POSITION PAPER

ESBG position paper on the proposed Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

ESBG

BACKGROUND

On 28 June 2023, the European Commission (EC) published proposals for a Regulation on payment services in the internal market (PSR) and for a Directive on payment services and electronic money services in the internal market (PSD3). These legislative proposals aim to further improve consumer protection and competition in electronic payments. You can find the factsheet here.

The proposals aim to amend and modernise the current Payment Services Directive (PSD2), which will become PSD3 and establish, in addition, a Payment Services Regulation (PSR). In particular, the proposals aim to ensure that consumers can continue to make electronic payments and transactions in the EU safely and securely, domestically or cross-border, in euro and non-euro. It also aims to provide greater choice of payment service providers on the market.

The EC states that these amendments represent an evolution, not a revolution of the EU payments framework. The amendments aim to improve the functioning of EU payment markets by:

- strengthening measures to combat payment fraud;
- allowing non-bank payment service providers (PSPs) access to all EU payment systems, with appropriate safeguards, and giving them a right to have a bank account;
- improving the functioning of open banking, especially as regards the performance of data interfaces, removing obstacles to open banking services and consumer control over their data access permissions;
- reinforcing the enforcement powers of national competent authorities and facilitating implementation of the rules, clarifying various elements;
- further improving consumer information and rights;
- improving the availability of cash;
- merging the legal frameworks applicable to electronic money and to payment services.

Links

- PSR here and PSR Annex here.
- PSD3 here and PSD3 Annex here.
- EC press release here.
- EC Q&A here.
- EC Have your say webpage here.

Table of Contents

General comments

Holistic approach

We understand the PSR, PSD3 and the Regulation for Access to Financial Data (FIDAR) as three legislative proposals that are highly interconnected and therefore should be treated in an aligned procedural way with due consideration for the Instant Payments Regulation (IPR). Although, we understand that aligning the three proposals in the decision-making process may be challenging, we believe that it will be crucial to prevent any conflict in the applicability of the different tranches of provisions. The application timelines of the three proposed legislative acts should be aligned and leave sufficient room (at least 24 months, as was the case for PSD2) to allow Payment Service Providers (PSPs) to adapt to the new rules that will impact both customer offerings and processing of transactions. This is even more relevant as there are a number of significant changes in other relevant legislative acts expected, such as the Settlement Finality Directive, the aforementioned IPR and implications for the SEPA Regulation. Regarding the integration of different regulatory frameworks for financial data sharing and for greater coherence thereof, access to, and sharing of payment data, as well as other financial data, must also be included within the framework of the FIDAR. In this way, all financial data would be shared through a single API, taking into account enhanced functionality for payment initiation. The establishment of two different frameworks and different rules for financial data sharing (FIDAR on one hand and PSR/PSD3 on the other) hinders customer permission management and, also, entails higher costs and operational difficulties. Under FIDAR, for example, it is to be possible to charge financial information service providers for the provision of data. Therefore, with the amendment of the legal framework for payment services, a way must be shown how this can be adapted to the specifications of interaction with third-party services in payment transactions. Finally, an appropriate legal framework for the use of financial services data offers long-term benefits for the entire payment ecosystem.

Impact assessment

The potential consequence of this proposal on existing payment businesses is immense. It will include process changes, system impact and customer offering including updates in customer agreements. In light of the focus on resilience, stability and the important AML work, the combined burden on banks as PSPs will be disproportionate and therefore require a significant implementation period. A considerable implementation period is further justified by the fact that the proposed PSR is not only extensive, but also highly detailed. While there are to be many technical standards provided, the industry is yet to be advised of the details of these standards which will determine the effect on PSPs and consumers. At times, the proposed PSR is very detailed in our view, provisions subject to technical standards should be less detailed and leave it to the technical standards to clarify the details. It is crucial that the banks and PSPs are able to deliver on their obligations under proposals, with diversity in their own systems and the challenge of aligning with numerous supervisory frameworks.

The impact assessment indicates "consumers' lack of confidence in payments". Without denying a problem of fraud in the market, which also has to be addressed by measures outside the payment industry, the constantly growing use of electronic means of payment does not support this statement which should be more orientated towards fraud prevention at Payment Service User (PSU) level. The constant and rapid growth of electronic payments in fact suggests that there is consumer trust in these payments.

Furthermore, we question the impact assessment stating that there is a "limited choice of payment services, with prices higher than they need to be". Today, PSUs can choose between multiple payment service providers offering different payment services, within a fully competitive marketplace, and they can even make use of payment initiation services.

Similarly, we do not agree with the statement that "Open Banking providers face obstacles" as it is for the regulators to identify and eliminate such obstacles. The market shows, rather, a very limited interest in Open Banking services by PSUs, explaining the small uptake in its solutions. In this context, we furthermore question the "specific objective 2" of Open Banking, as this means considerable investments for ASPSPs in Open Banking, despite very limited demand for such service. However, we support the ambition to not have an exemption for the fall-back procedure.

Associated costs
The statement in the Explanatory Memorandum that the costs are primarily implementation costs and there are no additional costs through ongoing operation, is not comprehensible with regard to the IBAN/name comparison (see page 6). Since at least one verification transaction must be sent for each payment transaction - and a fragmentation of the markets is to be expected with this IBAN/name comparison - the running costs for the processing of payment transactions will probably increase significantly, perhaps doubling. In addition to an expected increase in customer uncertainty, an automated "clicking away" of warning messages from customers is also to be expected.

Clarification
Besides, more concrete information (e.g., in Recitals) on how a CoP (Confirmation of Payee or IBAN check) is to be carried out seems to be necessary. The same applies to Article 55 PSR on the evidence on authorisation and execution of payment transactions.

Recitals

26 – In light of how many terms and conditions for the PSPs are worded and "designed" presently, and the relative lack of information provided to their PSUs (or how hidden that information is in T&C clauses), it can be questioned whether it is in line with customer protection interests to expand the possibilities for PSPs to share aggregated information without simultaneously ramping up

supervisory efforts in this area. It should be enforced that the "end consumer" of the aggregated account information should always be a licensed entity (AISP), with additional requirements on licenses and permits for any additional actions that this entity intends to take with the information. For instance, to perform credit scoring based on that information. Otherwise, the requirement that only licensed AISPs and PISPs should have access to the APIs (preamble 58) loses its effect. It can, however, be noted that Article 47.2.(b) does not include any other use of the data, specifically restricting access to data that is needed for the requested payment service to be provided. Further use of the information collected under PSR should therefore be considered as prohibited. 48 – National possibilities to further reduce the possibility to unilaterally change terms and conditions for payment services. This recital does not appear to have any corresponding regulation in the articles. If the recitals are to be used as grounds for interpreting the lawmaker's intentions within the regulation, it is important that the recitals are not too loosely formulated and far-reaching, since it could cause issues in interpretation.

I. Title on the subject matter, scope and definitions

Definitions, Account information service. We welcome an overview of the AIS definition, as some market actors use the AISPs' PSD2 APIs for other measures than for the AIS scope intended by the PSD2 legislator. However, introducing AIS through unlicensed technical service providers is not acceptable. Article 3 (20) Definitions, Payment initiation service. The definition is extended to cover payee-initiated payment orders. It is important to note that such a service must only be rendered by PIS based on a previously agreed mandate from the payer to the payer's ASPSP with SCA. We think this should be clarified in the regulations, perhaps Article 36 (4), Article 85 (2) by narrowing down the scope. We understand that the intention is for the one-off payee-initiated to be out of scope. This is important as otherwise it would open up payment orders to not be accepted by the payer at all with no means of control for the payer or the payer's ASPSP. It should be noted that currently other mechanisms for consent exist. As an example, in some countries the mandates are managed differently, orchestrated by a central entity, and, in the card world, the mandates are given in the merchant environment with little possibility to validate by Payers PSP.

II. Title on the transparency of conditions and information requirements for payment services

1. Chapter on general rules

No comments received so far.

2. Chapter on single payment transactions

Information for the payee after execution (Article 17)
We ask for clarification on how a bank, as the payer's PSP, shall be able to provide the payee's commercial trading name, as laid down in point (a), if this bank does not receive it from the payer (credit transfer) or the payee (card payment or direct debit).

With regard to point (d), we wish to highlight that the exchange rate for card payments is not yet known at the moment of the actual payment initiation/order. An extension of the information obligations of payment service providers regarding currency conversions for credit transfers to third countries, as foreseen by the EU Commission, is not appropriate (Articles 13(1) (f) PSR). It is already unclear which central bank is to be considered as the relevant central bank for the foreign exchange reference rate.

3. Chapter on framework contracts

As the EU payment services legislation is limited to the EU Member States, provisions for payments involving third countries are currently the exception. An extension of the information obligations of payment service providers regarding execution times is not appropriate (Article 20(a) (vi) PSR). Due to the lack of global effect of EU payment services legislation, a payment service provider cannot provide information on certain aspects that are outside its controllable sphere of influence, such as the execution time.

III. Title on the rights and obligations in relation to the provision and use of payment services

1. Chapter on common provisions

Article 27 (1) must include the new Article 57 on liability for incorrect matching in verification services. As with other regulations on liability including Article 60, this too should be left up to the PSP and the corporate customers to agree otherwise. The proposed Instant Payment Regulation does not entail liability for incorrect application of this IBAN matching service and the regulations should be harmonised at least in respect of the corporate market.

Article 27 (1) should include the new Article 58, consistent with including Article 60 and thereby the possibility to agree that the PSP shall not be liable to the payer for failure to require SCA, cf. Article 60 (2).

2. Chapter on access to payment systems and to accounts maintained with credit institutions

Provision by credit institutions of payment accounts to payment institutions (Art 32)
It is vital that the PSR does not introduce new AML requirements, rather, the PSR should refer to the AML regulations in force. For example, the requirements that should be applied before an ASPSP establishes or terminates a business relationship with payment institutions is already governed by applicable AML regulations, nullifying the stipulations in the PSR. Moreover, ASPSPs cannot be forced to accept risk profiles as long as they are below "excessive" as it is up to the ASPSP to decide on its risk appetite, we are also against the extension of this Article to agents and distributors.

Access to payment systems (Article 46 PSD3 and Article 31 PSR)
The Settlement Finality Directive (SFD) was intended to expand the range of participants in payment systems in order to maintain a fair competitive environment ('level playing field') and to prevent systemic risks by providing adequate specifications for the system operators. One such "SFD payment system" is the TARGET system of the Eurosystem. So far, only credit institutions are allowed to participate directly in this system. Payment institutions have so far only been able to participate indirectly, e. g. by means of a mandated credit institution. The different supervisory requirements for credit institutions and payment institutions beyond the scope of payment services legislation can nevertheless result in different risk profiles with corresponding effects on payment systems and their participants. Payment system operators must be given the opportunity to compensate for this through supplementary participation requirements or restrictions.

3. Chapter on account information services and payment initiation services

i. Section on general principles

No comments received so far.

ii. Section on data access interfaces for account information services and payment initiation services

Provision of dedicated access interfaces (Art 35)
In the requirements for the dedicated interface, there is a "built-in" requirement on identification of the PSP, specifically through the use of a certificate that identifies the PSP as a duly licensed payment institute. If PSPs are to be allowed, if only in the case of unavailability of the dedicated interface, to use an ASPSP's customer-facing interface (Article 38), there is a risk that the ASPSP either: i) must provide a customer-facing interface where the PSP can identify with a certificate and where the access to information must be possible to limit to

payment account data, in order to avoid GDPR incompliance; or ii) block (to the extent possible) any attempts from PSPs to access information through the customer-facing interface, in order to avoid a breach of GDPR requirements. Alternative i) means that the requirement of a fall-back interface persists (in essence contradicting Article 35.2) and alternative ii) means that the ASPSP can choose between breaching either PSR or GDPR. The proposal states (Recital 57) that "[i]t is indispensable that account information and payment initiation service providers be at all times able to access the data indispensable for them to service their clients." It must not be forgotten that the protection of customer information from unauthorised access and the compliance with regulations are some of the main priorities for ASPSPs. To set these against each other is not advisable. Even if the provision of access to account information through the customer-facing interface could be seen as a legal requirement for the ASPSP, through which it can be argued that the legal ground for the processing is established, the requirements on identification of the PSP and protection of any non-payment account data remain.

It should be noted that currently there are numerous entities that access customer data by performing reverse engineering techniques on the ASPSPs' websites and applications. Through these techniques they manage to extract a variety of customer data, even without sufficient legal basis. To ensure the protection and security of consumers, ASPSPs should be able to block this access through reverse engineering and redirect them to dedicated data access interfaces developed in compliance with PSR.

Requirements regarding dedicated data access interfaces (Art 36)
Article 36.1 (c). The requirement that the response times for the dedicated interface cannot be longer than for the ASPSPs' customer-facing interface should be relaxed to take into consideration all relevant circumstances, such as, that AISPs often request bigger data sets in each request than is loaded in the ASPSP's own interface. An ASPSP can opt to only load a smaller data set at a time (in interest of load reduction and faster customer experience). To compare nominal response times could, in light of the above, be misleading and comparable data is not always available.

Article 36.4 (g). The requirement should be that the account holder's identity is verified, rather than the name. In those member states that have centralised registers for personal identity numbers (such as Sweden), the identification by a personal identity number is a more accurate identifier than name and surname. The (indirect) verification of personal identification numbers has already been implemented on the Swedish market through the cooperation in the Swedish API Forum (by showing an error message if the id number provided by the PSU does not correspond to the id number tied to the credentials used to authenticate the order/user).

Data access parity between dedicated access interface and customer interface (Art 37)
We want to stress that a discussion on "how" this should be addressed should be left to the market, and that it should not be specified in the legislation.

Contingency measures for an unavailable dedicated interface (Art 38)
Article 38.1. It can be seriously questioned whether it is proportional that ASPSPs are required to take "all measures in their power to prevent unavailability of the dedicated interface". This is a very extensive requirement that does not appear to take costs or other potential obstacles into consideration. Other regulations that aim at operational continuity and infrastructural security (e.g. DORA and NIS) lack such general and open-ended requirements. Those regulations mention risk-based approach and appropriate systems. The choice of wording in Article 38.1 appears to mean that the PSPs' access to the financial system is more important to the lawmaker than upholding the effective functioning of the financial system itself. In the interest of a level playing field and a non-discriminatory approach to TPPs and the Open Banking/Open Finance ecosystem, the requirement on ASPSPs should reasonably be to take all measures to prevent unavailability of the dedicated interface as they would to prevent unavailability of their customer-facing interface(s). Rather, the wording should be that "ASPSPs should take adequate measures in their power to prevent unavailability of the dedicated interface".

Article 38.3. There is no obligation for a PSP that experiences (or claims to experience) unavailability in the dedicated interface to notify the ASPSP that supplies the interface. Nor is there any obligation to supply any information to the ASPSP about the unavailability and the attempted requests that have been performed (other than what the ASPSP can receive from the supervisory authority through reading the notice there). To re-establish the dedicated interface's functionality, it should be in the interest of all parties that the ASPSP is provided with all available and relevant information (as requested by the ASPSP) and that the unavailability is also reported without undue delay directly to the ASPSP.

Derogation from having a dedicated interface for data access (Art 39)
Article 39. A derogation from the requirement on maintaining a dedicated interface for, e.g., small ASPSPs may be well-meaning but would be hard to align with the requirements on PSP identification and the ASPSP's obligation to have control over the access to information (as further elaborated in the comment to Article 45.2.(a)).

It is welcomed that access to customers' payment accounts by means of third-party service providers will, in future, only be possible via the technical infrastructures and dedicated interfaces (APIs) created by the banking industry and that the requirement for a so-called "fall-back interface" is to be dropped (Article 35(1) PSR). This also increases transparency and security for the consumer. In this context, the orientation towards international industry standards, for example, as developed by Berlin Group, is welcome.

However, the expansion of the offerings to be supported free of charge vis-à-vis third-party services is viewed very critically. This means that legislation once again interferes with the freedom of credit institutions to design their products without any need for this. Free offers reduce the motivation to optimize the

offers of the credit institutions and at the same time hinder their ability to innovate. Under no circumstances should services be required to be provided for retail customers which they do not need or which are not yet offered today and which, in turn, may result in additional risks for customers and banks, such as "multiple beneficiaries" or the requirements for direct debits (Article 36(4) PSR). Last, but not least, such an extension would make the development of and participation in market-based procedures less attractive. This contradicts the declared goals of the legislator.

iii. Section on rights and obligations of account servicing payment services providers

Obligations of account servicing payment service providers regarding account information services (Art 41)
Article 41.2. There is no limitation to the number of requests per time unit that a PSP can send without the active participation of the PSU. (As in Art. 36.5(b) (i) SCA RTS.) This carries the risk of leading to overloading the dedicated interfaces (and possibly backend systems), since an AISP can call the dedicated interface continuously in order to get real-time updates for all PSUs. The scaling of the systems that would be required by the ASPSPs to facilitate this is enormous and not in any way proportional, especially since the ASPSPs don't have any right to charge fees for the provisioning of the dedicated interface. A limitation, as in the present SCA RTS, would be very reasonable. A reasonable and proportionate limitation would be four accesses per day.

Restriction of access to payments accounts by account information service providers and payment initiation service providers (Art 42)
Article 42.1. The clause should be amended with a possibility for ASPSPs to block a PSP from initiating payments or access payment account information in case of serious or repeated abuse of the dedicated interface. (E.g. by holding a session open/active in order to get real-time information about an account and thereby circumvent limitations in the maximum allowed requests without PSU presence, or other similar actions that directly or indirectly disrupt the function or availability of the dedicated interface.)

Data access data management by payment service users (Article 43) and Prohibited obstacles to data access (Art 44)
We want to point out that setting up and filling in the dashboard will be highly time-consuming and the compensation of related efforts and in exchange for access to data (in line with the Data Act and FIDAR) should be possible. Ensuring a fair compensation model will generate incentives for the industry.

Moreover, we ask for clarification on who (the account holder, AISP/PISP or the account-holding credit institution) will be responsible and liable for the correctness of the data, filing/maintenance and deletion. These points should be recorded in the PSR. The extent to which customers (consumers/non-consumers) will make use of this cannot yet be estimated. Furthermore, if the payment service user has multiple payment accounts with multiple ASPSPs, the

overlook and control of the user is reduced by the fact that multiple dashboards must be managed. Instead, the user should be entitled to have a dashboard with the PISP stating all the permits the user has granted the PISP, including the user right to pause, change or delete such promises. This should be the case, since the ASPSP and the PISP do not have any contractual relationship, while the PISP claims that it has a contractual agreement over its services with the user. Therefore, any changes or revocations of permits should be made at the PISP, and not the ASPSP.

Art. 44.2 implies a change to the GDPR, whereby the payment account number and account owner name should not be sensitive data when PISP activities are conducted but would be sensitive data in all other circumstances. This makes it difficult for the ASPSP to protect this data in a sensible way, and also allows the PISP not to provide protection to it.

ASPSPs will be required to facilitate the designation of the purpose of the aggregation of the data (such as if the data will be forwarded to another entity) and that this should be stated in the "dashboard") (Article 42.2. (a)(iii)), which would entail further development of the API and would furthermore be dependent on information obtained from the AISP. This would benefit greatly from a standardisation of the designation of purposes, since the ASPSP and the PSP should "cooperate to make information available to the PSU via the dashboard in real-time" (Art. 43.4), but Article 34.1 expressly prohibits either party (in reality the ASPSP) from requiring a contractual relationship for the provision of the information, thus eliminating any leverage for either party to require conformity to a certain standard unless set forth by the regulator.

Even though there could be benefits with a so-called "dashboard" in the ASPSP interface, in which the PSU can see which consents/permissions that at any given time are active and regarding what data, there could be risks associated with letting the PSU take actions (such as renew or withdraw previously given approvals). Revoking a previously given approval would presumably not have any further contractual consequences in the relationship between PSU and PSP, but the PSU might perceive it to be so. I.e., the dashboard will not function as a way for the PSU to terminate its agreement with the PSP, but only to block further access to the account information from that specific ASPSP (any further functionality than that is likely to require detailed agreements between the ASPSP and the affected PSP). It should be the obligation of the PSP to provide an easy way to withdraw the consent/permission (please compare with GDPR and the regulation of cookies in the ePrivacy legislation). Furthermore, allowing a consumer (the PSU) to periodically renew a permission, or to re-activate a previously withdrawn permission, poses some consumer protection concerns: the PSU would give approval of what must be considered the central part of an AIS (or PIS) agreement, without having access to the actual terms and conditions regulating that service in the same channel/interface. This is in stark contrast to the requirements on prior information in Article 19f.

The obligation for the ASPSP to develop these dashboards, and thereby managing (parts of) the relationship between a PSU and a PSP, and ostensibly

pay for both development and maintenance, cannot be considered proportional, in light of the fact that the ASPSP is prohibited from investigating the PSU permission purported by the PSP. It is disproportionate that the ASPSP should facilitate the PSU's possibility to withdraw the permission without any remuneration. The "strong measure of control over how their personal and non-personal data is used" that the PSUs will achieve through these dashboards should, reasonably, be paid and maintained by the very parties that use the data and also has the only possibility to charge the PSU for the use, i.e. AISPs and PISPs. Especially so, when the ASPSP's obligation in Article 43.4 (a) to provide the PSP with real-time information would require further development of the ASPSP's API/dedicated interface.

Finally, we want to highlight and support the position of the EDPS on the configuration of the permission dashboards, which indicates in its Opinion 39/2023 that "*in a sensitive area such as payment services, consumers may be particularly unaware of the consequences of sharing their personal data with payment service providers. The EDPS therefore recommends that the PSR Proposal, notably Article 43(b), specifies that the dashboard should not be designed in a way that would unduly influence payment service users to grant or withdraw permissions*". In any case, ASPSP should be able to warn customers of potential risks.

iv. Section on rights and obligations of account information service providers and payment initiation service providers

Use of the customer interface by account information service providers and payment initiation service providers (Art 45)
Article 45.2 (a). It is unclear how identification of a PSP is supposed to happen in the customer-facing interface. It is further unclear how an ASPSP is supposed to ascertain (and thereby uphold its obligations under GDPR) that a PSP cannot access other information than it is entitled to. These requirements have been clarified in EDPB's guidelines 06/2020 (on interplay of the Second Payment Services Directive and the GDPR) (Section 6.2, p. 19f). It is critical that an ASPSP has a real possibility to comply with one regulation (PSR) without automatically breaching another (GDPR).

v. Section on implementation

Role of competent authorities (Art 48)
Article 48. We question the proposals, stating that competent authorities' focus should be on ASPSPs compliance to PSR and implying that PISPs and AISPs compliance to PSR is of less significance.

4. Chapter on authorisation of payment transactions

Authorisation (Art 49)

Article 49. Recital 79 suggests that the conditions under which the customer authorised a transaction should be taken into consideration when determining whether a transaction is authorised or unauthorised. However, as is stated in Article 49, a permission shall be expressed in the form agreed between the payer and the relevant PSP. The vast majority of payment transactions are placed electronically, only allowing for PSPs to check whether permission is expressed in the agreed way by the authenticated PSU.

Authorisation of payment transactions, with regards to the preamble section 79: it should be clarified if, and to what extent, the payers' intent or awareness (knowledge) is relevant for constituting an authorised payment transaction, or whether the payer's mere performance of the agreed procedure for giving permission is sufficient. Alternatively, it should be specified whether this could be regulated in the payment service agreement.

Discrepancies between the name and unique identifier of a payee in case of credit transfers (Article 50)
According to paragraph 6, the IBAN/name comparison shall apply to payment orders placed via "electronic payment initiation channels" and to "non-electronic payment orders involving a real-time interaction between the payer and the payment service provider of the payer".

We believe that an extension of the IBAN/name comparison to SEPA payments is to be viewed critically. As, established fraud patterns cannot be stopped by this measure. The PSR largely adopts the provisions already criticised by large parts of the banking sector in the context of proposed Instant Payments Regulation on the verification of account wording and account holder by the receiving bank, whereby the account-holding payment service provider is (always) to be liable in the case of incorrect transfers. It is also unclear how large a deviation from the account wording must be for it to be reported to the originator. The question of how to deal with other alphabets (Greek, Cyrillic) also remains open.

There is also no definition in the PSR of what is to be understood by "electronic payment initiation channels". If, in the opinion of the European Commission, collective deliveries in corporate banking are also included here, we want to stress that this procedure is currently not possible via the customer systems in use, since the technical transmission of the entire payment file only takes place after authorisation of the payment order. In the case of collective deliveries, this IBAN/name comparison should be dispensed with in any case, as otherwise payment transactions for corporate customers are made considerably more difficult.

In addition, it is unclear which types of payment orders should fall under "non-electronic payment orders" and how the IBAN/name comparison should be integrated here.

The IBAN/name comparison should offer the possibility of a cost allocation and also should it be limited to payments in online banking in the retail sector.

Article 50 will have a greater impact on banks and PSPs in the non-euro Member States than the euro Member States. The implementation costs and the changes needed will be more extensive with PSR to banks and PSPs in these states. The banks and PSPs are of varying size and with different systems, and many depend upon older "legacy" systems that are not easily changed. Allowing for the banks and PSPs to recover their costs of implementation by being able to charge will provide a possibility to cover some of the costs. Non-euro Member States should also have longer implementation period than euro states, as we have seen in the proposal for the IPR.

Another important aspect is the fact that not all payees wish to be part of this service, however there is no opt-out for payees. This will have consequences for Swedish PSUs with protected identity and may also affect Swedish ASPSPs' ability to support the system with protected identities for Swedish PSUs.

The interaction with the other proposed anti-fraud regulations should be clarified in law. For example, it would be desirable that discrepancies resulting from reconciliation can be used for data exchange between payment service providers under Article 83 PSR. Likewise, it should be clarified that due diligence obligations for payment service users may arise from the offering of the matching service, which may have an impact on liability rules (in particular Article 59 PSR).

Regulators should allow for flexibility in the technical provision of the CoP service in order to ensure the effectiveness of the service in relation to the intended purpose, while providing a good user experience, and a guarantee that resources are not allocated needlessly. It would be worth considering whether the European Payments Council may be best suited to develop the design of the service, to ensure its homogeneity.

Limits and blocking of the use of the payment instrument (Article 51)
We support the provision laid down in paragraph 4 that allows PSPs to replace blocked payments instruments when it comes to tokenized wallets.

Obligations of the payment service user in relation to payment instruments and personalised security credentials (Art 52)
Article 52 (and Article 60)**.** Keeping PSUs' obligations related only to payment instruments, personalised security credentials and a timely notification in cases of loss of the payment instrument is too narrow in the light of the payment services provided on the market today. The PSUs should be obliged to comply with all obligations as stipulated in the payment services contract.

Obligations of the payment service provider in relation to payment instruments (Article 53)
With regard to point (e), we ask to clarify on how to avoid offline transactions at cards.

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

There is no clear definition of what is considered an authorised payment transaction and in this current proposed article it is not made clear either, making it impossible for PSPs to counterproof a consumers' claim that a payment transaction was not properly executed. Article 55 PSR must refer to "authentication" rather than "authorization" as the "authentication" of a payment transaction is something that PSPs are able to demonstrate. "Authorisation" means the payer's consent to carry out the payment transaction as outlined in the contract, encompassing the customer's expression of will. Typically, this will is expressed through the authentication process.

On the other hand, "authentication" relates to the procedure enabling the PSP to verify the identity of a payment service user.

Whilst PSPs may lack the means to effectively demonstrate whether a payment transaction has been authorised (they may be obliged in the contract to provide evidence for the 'client's will'), they are able to demonstrate whether the payment transaction has been authenticated or not.

Payment service provider's liability for unauthorised payment transactions (Art 56)
Article 56.2. Dispute errands are increasingly complex. It takes a lot of resources to be in line with the existing refund deadline in PSD2. Suggesting a cap of 10 business days, and only where there are reasonable grounds for the payer acting fraudulently, is not realistic as many disputes require analysis of many documents, for example numerous communications with the PSU, communications with the police etc. Taking actions against payment fraud includes being able to process disputes for unauthorised transactions in a qualitative way. The proposed 10 business day cap rule will reduce PSPs' possibility to examine and prevent new fraud patterns, and to properly assess who should bear financial responsibility.

It should also be clarified, if article 60 (1) third subparagraph on the customers full liability gives an exemption from the refund principles in article 56, or if the refund deadline in article 56 are solely procedural rules on refund deadlines, where the bank is required to refund the consumer within 1 day even if the customer could be liable according to article 60 (as is the case in the Norwegian model).

It says in article 60 "by the way of derogation from article 56, the payer may be obliged to bear the losses", however it is unclear if that only applies to the "loss" or if it also includes the deadline rights in article 56.

1) If article 56 gives an exemption to the rights of refund because of intent or gross negligence, the 1-day deadline needs to be extended since it will be unreasonable to expect that the bank can do this assessment in 1 day. Or;
2) If article 56 is to be considered as a procedural rule only, this needs to be clarified.

Also, the question whether the transaction is authorised or unauthorised, should in any case be excluded from any procedural rules.

Payment service provider's liability for impersonation fraud (Article 59)
Consumer protection is not absolute, as the European Court of Justice has recognized several times. In fact, even fundamental rights are not absolute. Payment services cannot be developed as an exception. The Regulation should establish mitigating situations in which the credit institution should not be obliged to make such reimbursement. These mitigating factors may refer to, inter alia, the commission of fraud through channels and means other than those usually used by the institution, the institution's efforts to educate and raise consumer awareness about this type of fraud through accessible and standardized channels, the institution's provision of online mechanisms for verifying communications that the consumer receives, etc. Additionally, full coverage by credit institutions for this type of fraud discourages consumers from being diligent to their own detriment. It could open the door to some first party fraud modus operandi where consumers misuse this situation regardless of whether it has occurred or not, resulting in credit institutions having to proceed with the refund regardless.

In general, we believe that all EU consumer-related law should be consistent. Payment services cannot be grounded on a total lack of consumer accountability, while all other fields of consumer law are based on an average consumer who is reasonably well informed and reasonably observant and circumspect. Gross negligence is a common field in the EU legal systems to regulate this issue and it is applied by the courts to come to reasonable conclusions on fraud accountability. Should further harmonization be deemed necessary around this legal institution to gain unified protection, boundaries can be refined or detailed. Erasing gross negligence from payment services legal framework would entail an unreasonable discrimination to the payment services industry as regards to any other industry (e.g. insurance, household supplies, etc.). Operator impersonation is unfortunately a sort of permanent fraud across the EU applying to household supplies (in Portugal, Poland) or even to the police (France, Germany, Austria). In this consideration, it appears unbalanced that PSPs shall be held accountable for damages sustained by customers, but not other impersonated companies or public bodies.

Therefore, we strongly oppose that credit institutions should be held liable if an account holder is induced by a fraudster posing as an employee of the credit institution concerned to correctly order transactions and transfer funds. The fraudsters use of spoofing mechanism or impersonation as a tool in social engineering should instead be a factor when considering if a customer has been negligent, not a separate rule in this regulation. The envisaged cooperation with corresponding providers of electronic communication services is insufficiently formulated and falls short. Instead, the issue should be addressed comprehensively, as fraud takes place outside the actual payment process and is extremely difficult for banks to detect. Banks do not have the tools to prevent this type of fraud.

When transactions are unauthorised, fraudsters use the customers personalised security credentials and can therefore be detected by the banks by way of geolocation, language settings etc. In instances where the customer is using their own PSCs to authorise a payment, the bank does not have other technical means of detecting the fraud, as the social engineering is happening outside the bank's sphere. It is therefore crucial that all actors in the relevant areas and in the payment chain, such as telecommunication operators, internet platforms and parties involved in user authentication or payment initiation, are included with appropriate legal obligations for fraud prevention, detection and mitigation. Particular attention should be given to the detailed specification of the collaboration of telecommunications operators in these cases of fraud to have effective counter-measures. However, it remains completely unclear how this may be done in practice and it has also been left open by the legislator. The specific obligations of telecommunications companies to cooperate with payment service providers must be defined by law.

We believe that transferring the liability to banks is excessive and inappropriate. PSD2 already contains a balanced liability regime that comprehensively protects the payer in the event of unauthorized payments. There is no possibility for the bank to exert influence if customers are providing credentials despite ongoing information campaigns and against the explicit recommendations of the banks. There is also no possibility of control by the bank to verify the statements of the customer harmed by a fraudster. Extending liability for authorized payments would burden credit institutions with further risks outside their own sphere of responsibility. This is also extremely problematic in view of the envisaged distribution of the burden of proof.

It is unclear how this would effectively prevent fraud: on the contrary, there is a risk that fraudsters will exploit these provisions, and that the related losses - to the detriment of the banking industry and its customers - could increase and also exacerbate other risks, for example in the area of money laundering.

The draft Regulation practically tempts customers to carelessly disclose data, as the bank is supposed to be liable for all damages if the defrauded person states that the fraudster has pretended to be a bank employee. It is important that the fraud has to be reported to the police and the burden of proof for bank staff impersonations should lie with the defrauded. It should not be sufficient that the fraudster "says" it is calling from a bank. It is ESBG's position that this article should be removed to avoid the unfair transfer of liability to banks, however, if the article is to be maintained, the wording of the article should be "Pretending to be an employee of the consumer's PSP by using the email or telephone number". It should in no case be sufficient that the fraudster is saying the name of the bank.

Article 59.2. Phishing fraud can be very complex and time consuming to assess. If PSPs are subject to a refund obligation in terms of authorised transactions, there must be reasonable time frames for PSPs to conduct an investigation of what has occurred. Suggesting a time frame of only 10 business days may lead to PSPs not having sufficient time to accurately assess the errand and PSUs may

choose not to provide detailed information on what has happened. It should also be taken into account that in these cases it is common for the payer PSP to consult the payee PSP for information, which can take time and slows down the process.

Payer's liability for unauthorised payment transactions (Art 60)
Article 60.1 last sentence: Allowing each competent authority to reduce liability on a case to case basis will lead to diverging liability regimes between Member States, unpredictability for both PSPs and PSUs, and potentially an upswing in disputes. To ensure a uniform application of the liability rules, the EU legislator should define the upper liability amount in the case of gross negligence, if any, and ideally also provide guidance, in this article or the preamble, as to how the concepts of intent and (gross) negligence should be understood in the context of breaches of obligations under Article 52.

To the extent that multiple occurrences of being defrauded can amount to gross negligence on the part of the PSU, we find that a greater maximum of losses borne by the PSU would be not only appropriate but a more effective incentive to take reasonable steps to avoid being defrauded. Taking into account the industry's efforts to educate and raise consumer awareness, when the payer is defrauded more than once, the payer could be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 100. To this end, we propose the following text: "*By way of derogation from Article 56, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50 the first time the payer is in this situation and up to EUR 100 from the second., resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument*".

Art 60.2: If the payee or the payment service provider of the payee fails to apply strong customer authentication for any reason whatsoever, the payment service provider of the payee must compensate the payment service provider of the payer. The PSP of the payer is in no position to claim any compensation from the payee.

Art. 60.4: If notification is not available at all times, the losses occurring due to such unavailability period should be carried by the PSP, but no other losses/financial consequences.

Payment transactions where the transaction amount is not known in advance (Art 61)
Article 61.2. The payer's PSP does not have a contractual relationship with the card acquirer or the merchant. Requiring that the payer's PSP can only block amounts that are proportional with the amount of the payment transaction is not reasonable – this should be clarified.

Refunds for payment transactions initiated by or through a payee (Art 62)

Art.62: A provision should be included that the PSP of the payer is entitled to a full financial refund from the PSP of the payee if the payer is executing his refund rights towards the PSP.

5. Chapter on execution of payment transactions

i. Section on payment orders and amounts transferred

No comments received so far.

ii. Section on execution time and value date

No comments received so far.

6. Chapter on data protection

We believe that the exchange of information between PSPs must be stipulated under Article 6(1) c (legal obligation) of the GDPR and ensure the coherence and compliance of said Regulation.

7. Chapter on operational and security risks and authentication

Transaction monitoring mechanisms and fraud data sharing (Article 83) With regard to point (c) in paragraph 1, we understand that preventing transactions is legislatively novel. We believe that PSPs should not be made liable if a fraudulent transaction was not prevented. With regard to paragraph 3, we want to highlight that it offers the possibility to exchange information between PSPs but is limited to the customer identifier. This makes it possible to react in instances of fraud that has already taken place. However, in order to prevent fraud, thus preclude harm to customers and banks, it is necessary to actively oblige TPPs, acquirers, merchants, etc. to exchange extended information on location data, environmental data and behavioural data. Only a networking of the available information enables active protection of the customer. Article 83. An efficient way of communicating potential fraud between payment service providers in line with data protection rules is welcomed. We think it is positive that the possibility of information sharing is clarified in the PSR, but it is important that the provision does not become too detailed or that it is formulated in a way that limits the possibility of information sharing. In this sense, Article 83.3 may become problematic, as it 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 is deleteriously restrictive. If the bank is required to wait for two customers to notify or otherwise get in touch with the bank regarding a request involving the same account in order for information to be shared, it will complicate the work of preventing and counteracting fraud. It may also be the case that the bank itself detects fraudulent transactions and accounts that have been used, such information should be able to be shared immediately. Consequently, we believe this article must not be too detailed that it might restrict or create doubt as to under which circumstances data can be shared. As EBA are to provide technical standards on Article 83, there should be latitude in the regulation for appropriate determination and clarification by the EBA

Another issue concerns the requirements to develop "information sharing arrangements" that will use "dedicated IT platforms". It is unclear what this means in practice, but there is a risk that overly detailed requirements may complicate information sharing.

Article 83 (2) second paragraph states that the PSPs "shall not store data referred to in this paragraph longer than necessary for the purposes set out in paragraph 1, and not after the termination of the customer relationship." It should be clarified that this is without prejudice to any rights or obligations according to AML CTF regulations or under national laws and regulations.

Finally, the meaning of Article 83.6 is unclear, and there is a risk that such a restriction will prevent an effective fight against fraud.

Regarding paragraph 4, it must be considered that, in addition to the multilateral "platform" solution addressed in the proposed rule, bilateral exchanges between payment services providers may also exist. The specifications for data protection impact assessment given in the proposed regulation shall not complicate this and thus only apply to multilateral platform solutions. This needs to be clarified.

In practice, fraudulent payments are often "forwarded" quickly. Therefore, there is a legal provision that payment service providers are allowed to "block" payments received in the event of suspected fraud, in order to be able to counteract this.

Payment fraud risks and trends (Article 84)
The transaction monitoring can, in principle, make an important contribution to combating fraud. Raising awareness of fraud risks is an important tool and is already widely provided by payment service providers.

We believe that it is excessive that payment service providers are required to inform their customers of new fraud scenarios via all appropriate means and

media. It should be up to the PSP to decide how to inform its customers, and no compulsion should exist for public media use.

The Regulation should also establish obligations for Member States to establish awareness measures aimed at consumers.

Outsourcing agreements for the application of strong customer authentication (Art 87)
Article 87. The PSR should not regulate when outsourcing agreements are triggered, as rules on outsourcing are governed by other regulatory frameworks.

Accessibility requirements regarding strong customer authentication (Art 88)
The Accessibility Act already stipulates the necessary requirements that should not be repeated in the PSR.

Regulatory technical standards on authentication, communication and transaction monitoring mechanisms (Art 89)
Article 89. It should be clarified whether the EBA mandate to draft and the Commission's mandate to adopt regulatory technical standards regarding derogations from the requirements on strong customer authentication should also include a mandate to draft, and adopt respectively, mandatory derogations from these requirements. I.e., the aforementioned authorities' mandate should extend beyond adopting legal acts that establish when SCA can be omitted (at the ASPSP's risk), but also to adopt legal acts that establish when SCA is not permitted. This is especially important in light of the ASPSPs' responsibility for unauthorised transactions when SCA is not used (Article 60.2.). If a derogation from the SCA requirement is made mandatory through a delegated act, the risk exposure of the ASPSPs is expanded disproportionately.

Additionally, we see the need that these provisions must also be placed in relation to the other proposals on fraud prevention (in particular the liability rules and associated customer due diligence requirements).

Strong customer authentication
Article 85 (2) in relation to Article 36 (4) and 3 (20): the inclusion of payee-initiated payment order in PIS warrants a need for a wider analysis of the extended scope for PIS as well as the "rules" around payee-initiated payments in general, especially since this would probably be the "new way" for retail payments. We understand that the intention is that one-off payee-initiated is out of scope, which is important because otherwise it would be opened-up to payment orders not accepted by the payer with no means of control for the payer or the payer's ASPSP. We think this should be clarified in the regulations, perhaps Article 36 (4), Article 85 (2) by narrowing down the scope. To protect the payer and ASPSPs of the payer in PIS use case, a mandate must be set up with the ASPSP and there should be no exemption from setting up of a mandate with the ASPSP with ASPSP's SCA in the PIS use case.

We support the aim of the Article 85(12) which introduces the possibility to use two or more elements of the same category to perform strong customer authentication, as long as their independence is fully preserved. However, it should not be possible to use two or more factors from the "knowledge" category as this is the riskiest factor and would not preserve security properly.

Recital 101 seems to introduce the possibility that environmental and behavioural information can be used as a valid factor to perform the SCA. If this is the case, it is important to define in the development regulation what is considered environmental and behavioural information and to what degree of coincidence the factor would be considered valid.

The change of responsibility for SCA towards the AISPs (Article 86(4) PSR) means that the customer can no longer obtain clear rules for SCA from the account-holding institution. The liability issues for this also remain open. Credit institutions should continue to have the possibility to verify the customer's will on a regular basis. Although the future dashboard is a useful addition, it is not seen as sufficient, because it is the customer alone who must take action here. If AISPs conduct their own SCA, the same obligations and requirements regarding SCA procedures as for account-holding institutions must apply to AISs for consumer protection reasons. The procedures must be regularly reviewed by the regulator.

We support the aim of inclusion underlying Article 88 PSR. However, the smartphone has high customer convenience, offers high security and is particularly suitable for meeting the requirements of the Accessibility Directive. Only a small proportion of customers who use online banking do not have a smartphone or do not wish to use one for authentication. If the PSR mandates the provision of alternative methods, i.e. non-smartphone-based, market-based pricing must still be possible.

Differentiation between corporate customers and consumers regarding matters of SCA

The PSD3/PSR follows the path of PSD2 to not make a clear distinction between consumers and non-consumers. The provisions of PSD2 are based on the need for protection and the technical designs in the retail customer sector. From our point of view, an explicit differentiation must be made so that corporate customers can be excluded. In the corporate customer sector, individual or bespoke standard agreements can be made and elaborate technical measures can be taken that would be inappropriate and impractical for retail customers but can meet the needs of corporate customers. In addition to technical measures et cetera, the corporates would want to assume the risk and responsibilities for potential losses, et cetera, in order to achieve the preferred solutions. Responsibility for loss in non-SCA cases should still be up to the PSP and corporate customers to agree (rather than consumers).

In addition, experience with PSD2 shows that it is especially difficult to apply SCA for automated corporate payments and information exchange, including

secure corporate payment protocols. Protocols could for example be based on internet connection, VPN and corporate certificates. Experience with PSD2's terms "online" and "remote" as criteria creates legal uncertainty as to whether or not such systems are exempted from SCA. If no general exemption from SCA for corporates are made, then at least payment and information exchange processes should be exempted where the security is equal to SCA. This should not be reliant on whether "online" or "remote" or not. Preferably in PSR, alternatively in the RTS to be developed by EBA.

8. Chapter on enforcement procedures, competent authorities and penalties

i. Section on complaint procedures

No comments received so far.

ii. Section on dispute resolution procedures and penalties

Administrative sanctions and other administrative measures for specific infringements (Article 97) We believe that the range of penalties now provided for in paragraph 2 (up to 10% of the annual turnover or EUR 5 million) is disproportionate to the severity and the effects of any violations of the Regulations listed in paragraph 1. So far, for example, the Austrian PSD2-transposition law (ZaDiG), provides for penalties of up to EUR 60,000 for such violations. Moreover, history has shown that the regulatory landscape created by PSD2 and the SCA-RTS has led to legal uncertainty, with a high number of opinions, guidelines and Q&As developed over time. Introducing heavy sanctions when it is still difficult to for all market participants to assure compliance due to complex law-making is not appropriate. The wording "a maximum administrative fine of at least …" is contradictory. If the clause is to set a maximum administrative fine, the words "at least" should not be used. Furthermore, it can appear disproportionate with a maximum administrative fine of 10 percent of the global annual turnover (Article 97.2.(a)(i)) in relation to, e.g., the maximum administrative fine under GDPR, where the subject matter may be the mismanagement of particularly sensitive, personal information.

9. Chapter on product intervention powers by the EBA

No comments received so far.

IV. Title on delegated acts

No comments received so far.

V. Title on final provisions

Concerning, the requirements for the planned implementation periods (Article 112 PSR), we believe, that appropriate implementation periods are fundamental. These should be based on the experiences gained from the implementation of PSD2 and should therefore generally be at least 24 months instead of 18 months. Supplementary implementations with comprehensive IT related effects, such as the proposed requirements under Articles 50 and 57 PSR, require an implementation period of at least 36 months in our opinion. These comments relate to the proposed PSR, but if implementation periods will be adjusted in the PSR, we assume that the implementation period of PSD3 article 49 is adjusted accordingly. Likely, the change from a directive to a regulation for many of the articles of PSD2 could require a longer transposition or adoption time in Member States. Moreover, the experiences from the implementation of PSD2 have shown that certainty about the timelines is also necessary, especially for the implementation of so-called "Level 2 regulations", so that banks can plan their implementations accordingly. If corresponding standards or supplementary delegated acts (e. g. RTS) are necessary, the corresponding implementation deadlines must be linked to the publication of the corresponding RTS standards. Divergent implementation deadlines for regulatory areas that involve dependencies with regard to their technical or customer-contractual implementation must be avoided in order to enable efficient implementation for the benefit of the institutions and their customers. This applies, in particular, to the areas of fraud prevention, strong customer authentication and access to payment accounts by third-party services and, above all, to those topics that also require changes to the contractual terms and conditions of the customer relationship.

Annex I – Payment services

No comments received so far.

Annex II – Electronic money services

No comments received so far.

About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 17 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 610,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €6.38 trillion, provide €3.6 trillion in loans to non-banks and serve 163 million Europeans seeking retail banking services.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. October 2023.