EBF_046389

EBF position paper on the Commission Proposal for Payment Services Regulation

Executive Summary

The Payment Services Directive has been a cornerstone of EU payments legislation and is fundamentally important in ensuring high levels of consumer protection and security of transactions, whilst fostering an innovative and competitive EU payments market, characterised by a level playing field between all providers of payment services.

The Payment Services Regulation (PSR) and the third Payment Services Directive (PSD3) proposals offer some welcome updates that can strengthen the current state of the payments market, provided that some important elements are integrated, most notably on fraud and liability, open banking and strong customer authentication (SCA).

Fraud and liability

Social engineering is a serious societal problem that has grown over the past years. The EBF acknowledges the necessity to address this matter promptly and supports the Commission's objective to counteract (online) scams. We welcome measures that aim to facilitate fraud information sharing, fraud monitoring and information campaigns as a broad spectrum of means is needed in the combat against the increasingly complex fraud landscape. The proposed measures on mandatory refund by payer PSPs for bank-employee impersonation fraud and explosion on bank-employee impersonation claims will, on the contrary, not contribute to reducing fraud. Indeed, it would be an ex-post measure once the fraud has been perpetrated and it would not nip the fraud in the bud as desired by all. This highlights how banks are limited in preventing online scams alone, as the manipulation happens *outside their sphere of competence* and are victims themselves of the fraud which can be effectively prevented/detected by other players (e.g., telecoms). To address the problem effectively, focus should be on prevention, detection and targeting criminals. Instead, all parties in the value chain (e.g., payer and payee's banks, payment initiators, governments, businesses providers, social media platforms, internet and mobile service providers, Big Tech, corporate and consumers), need to be required compelled to collaborate to make it as difficult as possible for criminals and to prevent scams.
Thus a one-sided refund obligation in the law is not a solution to prevent impersonation bank scams and reduces the pressure for real solutions. All the parties that can take action – in particular electronic communications service providers – should have clear legal obligations to take all prevention/mitigation measures possible (and should not be able to charge a fee for such measures), in the absence of which they should be liable for the financial loss of the payer. Therefore, it is of utmost importance to go beyond "close cooperation" and guarantee a fair distribution of responsibilities and liabilities between all players involved by also including electronic communication service providers and subjecting them to specific technical requirements. Several national legislations are going in this direction, notably the French law against spoofing requiring telco operators to implement technical solutions to avoid fraudulent use of telephone numbers on French territory, and to ensure the interoperability with the existing solutions. In other countries,

the responsibility of electronic communication service providers has been recognized by several Courts.

Open banking

It is paramount that PSR corrects the imbalances created by PSD2, in particular when it comes to enabling the compensation of all parties in the open banking ecosystem. The Data Act and the proposal for Financial Data Access Regulation (FIDA) recognize this need, and therefore there is no reason why it should not apply to payment account access under PSR as well. As to the modalities of access to accounts, the move towards the sole use of APIs is very welcome but it should be clarified that no new or permanent contingency access is required. Nor new functionalities are to be provided though the APIs and especially if not provided in the customer interface. The requirement to create permission dashboards would help consumers in adopting open banking but a number of amendments are needed to improve the operationalization of the dashboards and avoid misunderstanding in the role of the providers involved through an alignment with FIDA.

Strong Customer Authentication

The PSD2 provisions on SCA have been successful in bringing down authorized payment fraud. It is important that the review does not fundamentally alter the current SCA implementation and does not impose new and potentially costly aspects regarding SCA. The proposed requirement for PSPs to have in place outsourcing agreements with technical providers would not be feasible to achieve and would not add any value as it is currently drafted. In fact, on the one hand, it doesn’t have positive effects in terms of security of SCA compared to what is already foreseen with PSD2, and, on the other hand, the proposal does not include sufficient obligations for pass-through digital wallets, that have become an important part of the payments chain.

Fraud and liability provisions

Article 59 - Payment service provider's liability for impersonation fraud

Online frauds are a social problem that requires all parties in the value chain, including governmental authorities, companies and consumers, to be part of the fight against fraud.

We believe that the legislation should be future-proof and concentrate on allowing fraud prevention and mitigation and the detection of criminals. It is considered worrying and inadequate the exclusion of market players that provide support for the provision of payment services or sometimes directly interact with the final customers (e.g., mobile wallet solutions, electronic communication providers). The problem lies in the nature of digital online services and communication channels, therefore the most important measures that should be taken include legal obligations and specific requirements for telecom providers and online platforms to take measures to *prevent/detect* fraud from occurring, such as:

- An obligation for telecom operators to prevent that text messages or calls appear to come from a PSP, to block text messages and spoofed numbers, to immediately block phone numbers used to commit fraud and to screen for bulk messages being sent including URLs. A European solution providing a register of aliases of SMS senders in order to avoid spoofing could be explored. We note that several national legislations are going in this direction, notably the French law against spoofing requiring telco operators to implement technical solutions to avoid fraudulent use of telephone numbers on French territory, and to ensure the interoperability with the existing solutions.
- A new requirement for telecom operators should be the introduction of an ad hoc protocol to allow SMS sender verification by them to the benefit of PSP and of course the final user. In other terms, if there is any doubt about the truthfulness and reliability of a text message/call, the telecom operator should first verify the authenticity with the bank (which is therefore properly alerted thereof), and secondly, in case of a fraudulent message, immediately block the message or warn the PSU about the fraudulent nature of the SMS/call by giving notice (possibly conveyed in agreement with the bank) to the PSU. Mobile phone software providers to technically prevent SMS or phone calls that are displayed with the same alias than a bank, from being queued in the same thread.
- An obligation on internet platforms to control that the information provided is correct and to verify the identity of their customers and assess their risk profile. Further measures that could be considered include the closure or suspension of potentially fake/scam websites in a centralized manner, the revocation of the authentication web certificate of the website and stricter requirements during the verification process of Hosting Providers for opening a website.
- Commitment to Know Your Customer (KYC) and Strong Customer Authentication (SCA) for all parties in the chain: KYC and SCA should become the standard for all entities offering payments and other digital services (including telecom operators, social media, message platforms and digital marketplaces).

An obligation for providers of electronic communication providers to cooperate and prevent fraud, as stated in Article 59(5), is a good first step, but it is imperative to broaden this to compulsory measures that will actually help to prevent/detect fraud before it happens. To effectively combat fraud, regulators need to take a holistic, broader approach that covers the whole chain of a fraudulent conduct and not PSP only. It is crucial that PSR is amended to include concrete legal obligations for electronic communication service providers to put in place technical measures that will prevent fraud. A failure to put such measures in place should result in the legal obligation of the electronic communication service provider to refund the PSP that has refunded the consumer. With the recent Digital Operational Resilience Act (DORA), the Commission marked a milestone in cyber security and resilience

in financial services by acknowledging the importance of all actors in the ecosystem playing their part to that end. As a result, DORA introduces, among others, a new oversight framework for critical third-party providers of ICT services to banks. The review of PSD2 should take inspiration from the approach taken in DORA. Also, given the importance of the fraud prevention measures to be taken by electronic communication services providers, it is important to clearly define the providers that are in scope. All providers falling under the scope of the European electronic communications code (Directive (EU) 2018/1972) or the Digital Markets Act (Regulation (EU) 2022/1925) should be in scope of Article 59. In addition, the cooperation with electronic communications services providers as described in Article 59(5) should be broadened to go further than "cooperation". The proposal should provide an explicit obligation (concrete procedures, deadlines, sanctions, legal basis for processing of personal data), and a fair liability allocation should be guaranteed. The responsibility of electronic communication service providers should be extended to all types of frauds that customer can be victim of and complain about, not only bank employee impersonation fraud. For this purpose, we suggest developing adequately provisions to avoid margins of discretion and uncertainty. Also, a definition of electronic communications providers in Article 3 is needed.

At the same time, we are strongly opposed to the proposed payer PSPs' mandatory refund obligation for payment transactions that were duly authorised by the payer but subject to impersonation fraud. The knowledge that banks will reimburse reduces the incentives and pressure on other actors in the chain to help reduce the problem and expand the business-line for fraudsters. In 2020 Dutch banks decided to compensate damages caused by 'bank employee impersonation fraud. Unfortunately, since then the number of victims has tripled and the damage has doubled, despite all the efforts of the banks. It has taken away the incentive for other stakeholders (telecom and social media/online platforms) to cooperate with banks, as the complete financial burden is now carried by the banks.

A more comprehensive reimbursement policy would support the 'criminal business model' and therefore make EU citizens more vulnerable to impersonation frauds. It would contribute to increasing fraud levels and moral hazard, as consumers would not have an incentive to be vigilant and would gradually pay less attention to signs of impersonation frauds when instructing their payments. This would result in fraudsters being encouraged to perpetrate fraud at the expense of PSPs, using a generalised refund possibility to their advantage. In the long run, disincentivising consumers from keeping alert to online impersonation frauds would affect negatively their general digital security and wellbeing, as reduced attention to online risks would spill over their use of all kinds of digital services, leaving them more exposed to cyber risks.

Moreover, a refund right for authorised transactions would bring significant uncertainty in the payment system and to payment finality by essentially considering all payments non-final – it would conflict with an underlying principle and cornerstone of the legal framework to the detriment of PSPs, consumers and businesses alike. Such a refund right would inevitably also lead to more friction in the customer journey as it might reduce the incentives of banks and other PSPs to develop and implement user-friendly SCA solutions in order to get additional assurance about the will of the customer. In general, a refund right for authorised payments would not be in line with the principle of proportionality.

However, if a refund obligation was to be maintained – which, as argued, should be in any case accompanied with the right of the PSPs to obtain refund from the communication/media/platform channel operator that was the vehicle to the scam, the following amendments are needed:

- The current wording of the Paragraph 1 could lead to situations where the PSU has a refund right for impersonation fraud where only the name of a bank

employee has been used. This is a very broad definition and the text should be amended to require at least the name to be used with another element.

- Paragraph 2 should include some reasonable conditions for the consumer to fulfil in order to benefit from a refund, namely the obligation to provide reasonable documented evidence of the bank employee impersonation fraud and an obligation to file a police report and provide it to the bank. The police report is necessary for multiple reasons: (1) For the investigation of the PSP on the fraud, (2) That no false claims will be made by consumers and (3) that the police will trace the scammers and the prosecutor can prosecute the scammers.
- In order to allow for PSPs to investigate claimed fraud cases, the 10-day period should be extended to at least 15 business days and only start counting as of the presentation of the police report. The types of fraud covered by this Article are complex, include third parties' collaboration and cannot in all cases be investigated within a strict 10-day window, hence in exceptional cases more time should be allowed.
- Due to complexity and number of participant involved, specialised dispute and resolution mechanisms could be promoted.
- We welcome the inclusion of gross negligence in this article. In addition, we suggest exemplifying the concept of gross negligence in a uniform manner across countries and the associated liabilities for each case so that a more harmonized implementation can be achieved across the EU. Several examples of gross negligence in relation to bank-employee impersonation frauds can be recognized at EU level therefore at a minimum further examples of "gross negligent behaviour" should be added in Recital (82). Non exhaustive examples include:
    - If a victim has been alerted several times by the PSP about never providing his/her credentials by phone or email or not clicking on links included in SMSs or emails;
    - if a victim has already been a victim of the same fraudulent scenario and modus operandi (at another PSP) before;
    - Not preserving the security of the data associated with a payment instrument (password, confidential code, security code, etc.), communicating these elements to a third party; entrusting payment instrument to a third party (relative, coursier, etc.) or when a consumer confirms the payment notwithstanding a warning message to the contrary provided by the PSP during the validation path.

Article 55 - Evidence on authorisation and execution of payment transactions

The proposed changes in the draft, specifically (i) replacing the term "authentication" with "authorisation" in Art. 55(1) of the PSR and (ii) changing the phrase "not necessarily be sufficient to prove" to "not be sufficient to prove" in Art. 55(2) of the PSR, are incorrect and lack clear justification. PSD2 stated that in order to demonstrate that a payment transaction was duly authorized, the PSP had to amongst others provide evidence that the payment was authenticated by the payer. The PSR proposal deletes the reference to 'authentication' and only refers to the PSPs having to provide evidence of authorization, and it is not specified how this can be demonstrated. These is due to the fact that the concept of authorization is not defined compared to that of authentication under art. 3(34) of the PSR. If the new wording was kept, PSPs would face great uncertainty and difficulty in assessing whether a transaction is authorized or not. The changes could undermine both established procedures and legal principles evolved through constant jurisdiction and case-law to the detriment of legal certainty for both PSPs and their customers.

Therefore, it is of utmost importance to have a clear definition of the term "authorization" included in Article 3 of PSR by drawing down what is currently proposed in article 49(7) of PSR. At the moment of the authorisation, the customer consents to execute the transaction and only afterwards the person realises he or she has been scammed. When the transaction has been conducted according to the regular technical authorisation steps it should be considered authorised from a legal point of view, as the bank cannot detect the intent behind the authorisation. To avoid ambiguity or misinterpretation, we advise adding the following definition of authorisation in the PSR: "*the expression of the permission for the execution of a payment transaction given by a payer to his payment services provider, through the process and in the form agreed between the payer and his Payment Services Provider*".

Furthermore, as mentioned above, we suggest clarifying the concept of "gross negligence" and "manipulation of the payer" in a uniform manner across countries and the associated liabilities for each case. If this not considered a viable solution, at a minimum further examples of "gross negligent behaviour" should be added, in line with Recital (82).

Article 56 – Suspicion of fraud in unauthorized payment transactions

In Art. 56(1) PSPs are required to refund the payer the amount of the unauthorized payment transaction immediately if there are no reasonable grounds for suspecting fraud committed by the payer and communicates those grounds to the relevant national authority in writing. Such investigations take time and require attention. PSPs need more to investigate if a payment is unauthorized or not.

Article 83 paragraph 3: fraud data sharing

In general, we are supportive of this Article. However, we suggest the following amendments should be introduced:

- Paragraph 3 states 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 should come into effect from the very first notification to avoid unnecessary further attempts without waiting for two customers to be frauded.
- Recital 103 mentions that fraud detection can be made more effective with a greater amount of information and, therefore, that "sharing of all relevant information between payment service providers should there be possible." This is very welcome; however, in recital 104 and then in Art. 83, it appears that the only information that can be shared is the IBAN. While this is a good start, there is other information such as email addressed, telephone numbers, Ip addresses, unique device numbers (IMEI), name and address details, birth dates, device fingerprints, social security number or equal and modus operandi (vishing, smishing etc) the sharing of which can aid in fraud prevention, particularly in the increasingly sophisticated fraud landscape. There should not be an exhaustive list of information that barely covers existing needs according to known modus operandi, but it should be future-proof and allow new elements to be included, as much as they are relevant for the purpose.
- Paragraph 3 states that PSPs shall not store data longer than necessary for the purposes set out in paragraph 1, and not after the termination of the customer relationship. This provision should be deeply analyzed in order to evaluate if the

wording is coordinated with the requirements on the payment services provider to store data for a longer period and the legal basis for doing so in order, for example, to handle legal claims that could arise even years later from the termination of the relationship or information requested by the police for investigations. This point should be clarified also in light of the fact that transaction monitoring is a batch mechanism (EBA Q&A 2018_4090) and alignment with GDPR's provisions on data processing/limitations is required. The list of data that can be used for transaction monitoring should not be limited, as currently proposed, but should allow for other data to be monitored in order to be able to adjust monitoring to potentially upcoming future fraud scenarios. Furthermore, there is a need to clarify the meaning of "previous payment transactions".

- Paragraph 6 implies that the PSP a) may not be able to terminate a customer relationship and b) the processing of the personal data must not have an impact on obtaining a bank account with another PSP. Our proposal would be to have paragraph 6 removed. This ensures that fraudsters cannot continue their activities neither in their current bank nor in another bank.
- In the proposal there is no specific mention anymore of "permitting" processing personal data for fraud purposes, except for transaction monitoring and information sharing arrangements in Article 83. However Recital 102 seems to go in this direction in terms of processing information about customer transactions and payment account for fraud prevention. Consequently, the text should clarify if the legal obligation provided in Article 83 (as GDPR legal basis) applies for all situations of processing personal data for fraud prevention, investigation and detection of fraud or if it is related just transaction monitoring and info sharing and the relevant legal basis, for all the different process for fraud purposes, maybe legitimate interest.

Article 83 (1) & (2) – Transaction monitoring mechanisms

- While this Article builds upon Articles 1 and 2 of Delegated Regulation 2018/389, we believe it has not been properly transferred and would recommend the intention of the delegated regulation is retained, which provides greater flexibility to PSPs in terms of SCA and exemptions application as well as fraud prevention. Therefore, we would recommend copying the exact language from the delegated regulation into the Level 1 text or specifying the principle of PSP's discretionary when it comes to making use of the SCA, SCA exemptions and fraud prevention.
- Furthermore, in Article 89 the EBA is mandated to develop RTSs for the technical requirements for these transaction monitoring mechanisms. Having detailed technical rules in place may however prove to be counterproductive since such systems should be flexible and continuously and quickly adaptable, based in algorithms and dynamic AI tools. Legislation should refrain to be too much prescriptive and instead, maintain the existing requirements on TMM already foreseen in the current RTS and clearly allow for such important tools to exist, although taking a more result-oriented approach.

Article 50 - IBAN name check and Article 57 - Payment service provider's liability for incorrect application of the matching verification service

In general, these provisions should be as closely aligned as possible with the final requirements of the Instant Payments Regulation, in order to ensure that a common solution with the same provisions can be implemented by PSPs.

Article 82 (2) - Fraud reporting requirements

- Under Article 82 it is stated that the EBA shall develop draft regulatory technical standards (RTS) on fraud reporting data so that PSPs can report statistical fraud to competent authorities on an annual basis. Creating a single harmonized template for all PSPs to use across the EU is a welcomed proposal.
- This is especially the case as there are existing reporting requirements in Articles 19 and 21 of the Delegated Regulation on SCA (389/2018) which provide for ongoing maintenance of data and quarterly reporting, respectively, and in addition some home and host Member States have imposed additional requirements (with different templates).
- We therefore see the proposed RTS in Art 82 as an opportunity to streamline reporting requirements across the various SCA/fraud requirements. This is vital to ensure a level-playing field across the EU. We would also recommend that reporting should only be made to the home Member State competent authority and that any sharing with other NCAs is coordinated via the home authority.

Additional measures needed for fraud prevention, detection, and mitigation

When it comes to cooperation among PSPs for fraud prevention, detection and mitigation, it is necessary to go further than what is foreseen in the proposal, foreseeing other mechanisms that grant clear grounds for cooperation among PSPs. Such measures should include the possibility for both the payer and the payee's PSPs to block and recover funds/instruments for payment transactions for which PSPs involved have legitimate grounds to suspect fraud (e.g., the payer has provided a copy of the report made to the police authorities) both in cases where there is a claim from the payer and where the bank itself has a suspicious of fraudulent activities.

Therefore, concerning article 51, providing for the block of the payment instrument in case of fraud, we suggest including the possibility to also block the payment account of the payee in case of suspected fraud under investigation by taking into due consideration the need to balance the respect of the privacy of the beneficiary and his/her rights under GDPR with the interest of the payer and of the payer's PSP to avail themselves of the personal data of the beneficiary/ potential fraudster.

Furthermore, these additional measures are essential to ensure that fraudsters are left with no financial incentives to keep perpetrating these frauds, as well as to mitigate damages incurred by the payments system stakeholders.

Open banking

Article 34 – Contractual obligations

For the future development of a successful open banking ecosystem in Europe, it is paramount that PSR is amended to allow for Account Servicing Payment Service Providers (ASPSPs) to be compensated for data sharing. The proposed framework for the revised open banking does not follow the developments envisaged in the remuneration proposal for the new FIDA Regulation, which has a contractual base and potentially enables benefits for all stakeholders. Also, the Data Act allows for compensation for

parties sharing data. Maintaining the payment services in a different and unrewarded model would undermine the development of open banking and the efforts of the sector while leading to an unfair distribution of the value and risk.
The principle adopted in PSD2, according to which banks must offer their interfaces free of charge to TPPs operating on commercial terms, is totally exceptional and against market economy principles. The imbalance is further increased by the fact that banks have to implement all the same new functionalities in the API interfaces that they bring to the interfaces available to customers. The consequence of this imbalance becomes even more obvious in the corporate segment where the ASPSPs would have to develop solutions free of charge for the TPPs. Solutions that TPPs then sell on to a more competitive price than what the ASPSP would be able to, having to bear all costs for development, maintenance and support. The Commission's reasoning as to why compensation could not be extended to PSR as well - because there is no evidence that the compensation model would improve the quality of API interfaces is unfounded because compensation has not been used and therefore there can be no evidence of its effects. As another justification for continuing the non-compensation, the Commission mentions the disruptive effect the compensation would have on the market. In this regard, an imbalance could occur since, in addition to the one-time costs of setting up the dedicated interface, the running costs of maintaining PSD2 infrastructure compliance would have been incurred anyway. This is even true considering that the payment system will have to be continuously maintained to support further innovation/regulation of the market and something where the Commission is reasoning differently in both the Data Act and in FIDA.

According to the Study on the application and the impact of PSD2[1] the combined costs of the banks for the construction of PSD2 API interfaces built by ASPSPs were approximately EUR 2.2 billion. Despite this, the Commission's proposal includes new obligations and responsibilities for ASPSPs, likely causing large costs, e.g.:

- Those ASPSPs currently not offering APIs having to develop APIs for third party access.
- Construction of the so-called Permission Dashboard, i.e. the consent management tool.
- Removal of the limit for AISPs to access payment information not more than 4 times a day if the user is not actively requesting it.
- Obligation to compensate a customer who has been the target of a fraud in the name of the bank for the lost funds, even if the customer himself authorized the payment.
- And those that are refuted by the industry such as direct debits and strong customer authentication exemptions.
- Support of direct debit without any clear indication of the provisions to be implemented on the dedicated interfaces (e.g., release/cancellation of a new mandate or confirmation/revocation of the first debit of an SDD B2B or initiation of a collection).
- Support of strong customer authentication exemptions.

Hence Article 34 should be amended to include a new paragraph stating that ASPSPs are entitled to compensation, in line with Article 9(1) of the Data Act.

Article 35 – Provision of dedicated access interfaces

We strongly believe in high quality APIs ("dedicated interfaces") to exchange data between ASPSPs and TPPs. We therefore welcome the Commission proposals to abandon the use of an alternative interface (the online customer interface), including the use of such interfaces as a so-called 'fallback mechanism' in case the primary (i.e. dedicated) interface is temporarily unavailable, as well as the rather heavy administrative burden on ASPSPs

[1] A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2) - Publications Office of the EU (europa.eu)

to qualify for an exemption to the obligation to offer on a permanently basis such fallback mechanisms. However, as we note below, Article 38 must be amended so that effectively no fall-back interface is required.

The current requirements on availability and performance of dedicated interfaces regulated in Art 32(2) RTS and as further specified in the EBA/GL/2018/07 are sufficient and should be maintained. The PSR seems not to incorporate these Guidelines, but instead introduces new key performance indicators (KPIs) (Art. 35(5)). Current KPIs as prescribed by the EBA have proven to be reliable and should be better enforced rather than adding new ones.

Article 36 – Requirements regarding dedicated data access interfaces

Article 36(4) requires ASPSPs to ensure that the dedicated interface allows PISPs, at a minimum, to initiate several types of transactions, such as "place and revoke direct debits", initiate payments to multiple beneficiaries, single payments and future-dated payments, etc. The principle of "minimum services" however violates the one of "data parity"– included in Articles 37 and Recital 59 – that requires ASPSPs to provide TPPs access to the same payment account data and initiation of the same payment services that are available directly to the PSU via the online customer interface. We strongly recommend applying data parity to Art. 36(4), meaning that ASPSPs only have to offer services to the TPP that are also offered directly to the PSU in question. Otherwise, it seems that an ASPSP is obliged to offer a service that is not present in its direct customer interface (i.e., not implemented into that interface) and as a consequence, no contract is in place or is possible to sign with/by the customer. In fact, this is also important from a legal perspective, given that rights and obligations in relation to a service need to be made clear and agreed upon before a PSU can use a service. The list currently in paragraph (4) should be drafted as an exemplification of the "parity principle" rather than a list of mandatory information to be provided.

In addition, a direct debit is not a payment that the PSU initiates. The PSU mandates the payee to initiate the payment at a later stage. Direct debit should either be deleted from the paragraph or it should be clarified what the paragraph is about provided this possibility is offered directly to the PSU. In fact, we believe that a reflection around direct debit service should be carried out according to the effective demand for such service from the market and based on an in-depth functional/technical analysis which considers the possible technical constraints (e.g., it should be better clarified which are the part of the process that need to be made available on dedicated interfaces, e.g., release/cancellation of a new mandate or confirmation/revocation of the first debit of an SDD B2B or initiation of a collection).

Also, in relation to Art. 36(4), it should be further clarified that e.g., e-invoice/request to pay services, file upload and download services, Premium API services and add-on services (like alias services based on telephone numbers) shall be out of scope for Open Banking API as they are under PSD2. It needs to be completely clear which services are part of the compliance scope and thus have to be supported by the PSD API.

Articles 36(2)(d) and 36(4)(g) require ASPSPs to provide PISPs certain information via the dedicated interface, for instance, the associated names of the account holder. We strongly recommend requiring that these types of data can only be provided by an ASPSP to a PISP when strong customer authentication has been performed, for customer protection reasons (fraud prevention and GDPR purposes). Only after strong customer authentication the payment account data or confirmation can be (safely) provided.

Importantly, however, it is not clear what the purpose would be of providing this type of information. It requires providing privacy-sensitive information and could violate the data minimisation principle under GDPR, while – at least within the European Economic Area (EEA) – credit transfers can be currently processed solely based on the unique identifier of the payment account. Additional information (such as described in these sub-articles) is not needed.

Transmitting such information before strong customer authentication would not be prudent and there would be a high risk of misuse. Also, the meaning of different terms needs further clarification (e.g., associated names; verify the name; available currencies - which we would deem to be the currency in which the account is held and not any potential FX currencies offered by the ASPSP - and if the term "confirmation of the execution of the operation" in Art. 36(5)(b) refers to the message in Art. 36(5)(a) or something else). It also needs to be clarified if Art. 36(2)(d) - which seems relevant only in the context of PIS - now requires that all account numbers of a PSU are provided to a PISP (and thus does not any longer require an AIS license and is not seen as AIS in the context of the dashboard).

Moreover, the ASPSP is not able to comply with the requirements laid down in Articles 36(2)(d) and 36(4)(g) for one-off payments (such as e-commerce payments). This type of transaction is directly executed after SCA has been applied. Therefore, it is not possible to provide additional payment account data prior to the initiation and execution of the payment with this type of payment transaction. If ASPSPs must oblige with this requirement, it could result in very cumbersome and inefficient customer journeys, negatively impacting the conversion rates of TPPs.

Moreover, it is unclear what purpose additional payment account data serves in a PIS-only scenario. As explained, this data is not necessary to execute a payment transaction.

ASPSPs should be able to make available additional payment account data (by means of the unique identifier of the account and associated names of the accountholder and currencies) to a PISP, but only after the initiation of the payment where SCA has been applied and for certain payment transaction types only after the execution of the payment, when the transaction is directly executed by the ASPSP after SCA has been conducted (such as the one-off payment).

The scope of Art 36(2)(c) should be better clarified so that only those SCA exemptions need to be supported for which the ASPSP can verify on their side that the conditions to grant their application are fulfilled. Otherwise, the liability for transactions should be on the PISP in case of an SCA exemption used by the PISP itself because of its transaction monitoring. Further, the transaction monitoring mechanism should allow the exchange of all the data necessary to apply the paragraph 1(c), namely, to enable PSPs to prevent/detect potentially fraudulent transactions instead of the IBAN only.

It should be specified that in the event a PISP applies an SCA exemption which is supported by an ASPSP and the ASPSP does not revert it to SCA, then, the PISP should be liable towards the payer's PSP for any such transactions for which the payer's PSP is obliged to refund the payer. Further, in addition to what is already regulated in Article 55(1) and 56(5)PSR, PISP should also be obliged to compensate the ASPSP in case of impersonation fraud where a PISP is involved and – should payee initiated payments continue to be in scope – for refunds to the payer under article 63 PSR. Also, AISPs should be liable for any misuse of payment data (e.g., IBAN) in case they or customers to which the data was forwarded failed to protect the data sufficiently and this caused fraud (e.g., in the context of creating wrong direct debit mandates).

Finally, Article 36(5) should be amended by identifying and providing for only the main status changes that are relevant (e.g., Payment authorised by the customer, funds blocked, payment executed). Indeed, from our perspective simply transferring to AISP/PISPs all the statuses managed by each ASPSP can be an overwhelming amount of information structured in a different way and with different business meanings from bank to bank (also potentially depending as said on payment type/channel / customer) and could imply changes in ASPSPs approach to implementing the PIS service in the API channel. Said that we suggest amending the last paragraph of Article 36(5) in order to reflect what is provided in Art. 37(3), i.e., "*the information shall be provided after receipt of the payment order and on an ongoing basis until the payment is final*" and avoid inconsistency.

Article 37 – Data access parity between dedicated access interface and customer interface

It needs to be clarified that status updates need to be provided by ASPSP upon request only. The current wording in Article 37(3) "provide" vs Article 40 last section "made available" is unclear. Actively informing the AISP or PISP would come with very large complexity, as it would require that the banks can identify themselves towards the TPP when sending them API calls, and that TPPs can accept and process information coming from the AISPS. Therefore, we suggest substituting the term "shall be provided" in Art. 37(3) with "shall be made available" and include that the information is made available upon request of the PISP (and not pushed by the ASPSP), aligning this article with article 40.

Article 38 - Contingency measures for an unavailable dedicated interface

We note that whereas the proposal clearly aims to the use of dedicated interfaces only, the text is ambiguous whether and how precisely an eventual fallback mechanism should be offered, as for example Article 38 may be read as if a permanent fallback still must be offered, and the prohibited practise of access by third parties using screen scraping technologies without identifying themselves vis-à-vis the ASPSP seems to be reintroduced and legitimised (despite Art. 35(2)). TPPs' contingency access to payment accounts may raise concerns about potential security risks for payment service users. These risks include unauthorised access to users' credentials, and data that may not be adequately covered by PSR. Instead of maintaining the existing fall-back mechanism (the obligation to maintain them has been removed under Art. 35(2) of the PSR), the proposed requirement for ASPSPs is to provide unspecified "alternative solutions".

Art. 38(1) provides that ASPSPs should "take all measures in their power" to prevent unavailability of the dedicated interface. The proposed provision unacceptably undermines the acquis developed under PSD2 and RTS SCA 2018/389. Namely:

- Instead of obliging ASPSPs to have strategies and plans for contingency measures as before, the current draft Article 38(1) PSR basically introduces a guarantee-basis liability - and therefore the most far-reaching type of liability - of ASPSPs to prevent unavailability of a dedicated interface. By indicating that ASPSPs "shall take all measures in their power" means that, disregarding proportionality rules, ASPSPs should allocate all possible resources, including financial ones, to ensure the continuous availability of a dedicated interface. Such a wording of the provision cannot stand, as it distorts the rules of competition between the ASPSP and the TPP, placing too much burden on the ASPSP, and at the same time threatens the stable management of the ASPSP;
- Secondly, contrary to the correct RTS SCA 2018/389 rules in this respect, the current wording of Article 38(1) PSR assumes that the ASPSP has an obligation to prevent any unavailability. Meanwhile, RTS SCA 2018/389 properly indicated that it was about unplanned unavailability, and a system breakdown. However, it cannot be ruled out that ASPSPs will conduct development work on a dedicated interface, which is desirable, but may lead to temporary unavailability.

Art. 38(2) mandates that in the case of the unavailability of the dedicated interface, ASPSPs must promptly offer TPPs an *effective alternative solution*, such as "the use of the interface that the account servicing payment service provider uses for authentication and communication with its users directly". At the same time, however, Art. 38(7) requires TPPs to identify themselves to ASPSPs when using the direct customer interface as an alternative solution. We suggest the PSR specifies the method of identification for TPPs both when using dedicated interfaces and an alternative solution, such as whether an eIDAS certificate is still required. Moreover, it should be clarified in Art 38(7) that there is no obligation for an ASPSP to provide an identification solution for a TPP as part of the effective alternative solution under Art. 38(2) or as part of the technical specification under

Art 38(6). In fact, implementing such extra identification solution will result in significant costs for ASPSPs and would in fact make the development, operation and maintenance of a fallback solution mandatory.
Art. 38(3) stipulates that, where the dedicated interface is unavailable and the ASPSP has not offered a rapid and effective alternative solution, the TPP may request its competent authority to allow it to use the interface used directly by the PSUs. At the same time, in accordance with Art. 38 (5), as long as the competent authority has not taken a decision on the request, the requesting TPP may use interfaces directly used by the PSUs. This approach may create opportunities for abuse, and could enable TPPs to circumvent their obligations to communicate securely through APIs. It can also lead to the continued use of the undesirable practice of screen-scraping (cf. Recital 61 of the PSR). It is recommended that the sequence of actions be reversed, whereby a TPP should not be permitted to use an interface directly used by a PSU until it has obtained approval from the competent authority. At the same time, it is advisable to establish a requirement for the competent authority to issue a decision within a short timeframe, such as two working days. It should further be clarified in Art 38(3) that the ASPSP needs to be informed about such request by the competent authority. The ASPSP should also be able to take action against the decision.

Articles 40 and 41 – Obligations of account servicing payment service providers regarding payment initiation services and account information services

With regard to Articles 40(c) and 41(1)(b) the wording "without any discrimination other than for objective reasons" should be introduced again. There can be objective reasons to treat a payment differently, for example if equal treatment would breach obligations towards the TPP such as not to allow deletion towards the ASPSP after a certain point in time or otherwise conflicts with the typical business model of TPP. This would cater to for instance national characteristics or other types of complexities or risk willingness of institutions.

Art. 41 does not limit the number of requests a PSP can issue per day (or other time unit). This proposal sets incredibly high standards on the systems' scalability. There is an obvious and very likely risk that this will lead to an overload of the ASPSPs' systems as the PSPs can and will make numerous subsequent requests to maintain a semblance of real-time updates to the PSUs. A limitation, according to the current SCA RTS Art. 36(5)(b), should remain.

Article 43 – Data access management by payment service users

We generally welcome the proposal to have permission dashboards to provide PSUs with an overview but needs some amendments in wording to serve its purpose and function properly:

- Since ASPSPs are not part of the PSU – TPP relationship, they are not in the position to "monitor and manage" permissions. They can however provide their customers an overview of the (third) parties that had access to specific payment accounts, including the possibility to withdraw or simply block (and unblock) any future access with immediate effect. The provision should therefore read: "*The account servicing payment service provider shall provide the payment service user with a dashboard, integrated in its user interface, to monitor and manage the ~~permissions~~* ***authorised access*** *the payment service user has given for the purpose of account information services or payment initiation services covering multiple or recurrent payments."*
- It should further be clarified which consequences a withdrawal of access by the payment service user under 43(2)(b) has in the context of payment initiation

services. It is unclear whether a withdrawal means that upcoming recurring payments shall not be executed any longer. It is also unclear when the criteria for multiple payments are fulfilled and what a withdrawal of access means in the context of multiple (potentially already executed) payments.

A definition of "permission" is necessary to avoid any misinterpretation, also according to what is stated in GDPR with the concepts of "consent", explicit consent" and so on. In this regard, we suggest considering the recommendations made by the EDPS Opinion 39/2023 on PSR/PSD3 according to which it is relevant "*to differentiate clearly between 'permission' (referring to the acceptance of the commercial service by the consumer), on the one hand, and 'consent' (under Article 6(1)(a) GDPR) or 'explicit consent' (under Article 9(2)(a) GDPR), on the other hand. Recital (69) should therefore be amended to clarify that "permission should not be construed as 'consent' or 'explicit consent' or 'necessity for the performance of a contract' as defined in Regulation (EU) 2016/679".*

- We strongly suggest removing from Art. 43(2)(a) sub (iii) "purpose of the permission" and as a consequence also paragraphs 4(a) and 4(b) sub (i) should be deleted. It is unclear whether the purpose refers to the PSU (i.e. the purpose of permission provided) or the service offered by the TPP (i.e. the purpose of the service). In both cases, it is not for the ASPSP to know and the ASPSP should not be involved. Also, ASPSPs may not have such information at their disposal and are unable to ask TPPs for such information (as ASPSPs shall not verify the permission according to Article 49(4) and any additional checks of the permission is considered an obstacle according to article 44(1)(c)). Therefore, the purpose of the permission should be provided in the dashboard only if such information was previously provided to ASPSP by the TPPs. In addition, ASPSPs and TPPs must manage the permission also in a way that is agreed together with the PSU according to Articles 49(5) and 49(6).
- In the case a third party without a license uses an aggregator with a license (a business model known as "license-as-a-service") to access a customer's data, it is desirable to include the name of the unregulated third party who is using the customer's data. Only mentioning the name of the aggregator is mildly informative to the PSU and not really transparent.
- Prescribing the dashboard to show "the categories of data being shared" (Art. 43(2)(a)(v)) lacks specificity and may prove difficult to implement, let alone implement it uniformly across the EU; we think the informational value of a dashboard will not decrease if this sub were to be deleted; conversely it should be clarified what is intended with "categories of data being shared".
- Re-establishing a withdrawn permission (art. 43(2)(c)) should be performed via the AISP or PISP, not via a dashboard since these TPPs have no access to the dashboard and would be unaware of changes. Moreover, we assume that this requirement is limited to the data access permissions that have been withdrawn or expired in the past two years, as per Art. 43(2)(d).
- Art. 43(4)(a) states that "the account servicing payment service provider shall inform the account information service or payment initiation service provider in real time of changes made to a permission concerning that provider made by a payment service user via the dashboard". The wording of Art. 43(4)(a) of the PSR may imply that users should have the ability to not only withdraw permissions and re-establish data access but also modify the permissions granted. It should be clarified that this is not the case. There should not be a requirement to push information in real time from the ASPSP to the TPP as this would come with the complexity mentioned earlier. Instead, the information could be provided on request but limited to 4 times per 24-hours period.
- We strongly suggest maintaining alignment with the permission dashboard requirements foreseen in FIDA proposal since it is relevant in terms of containing the bank's implementation efforts and of offering a comparable experience to the user. Thus, it should be clarified that the dashboard for the purposes of PSR and FIDA needs to be based on the same legal and technical principles in order to

ensure a consistent customer experience and economic synergies. In the context, also further guidance on the dashboard content could be provided.
- An obligation of TPPs to inform ASPSPs about the withdrawal of an ongoing permission should also be added (e.g. in Art. 43(4)(c).

Article 44 - Obstacles to the use of API

Some of the obstacles listed in this Article are not worded in the same way as the EBA has so far clarified regarding obstacles. It is important that alignment with the existing EBA clarifications is ensured so as to limit implementation changes.

Articles 43, 46, 47, 49, 86 – Obligations of PIS and AIS, especially in relation to permission for corporates

It needs to be clarified that TPP need to obtain a separate permission from the corporate/authority in the corporate area and that performance of SCA is not sufficient. Especially in the large corporate area and for solutions used by authorities, access rights and signing rights for payments can be complex and on a very detailed level. Often, these set-ups consist of an appointed administrator, which has the right to appoint users, but not necessarily own access rights/signing rights. Appointed users often only have access to certain account data or certain payment related rights. Such administrators and users are usually not authorised to sign agreements on behalf of the company. Our understanding is therefore that permission on behalf of the company cannot be given through performance of SCA by an administrator or user. Instead, the TPP needs to negotiate permission with authorised representatives of the company and ensure to only use the dedicated interface once such permission has been given by the company in question. Any other approach, especially in the AIS area, would pose a security risk for the company/authority. Confidential and potentially even classified information could be transferred to a third party upon performance of SCA by a single user, without the company/authority being aware of such transfer. This makes it impossible for the company/authority to remove access rights in case of termination of the employment or to have access controls in place.

Under PSR, it further needs to be clarified on which level the SCA to access payment account data as described under Art 86(3) should be performed for corporate customers. To our understanding, such SCA would have to be performed by someone who is entitled to give access to all data (hence usually on administrator level). We would also understand PSR in a way that the ASPSP upon such SCA can assume that permission for payment account access has been given and hence reflect such access in the permission dashboard. A similar clarification is needed with respect to payment initiation services covering multiple or recurrent payments – can it be assumed that permission has been given as soon as one such payment was created for a corporate PSU? It should further be clarified what access rights are needed to withdraw such permission in the dashboard.

Given the complex, tailor made solutions in the large corporate area, it should be generally considered to allow more flexibility for such solutions, for example by excluding this area from the compliance scope or introducing some derogations.

Article 48 - Role of competent authority

Prior to issuing enforcement measures and sanctions, competent authorities should be obliged to provide specific guidance to an ASPSP as to (a) if a matter addressed by a TPP

is indeed an obstacle and if so, (b) which concrete measures should be taken to mitigate the situation, combined with a realistic period to implement requested changes.

The enforcement measures towards TPPs should be equally strict as those towards ASPSP and should not only comprise the use of the access interface, but also measures to prevent fraud and money laundering. Art 48(7) should also oblige TPPs to provide data about their data access (and not only were deemed appropriate by competent authorities). This would allow competent authorities to detect screen scraping more easily.

1. Strong Customer Authentication

Article 86 - Strong customer authentication in respect of payment initiation and account information services

The PSR now provides that the first SCA is carried out by the ASPSP and that subsequent SCAs (after 180 days) are carried out directly by the AISP. This is a novelty, as the subsequent SCAs are currently carried out by the ASPSP. No guidance has been provided to ensure communication between the AISP and the ASPSP regarding this SCA renewal.
From a fraud prevention perspective, it appears important that ASPSP have information on performance of SCA (and related information relevant for transaction monitoring) and such data should therefore be provided from AISP to ASPSP. It should further be clarified how this provision is to be understood in the context of re-establishing withdrawn access and/or extension of access to further payment accounts. We assume that in such situations, ASPSP-SCA would have to be applied again (otherwise AISP's would forever be able to obtain access without ASPSP-SCA).

Article 85 – Strong customer authentication

Generally, there is a need for clarification for the different scenarios mentioned in Art. 85 as to which payment service provider(s) is supposed to perform strong customer authentication in the situation at hand. The principles developed under PSD2 that it is the responsibility of the payer PSP to perform SCA should still apply and should be reflected in the provisions. For Article 85(2) vs 85(3) and Article 85(5) vs (6) there appear to be different requirements for transactions made with payment instruments and direct debit transactions (given that the wording differs). The same conditions should apply for all payee initiated transactions. A different treatment appears to be unjustified.

In contrary to Article 85(12) the principle that the SCA elements should belong to different categories should be kept. Else, there appears to be a higher risk for fraud.

Article 87 - Outsourcing agreements for the application of strong customer authentication

We are concerned this Article may lead to PSPs needing to enter into outsourcing agreements with several companies. We therefore would like to ask for a clear definition of a technical service provider be included in Article 3 of PSR, to understand which parties fall in the scope of this Article.

For instance, we are concerned that manufacturers of smartphones that produce phones with device features like face-ID or fingerprint reading could be viewed as 'technical service providers' and therefore subject to outsourcing agreements with every PSP that decides to use such features for authentication/authorisation purposes. Not only would this result in millions of contracts (which may also be subject to auditing under current EBA outsourcing guidelines), it would most importantly be unclear and unproven how such requirement would increase the security of authentication processes. Currently PSPs can decide whether a particular phone offers sufficiently secure device features to be used for authentication purposes based on relevant international security standards and device specification documentation. In general, it should always be the bank that assesses the risk whether outsourcing is involved or not, and providers should be required to enter outsourcing agreements in that case based on the rules already in place in this area. A general requirement to enter into outsourcing agreements for all SCA methods where other parties are involved, could create barriers to entry for new and smaller players instead of opening up the market and enabling the development of innovative solutions. European regulation should be clear enough to allow banks to take proportionate decisions as to whether outsourcing agreements are required. Therefore, instead of a generic provision on outsourcing agreements, PSR should make TSPs subject to a certain number of mandatory provisions to ensure PSU's safety and a fair distribution of duties and liabilities between digital pass-through wallets and ASPSPs by drawing down or make a proper reference to the existing requirements under EBA Guidelines on outsourcing arrangements.

Article 88 - Accessibility requirements for SCA

We appreciate the proposed text and hope that a proper alignment with the European Accessibility Act (EAA) is maintained in terms of contents as well as timing of adoption and transposition at the national level. We believe that this Article should retain the reference to the ASPSP's specific user base to allow for the development of different models in the market and to ensure the necessary technological neutrality so to equally allow for the development of as diverse solutions as possible that meet the various needs of users.

Indeed, PSPs already offer a variety of SCA methods to cater for their entire client base. We acknowledge the Commission's aim to ensure that all client segments have access to at least one SCA method. However as currently drafted, the Article is too wide/generic in the description of customers with specific regards to the concept of "person with low digital skills" who should benefit from these alternative ways of carrying out SCA. Therefore, we suggest better specify the proposed text to avoid any misunderstanding and provide for a common methodology for assessing the digital competencies of users.

Also, we believe that this provision would entail a very large financial and operational burden to PSPs and seems to be in contradiction with or stricter than the requirements from the EAA. Moreover, this requirement could conflict with GDPR, as it could force PSPs to register the specific needs of customers resulting from their disabilities which may include sensitive personal data. We therefore suggest sticking to the EAA scope and requirements in this context. The EAA accessibility requirements are already extensive and tailored to online methods. In section IV the following requirements are included:

i. providing identification methods, electronic signatures, security, and payment services which are perceivable, operable, understandable, and robust;
ii. ensuring that the information is understandable, without exceeding a level of complexity superior to level B2 (upper intermediate) of the Council of Europe's Common European Framework of Reference for Languages.

Finally, while we agree with the underlying principle of the Article in leaving room for different models of SCA beyond smartphone ownership, we believe that it should be better clarified that this provision is not aimed at non-consumers, (e.g., corporate card programs by adding Article 88 to the list of opt-out provisions in Article 27 for non-consumers) in order to preserve the specificities of a bank's strategy in SCA application and, consequently, market competition.

2. Access to payment systems and to accounts maintained with credit institutions

With regard to access to payment accounts (Article 32), the following amendments are required:

- Paragraph 1 introduces a closed catalogue of reasons for which a credit institution may refuse to open a payment account for a payment institution, its agents, distributors or applicants, or close such an account. Predicting the exact catalogue of events that may lead to the denial of an account by a credit institution is essentially impossible due to the specific risk management rules and criteria employed by credit institutions. The introduction of a closed catalogue of cases will limit the ability of credit institutions to refuse to open an account in cases where such refusal is justified. For instance, credit institutions must be able to assess which AML risks it accepts. The PSR should not interfere with AMLD/AMLR provisions and should allow credit institutions to fully consider AML/CTF risks associated with opening the account. Therefore, the grounds for refusal indicated in this provision should be presented as illustrative rather than exhaustive, and an explicit reference that AML regulations remain in place should be included. When refusing to open or close an account, a credit institution should adhere to general but specifically justified reasons. Further, we believe essential to ensure that the EBA provides further guidance on how credit institutions can deal with the interplay with AML/CFT obligations. The wording of Art. 32(5) 'EBA shall develop draft regulatory technical standards specifying the harmonised format and information to be contained in the notification and motivation' does not seem to include such guidance.
- It should be further defined what precise services should be considered in scope of this Article (i.e. what is considered as 'payment account services' as referred to in paragraph 4. For instance granting credit facilities should not be in scope of these services).
- Article 32 should not apply to 'applicants for a license as a payment institutions as that would mean that de facto the credit institution would have to determine whether the institution actually meets the requirements to be licensed as a payment institution. All the provisions should apply only to payment institutions that have obtained their license.

With regard to access to payment systems (Article 31), it is important that providers, whether bank or non-bank PSPs, should be subject to equivalent safeguards and requirements when accessing payment systems in order to safeguard the security and the stability of the systems.

Moreover, we suggest guaranteeing full alignment between what is provided in Articles 31 and 46 of PSR and the measures provided in the IPR regarding the amendments to SFD and PSD2.

3. Data Protection

Overall, the proposal takes a welcome step forward in terms of clarifying the interplay with the General Data Protection Regulation, which was one of the **main lessons learned from PSD2 implementation and the subsequent EDPB Guidelines** on the interplay between the two frameworks.

Reference to this interplay is present in several places in the Regulation:

- **Recital 69** rightly points out the confusion caused by the using the term "explicit consent" under PSD2 – a term also used in the GDPR. The European Data Protection Board (EDPB) Guidelines on the Interplay between PSD2 and GDPR clarified that under the PSD2, "explicit consent" is a contractual consent. The current proposal also takes a welcome step by seeking a clear differentiation between data protection rules through using the word "permission". **This differentiation should be maintained.** Yet, in the final sentence of the paragraph "*Therefore, permission should not be construed exclusively as "consent" or "explicit consent" as defined under…"* we suggest to delete "exclusively" as this can cause even more confusion.

- **Recital 97 clearly indicates that GDPR applies when there is processing of personal data under PSR** and that it in order to process personal data under the PSR lawfully, **it is necessary to fulfil the conditions of the GDPR**, including having an appropriate legal basis (e.g. performance of a contract) and respecting the data protection principles. We also welcome the reference to so called "silent party data": that the provision of AIS services may entail the processing of personal data of a data subject who is not the user of a specific payment service provider, but whose personal data processing by that provider is necessary for the performance of a contract between the provider and the PSU. This should also include the ASPSP obligation to process this data as part of their obligations under PSR.

- **Recitals 93 and Article 80** cover the issue of **processing special categories of personal data** (SCPD) and, importantly, **give a clear legal basis** to processing this type of data in the context of PSR – Art. 9(2)(g) – for "substantial public interest." An explicit reference to Art. 9(2)(g) GDPR should be directly included in Art 80. This was missing under PSD2. However, we do recommend to make a distinction in Article 80 when it comes to the processing of SCPD "*to the extent necessary for the provision of payment services".*

  There is a difference between personal data that, on the one hand, are processed as such to **deduce specific information** such as any of the categories of data outlined under Art. 9(1), e.g., medical devices used to assess the medical situation of persons) and on the other hand, personal data which are **not used for their inherent characteristics but which are part of the set to be processed**.

  In the first case, processing has to be **intentionally undertaken by the controller with the purpose element** in mind and here, controllers would apply the conditions under Art. 9 GDPR and, in the case of PSR, requirements such as those under paragraphs (a) and (b) of Art. 80. However, if financial transaction data are not processed in order to infer SCPD, Article 9(1) GDPR nor Art. 80(a) or (b) should apply. This is important to clarify because it can have significant operational consequences for banks, particularly as additional technical measures need to be taken.

  We would therefore suggest to delete the reference to "necessary for the provision of payment services".

  Payment systems and payment service providers shall be allowed to process special categories of personal data as referred to in Article 9(1) of Regulation (EU)

2016/679 and Article 10(1) of Regulation (EU) 2018/1725 ***~~to the extent necessary for the provision of payment services and~~*** *for compliance with obligations under this Regulation, in the public interest of the well-functioning of the internal market for payment services, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including the following:[..].*

- **Recitals 102 and 103** and Article 83 cover the issue of processing personal data to help the investigation and detection of payment fraud and, notably, include a legal basis for information sharing to help combat fraud. Yet, there are still some open questions:
    - Is processing personal data for fraud purposes now based on a legal obligation (Art. 6(1)(c) GDPR) or does processing personal data for fraud purposes still rely on legitimate interest (Art. 6(1)(f) GDPR, as under PSD2) except for the case of transaction monitoring, in which case it is based on a legal obligation (Art. 6(1)(c)? We recommend to clarify this in the text.

- We would like to remind that a TPP needs to secure a lawful ground to process data (also mentioned by the EDPS under paragraph 15 of their opinion on the PSR). As data controllers, TPPs must meet the necessary requirements and responsibilities of the GDPR.

6. Miscellaneous

Article 51 – Limits and blocking of the use of the payment instrument

We strongly advocate for the removal of the sentence "Payment service providers shall not unilaterally increase the spending limits agreed with their payment service users" from Art. 51(1). It is currently unclear what 'spending limits' refer to, it could for instance be the limit for credit transfers or the maximum spending limit on contactless card payments. Regarding the latter, it is in the consumer's best interest to ensure that PSPs can increase the limits without PSU involvement, which PSPs for instance did during the COVID-19 pandemic when contactless limits for card payments were increased from 25 to 50 euro. Also in normal times, PSPs might need to increase the spending limits due to, for instance, inflation. Requesting each PSU's permission will result in an operational disaster.

Article 75 – Payment service providers' liability for non-execution, defective or late execution of payment transactions

PSR introduces the term "execution of a payment transaction" in art. 3(8). This definition concerns the phase after the initiation of a payment transaction has been completed. This flow can be illustrated (in a simplified manner) as follows:

1) The payer's bank deducts the amount from the payer's payment account;
2) The payer's bank transfers the amount to the payee's bank;
3) The payee's bank transfers the amount to the payee's payment account.

The term "execution of a payment transaction" will however lead to problems in relation to the liability of the payer's bank. This is because – in its current form – the execution phase of a payment transaction only ends when the transaction amount arrived at the payee's payment account. However, as becomes clear from the simplified illustration, the payer's bank has no control on the last step of the execution of a payment transaction. The last step is performed by the payee's bank, after receiving the transaction amount from the payer's bank. The payer's bank should only be responsible for the steps that it controls.

The definition could lead to problems in Art. 75(1), that both refer to term "execution of a payment transaction". The Article clarifies in Art. 3(8) that payer's bank is not liable to the payee, when it can prove that the transaction amount arrived at the payee's bank. This liability should be extended to the payer. In its current form, Art. 75(1) holds the payer's bank liable for a part of the transaction that is out of its control.

Art. 49 - Authorisation

The predecessor of Art. 49(7) in PSR is Art. 64(3) in PSD2. Compared to Art. 64(3), two major amendments were made in Art. 49(7) of the PSR:

- Removal of the reference to Art. 66 in PSR (art. 80 PSD2);
- Introduction of the term 'execution of a payment transaction'.

These two amendments lead to confusion on the exact relation between Art. 49(7) and 66(1) in PSR. Art. 66(1) states that a PSU shall not revoke a payment order once it has been received by the payer's PSP, while Art. 49(7) states that the PSU can withdraw permission to execute a payment transaction at any time. As explained, execution of a payment transaction only ends when the funds have arrived at the payee's payment account. Due to the use of the new term "execution of a payment transaction" in Art. 49(7), no transaction is final anymore. For instance, in the current wording of Art. 49(7), the payer could revoke a payment when the funds were credited to the beneficiary's PSP but not to the payee yet.

Given the above-described issues, we suggest to stick to PSD2 Art. 64(3).

Articles 25 – Information for the payer on individual transactions

Especially with regard to paragraph 1, point (a) and the reference to the payee's commercial trade name, it should be noted that this information is not necessarily collected/stored by PSPs; moreover, PSPs are only able to provide the information if it is provided by users (beneficiaries or debtor for transactions initialized by the debtor).

Article 60(3), 76(2), 78 Right of recourse between payment service providers

The scope of the different rights of recourse should be extended. Article 60(3) should not only exemption cases (which we understand as cases where SCA would have to be applied, but an SCA exemption is used). It should also cover:

- Cases where only the payee knows if the requirements where SCA does not have to be applied under Art. 85 PSR are fulfilled (e.g., where an action of the payer preceded the transaction - MIT, or where MOTO requirements are not fulfilled etc); and
- Missing mandates; and
- Mandates created by the payee PSP/other PSP involved without SCA (provided that in such case payee SCA would have to be applied - see comments on art 85 for unclarities in the related provisions).

A direct compensation right for the payer PSP towards the payee could also be introduced in case of misuse of MOTO/MIT requirements.

Article 60(3) should also cover PISPs given that the same exemptions are to be used also in PISP cases, but may not control the flow in a similar way. It should be clarified that the liability in Art. 85(7) is on the payee's PSP if the security checks have not been carried out by the payee/payee PSP.

Article 74(1) - Incorrect unique identifiers

Article 74(1) states that the payment transaction shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier. We suggest amending the article to consider that the check service could be carried out with other elements (e.g., VAT, fiscal code, etc.) in addition to the name of the payee so as to leverage the existing market solutions. However, we strongly suggest that no change to the definition of "unique identifier" is introduced in PSR, because this might have far reaching implications for all obligations related to unique identifiers, included but not limited to art. 74, and may have unintended consequences if not carefully assessed.

Article 79 – Abnormal and unforeseeable circumstances

It should be considered if Article 79 should also cover Open Banking Chapter 3.

Article 112 – Entry into force and application

- Art. 89 states that "EBA shall submit the draft regulatory technical standards referred to in paragraph 1 to the Commission no later than 12 months after the date of entry into force of this Regulation. Power is delegated to the Commission to adopt those regulatory technical standards in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010." Now most of the provisions of PSR shall apply 18 months after the entry into force, i.e. the transaction monitoring. This means that the final RTS requirements will not be known likely until a few months before the provisions of PSR become applicable, giving little time to implement them.
- Having said that, we strongly ask for an alignment of the timelines for adoption considering that PSR will be immediately applicable, and a long interim period should be avoided in order to limit as much as possible the legal/operational uncertainty in the rule's application.
- Alternatively, we would ask to insert rules on the transitional period to allow PSP for the correct application of the provisions where RTS/GLs are foreseen.

Article 107 - Remove fragmentation in the payments landscape through further harmonization

One of the overarching objectives of establishing a Regulation (e.g. PSR) was to ensure a harmonized set of rules for PSPs and PSUs and remove existing fragmentation in the EU payments landscape. Unfortunately, by including Article 107 we believe it would promote further fragmentation in terms of refund rights and SCA obligations, thereby potentially distorting the level playing field. In our view, the EU payments landscape requires more harmonization to ensure that all financial entities and consumers are subject to the same level of regulation. Therefore, the provision should not allow for disparate and additional requirements on refund rights, transaction monitoring mechanisms and fraud risk and trend communications and training, as the purpose of PSR is to ensure consistency between Member States on the implementation of requirements.

For more information contact:

Alexandra Maniati

Senior Director, Innovation & Cybersecurity, a.maniati@ebf.eu

Anni Mykkänen

Senior Policy Adviser, Payments & Innovation, a.mykkanen@ebf.eu

About EBF

The European Banking Federation is the voice of the European banking sector, bringing together national banking associations from across Europe. The federation is committed to a thriving European economy that is underpinned by a stable, secure, and inclusive financial ecosystem, and to a flourishing society where financing is available to fund the dreams of citizens, businesses and innovators everywhere.

www.ebf.eu **@EBFeu**