and operators at a systemic level.
- A close-ended list of refusal scenarios, in particular a too restrictive one, fails to account for scenarios where these imperatives are jeopardised.

- For example, where the credit institution has serious grounds to suspect defective money laundering or terrorism financing controls by the applicant or illegal activities by the applicant or its customers, this should constitute a distinct reason to refrain from opening or maintaining such accounts. The amendment proposed by the Council mandate in lit. (a) is therefore inadequate since, as a mere reference to the AML regulation may not be sufficiently specific.

The suggested deletions of lit. (d) and (e) of Article 32 paragraph 2 should be reversed. Lit. (a) should continue to include the above-mentioned AML and CTF-related reasons, possibly alongside or in addition to a general reference to the AML regulation.

Furthermore, legal and supervisory clarity to the benefit of both CRR institutions and payment institutions relies on a uniform understanding of the extent, rights and obligations as regards *"the provision of payment accounts to payment institutions"* and to unambiguously delineate it from other financial services. At the same time, this must be balanced with an adequate degree of freedom to facilitate competition and innovation. Legislators could seek explicit feedback of competent authorities whether this premise is already fulfilled or if further clarification at the level of the regulation might be helpful.

5. Unnecessary complexity due to high number of delegated acts

The current legislative state envisages a significant number of delegated acts (level 2 legislation). There is an urgent need to review this plan with a particular focus on the complexity of implementation and the suitability of this legal instrument for the intended regulatory purpose in each case. In particular, the following delegated acts should be reconsidered and removed:

- *Article 16 paragraph 2 of the Council mandate (regarding the term "commercial trade name"):*
  The Council's proposal correctly reflects that no unionwide definition of the term exists. However, a uniform definition should be given at the level of the PSR (level 1) due to its significant implications from a civil law perspective. The Commission should be invited to develop a corresponding proposal for further consultation with the co-legislators.
- *Article 89 paragraph 1 lit. (d) (regarding the outsourcing agreements pursuant to Article 87):*
  Following the EP's suggestion to delete Article 87, which we welcome, the provision for this delegated act becomes redundant (see also section V.2 of this document).
- *Article 89 paragraph 1 lit. (a), (b) and (c) (regarding the general provisions on strong customer authentication pursuant to Article 85):*
  The PSR should expressly provide that this delegated act shall maintain a maximum of consistency with the current delegated act (Commission Delegated Regulation (EU) 2018/389). Any amendments may only be performed where necessary due to material changes given by the PSR. This is necessary to maintain a high degree of stability regarding established customer procedures, avoid the risk of legal uncertainty and to prevent disproportionate implementation costs.
- *Article 85a of the Council mandate (regarding dedicated SCA provisions for credit transfers):*

We strongly suggest removing Article 85a entirely (see section V.1 of this document). However, if legislators were to maintain this Article, the relevant exemptions would have to be defined at the level of the PSR (level 1) due to their significant implications from a civil law perspective.

- *Article 82 paragraph 2 (regarding "fraud reporting"):*
  The current PSD2 fraud reporting regime – based on EBA guidelines – has been successfully harmonised with the reporting obligations under the ECB payment statistics. There is no need to apply a stricter legal instrument (delegated act). Besides maintaining the current instrument (EBA guidelines), the PSR should expressly provide that a maximum degree of consistency with the current fraud reporting regime shall be maintained. This is necessary to prevent disproportionate implementation costs for PSPs, NCAs and NCBs.
- *Article 15 paragraph 3 of the SEPA regulation (regarding reporting obligations for instant credit transfers):*
  The reporting requirements should be revoked entirely. They impose disproportionate costs for PSPs without sufficient countervailing benefits for legislators with a view to future legislation on payment services.

6. Implementation deadlines and related dependency on delegated acts

Several provisions of the PSR will result in significant burdens in regard to implementation on the part of PSPs. These will include highly complex interdependencies between infrastructure components and far-reaching civil law requirements (especially in the area of fraud prevention). Against this backdrop, we welcome the fact that both the European Parliament and the Council envision later dates for the entry into force in Article 112 than that suggested by the Commission proposal.

Nevertheless, the overall complexity of implementation, and in particular the dependency on the significant number of delegated acts envisaged, continues to be underestimated. PSPs require at least 24 months after publication of all regulatory provisions to successfully implement provisions in a risk-minimising way.

Furthermore, previous legislative procedures in the area of payments have shown that the enactment of delegated acts, or the provision of implementing technical standards, can be subject to delays for a variety of reasons. If this does turn out to be the case, the regulation should ensure that the entry into force of all affected provisions is also postponed.