Dutch Payments Association

Gustav Mahlerplein 33-35
1082 MS Amsterdam
P.O. Box 83073
1080 AB Amsterdam
The Netherlands

www.betaalvereniging.nl

T +31 (0) 20 305 19 00
F +31 (0) 20 305 19 12

Date
03 October 2023

Telephone
-

Reference
Response DPA PSR Have Your Say

E-mail
n.pranger@betaalvereniging.nl

Subject
Feedback by the Dutch Payments Association on the European Commission's PSR proposal

Dear Sir, Madam,

The Dutch Payments Association welcomes the Commission's proposal for a Payment Services Regulation ('PSR').

In the following pages we will provide you with our response. Hoping to make a meaningful contribution, we wish you all the best with the next steps.

Yours sincerely,
DUTCH PAYMENTS ASSOCIATION

Gijs Boudewijn
General Manager

About the Dutch Payments Association

The Dutch Payments Association[1] (hereinafter: 'DPA') organises collective and non-competitive tasks in the national payment system for its members. Our members are payment services providers who are active on the Dutch market: credit institutions, payment institutions and electronic money institutions. Our responsibilities lie in the areas of infrastructure, standards, and shared product features. We aim for an optimal efficient, secure, reliable, and accessible payment system.
This paper provides our feedback on the PSR and has been drafted together with the Dutch Banking Association, who provided their input to the fraud related articles of PSR. In a separate response we provide feedback to the proposal on PSD3.

The next page shows an executive summary of our feedback, followed by a detailed analysis of the articles including our input and proposals.

[1] https://www.betaalvereniging.nl/en/

Summary

The DPA and its members welcome the European Commission's (hereinafter: 'Commission') proposal for a Regulation on payment services in the internal market (hereinafter: 'PSR'). We have witnessed the Commission's thorough review process of PSD2 and are pleased to see that the Commission has proposed to make targeted amendments.

We support the Commission's proposal for a Regulation instead of a Directive to regulate the payment services and to include Level 2 (e.g., RTS SCA & CSC, EBA guidelines) and Level 3 (EBA Q&A's) provisions into PSR. This will avoid new fragmentation between Member States, remediate some of the current fragmentation and decrease 'license shopping'. Furthermore, we support the merger of PSD and EMD as well as the proposal to allow payment institutions to directly access settlement systems.

Overall, we see that the PSR proposal contains two themes where new requirements in particular have been introduced compared to PSD2: open banking and consumer protection.

Open Banking

We support the proposals from the Commission for (legal) requirements for dedicated interfaces, to abolish the use of fallback mechanisms based on online customer interfaces (including the exemption procedure) and support the use of a "permission dashboard". The latter enhances consumer trust but does need some refinements in the wording of the text to function properly and serve its purpose, while the former ensures the quality of dedicated interfaces. As a Dutch payments community, we strongly believe in high quality APIs ("dedicated interfaces") to exchange data between ASPSPs (banks) and Third Party Providers (TPPs). Because of an increased quality of APIs, TPPs will less often (or not anymore) have to rely on the use of fallback interfaces or even screen scraping.
However, we notice that whereas the Commission is clear in its intention to let the market use dedicated interfaces only (e.g., in its PSD2 Review Report and in the explanatory memorandum enclosed in the proposal), the PSR is ambiguous whether and how precisely a fallback mechanism should still be offered. Moreover, the prohibited practice of access by third parties using screen scraping technologies without identifying themselves vis-à-vis the ASPSP seems to be reintroduced and/or legitimized.

Consumer protection

We appreciate the efforts made by the Commission to combat fraud and protect consumers even further. However, speaking from experience, we believe that reimbursement of 'bank-employee impersonation' scams is not the right approach and should be excluded from the provisions. Instead, to combat fraud effectively, we recommend focusing on *prevention, detection and targeting* criminals. This includes involvement of all parties whose services and systems are abused by criminals to commit online scams – also known as the 'scam chain' - and fraud data sharing. In case of fraud, electronic communication providers are required to cooperate closely with the payment service providers and, moreover, PSR aims to create a foundation for data sharing. We appreciate the proposals by the

Commission for these subjects, but we notice that more is required to combat online scams. We therefore propose the following:

A. Limit reimbursements to unauthorised payments

The inclusion of a compensation obligation for ‘bank-employee impersonation scams‘ in the Regulation does not address the actual problem. In 2020 the Dutch banks decided to compensate damages caused by ‘bank-employee impersonation scam’ out of leniency. Although the reimbursement helps victims financially, it has taken away the responsibility from other actors in the ‘scam chain’ to take responsibility and implement effective measures. Reimbursement does not contribute to reducing fraud. The number of Dutch victims is still very high. Therefore, we recommend that reimbursements remain constrained to *unauthorised payments*.

B. Implement fraud detection throughout the whole scam chain

All parties through the scam chain should perform fraud detection. The effectiveness is, however, limited because criminals do not breach the integrity of the payment system. Instead, victims are manipulated by social engineering into transferring money to accounts held by criminals themselves. The authorisation and authentication are legitimate, and the payment transaction as such can rarely be identified as fraudulent. It is therefore difficult for a bank to detect fraud. Focus should therefore be on the early detection of criminals by parties whose services and systems are also abused by criminals to commit online scams (e.g., electronic communication providers, Big Tech, social media platforms). Implementing fraud detection by those parties helps to detect irregularities within their services and systems. These professional providers are part of the scam chain and should be obliged to have effective fraud detection.

C. Establish a definition for ‘authorisation’ to avoid ambiguity or misinterpretation

Using social engineering techniques, scammers manipulate victims into authorizing transactions. At the moment of the authorisation, the customer *intends* to do the transaction. Only afterwards does the customer realize 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. We suggest defining the term "authorisation" so that it is clear that the PSP does not need to consider what the intent of the PSU was as this is impossible for the PSP to determine. Attempting to do so would cause major disruption within the payment landscape.

D. Enable rapid data sharing and allow banks to offboard criminal clients who abused the bank’s payment services

We welcome legislation that supports data sharing for fraud prevention. In the PSR, data sharing is only possible when at least two different customers have informed the bank about fraud. We recommend for banks to be given the possibility to share information - including data on criminal offences - on the criminals following the first report of fraud. This is already possible in the Netherlands and prevents many scams. Moreover, we recommend allowing PSPs to offboard fraudulent customers after a detailed fraud investigation as this measure restricts criminals from continuing their activities.

Miscellaneous

Next to the two themes open banking and consumer protection, we believe the Commission's PSR proposal requires several amendments and clarifications to be implemented effectively, efficiently and uniformly to reach the goal of further enhancing payments in Europe to the benefit of the European payment service users. As a general comment – similar to PSD2 – several articles mention 'the PSP' without specifying *which* PSP is meant (payee PSP or payer PSP which in turn can be either the ASPSP or the PISP) and the responsibility of this PSP. This resulted in a lot of confusion in PSD2, we therefore would recommend preventing this issue from reoccurring in PSR.

- **Confirmation of Payee (CoP)**

We welcome the proposal for a confirmation of payee (CoP) service to reduce invoice fraud and incorrectly addressed payments. The service is appreciated by PSUs in the Netherlands and thus we support the requirement of real-time client interaction for the execution of CoP. This real-time interaction with the client is important for efficient follow-up in case of a "no match" or "partial match." We recommend extending this requirement of "real-time client interaction" to CoP for electronic payment initiation channels. For bulk payments, regularly processed outside of business hours, additional agreements must be made with corporate clients on how the PSP should act in case of a "no match" or "partial match." Therefore, it would be rightfully out of scope, of such amended provision. It should be left to the competitive space.

Furthermore, we advocate for the removal of the opt-out function for CoP, just as we do so in the discussions on the Instant Payments Regulation proposal. An opt-in/-out function does not serve any purpose where CoP is offered free of charge, resulting in significant implementation costs where such opt-out does not exist in today's customers journeys, as well as confusion and discord with (millions of Dutch) customers. To ensure quality, we also welcome a clear delineation of responsibilities between the chain parties. Furthermore, we found differences between the proposed Instant Payments (IP) Regulation and the PSR in the representation of the verification result, we recommend very precise alignment on this point.

- **Strong Customer Authentication (SCA)**

We would like to emphasize that the smartphone has become an indispensable tool in promoting the accessibility to and usability of banking services. For accessibility, smartphones offer multiple functions such as contrast options, dark mode, zoom functions and more. The smartphone is the preferred option for many users that depend on these accessibility functions. From the viewpoint of usability, smartphones provide better security and authentication than most other devices. According to the proposal the specific situation of all customers should be catered for. The chosen wording may suggest that tailormade individual solutions are required but with a large and heterogeneous group of people with (temporary) disabilities. This is unfortunately not feasible and seems also to be in contradiction with or stricter than the requirements of the European Accessibility Act (hereinafter: '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 relying on the EAA in this context.

Limits and blocking of the use of the payment instrument

We strongly recommend ensuring that PSPs can amend the spending limit unilaterally (for instance in circumstances like COVID-19, inflation, or in relation to security threats) with the option for the customer to determine his own limit within. Agreeing to increase a standard limit with each customer separately is not workable and creates a tangle of standard limits that applied at a certain time when somebody became a customer.

Relation with the digital euro

We noticed a proposed change in the definition of “Funds” as to cater for the arrival of a Digital Euro. Given the current state of the development of a Digital Euro, where numerous choices have yet to be made, this change is in our view premature, prone to unclarity and insufficient to properly govern digital euro transactions. Amendments to the PSR should be considered by the time the desired functioning of a Digital Euro has been established. The definition of ‘Funds’ should therefore be kept to the current definition under PSD2.

What follows on the next pages are detailed comments on the specific articles and sub-articles proposed by the Commission, divided per section. The related articles are written in **blue**, the sub-articles ***in bold and italic***, and comments are written in standard style.

Recitals

Recital (69): ***[…] Where the term 'explicit consent' was used in Directive (EU) 2015/2366, the term 'permission' should be used in the present Regulation. […]***

The introduction of the term "permission" is intended to avoid the current discussions around "explicit consent", as described in recital (69). However, after several years of dealing with this issue, the market understands what "explicit consent" under PSD2 entails. The proposal by the Commission to introduce the term "permission" results in more confusion, exactly the opposite of its intended goal. The added term "permission" is understandable, but it poses questions as to how it should be understood or what it exactly entails. Clarification and confirmation of its contractual nature as opposed to the term explicit consent in the GDPR would help the market.

Recital (97): *Provision of payment services by the payment services providers may entail the processing of personal data […]*

In this recital it would be useful to refer to the grounds on which personal data can be processed. In practice, concerns arise as to whether the ground is legal obligation, contract between data user and PSP or legitimate interest. The ground for the processing of "silent party data" should be referred to. It can be either "necessary to abide by a legal obligation to which the data controller -the ASPSP/PSP- is bound or "legitimate interest" of the PSP to be able to provide the services to the user. Silent parties may also be a data subject as defined in the GDPR. Data subjects have in general a right to object. It would be convenient to explicitly refer to the fact that such a party cannot object to the disclosure of his or her data, since this would jeopardise the purpose of the PSR. Reference is made to the principle of data minimisation. The DPA did have questions as to whether PSD2 had sufficiently considered the data minimisation principle. It would be useful to include in the recitals that it is up to the parties involved in the payment services chain and to the extent that they are data controllers how they can achieve the goal that only those personal data that are strictly necessary are processed.

Recital 102: ***[…] A typical use of payment services that could indicate a potentially fraudulent transaction […]" and […] prohibition to use data processed for fraud monitoring purposes after the payment services user has ceased to be customer of the PSP […]***

'Detecting atypical use' will require "profiling". It would be useful to indicate this in the recital and add safeguards to consider the privacy of clients in such a way that detection and investigation is not jeopardized. The restriction of not being able to use the data as referred to in this recital can pose problems. Such data could still be used to train fraud detection algorithms. It is necessary that this exception is included.

Articles

Article 2 – Scope

Art. 2(2)(b): ***This Regulation does not apply to the following services: (b) payment transactions from the payer to the payee through a commercial agent, as defined in Article 1(2) of Directive 86/653/EEC, provided that all of following conditions are met: i) the commercial agent is authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee, but not both of them, irrespective of whether or not the commercial agent is in the possession of the client's funds, and ii) such agreement gives the payer or the payee a real margin to negotiate with the commercial agent or conclude the sale or purchase of goods or services;***

We would like to receive more clarity on the 'commercial agent' exemption, more specifically which platforms are and are not in scope of the commercial agent exemption.
Under PSD2, the commercial agent exemption has been interpreted differently by different Member States which led to unnecessary fragmentation in the market. This fragmentation remains in PSR, as the Regulation refers to Directive 86/653/EEC for the definition of a commercial agent. This Directive is implemented in national laws and interpreted differently among Member States. Some Member States have a very strict interpretation of the commercial agent exemption, while others interpret it more broadly.

As a result, this could lead to forum shopping whereby platforms choose to operate in a specific Member State that applies a broad exemption-regime. This results in an unlevel playing field; platforms could offer payment services in a country with a broad interpretation of the exemption, while for platforms active in other countries this would not be possible. This is an unfair advantage and potentially a risk for customers and merchants active on that platform.

Art. 2(2)(j)(i) & (ii):
This Regulation does not apply to the following services:

(i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a single limited network of service providers under direct commercial agreement with a professional issuer;
(ii) instruments which can be used only to acquire a very limited range of goods or services;

We would like to receive more clarification on this exemption. Considering the above-mentioned article as well as recitals 12 and 13, it is still not clear when a party should be deemed to fall under this exclusion. Take for example a card which can be used to purchase fuel as well as all other items in a petrol shop, making this a wide range of goods and services but still from one issuer, the fuel company. This company has shops all over Europe, so geographically they are not confined to one place. Would the exemption apply in this example or not?

Article 3 - Definitions

We welcome the proposals to define both (i) initiation of a payment transaction and (ii) execution of a payment transaction (art. 3(6) and (8), the definitions however require more clarification.

Art. 30(6): Initiation of a payment transaction: ***means the steps necessary to prepare the execution of a payment transaction, including the placement of a payment order and the completion of the authentication process.***
The difference between "initiation" and "placement of a payment order" (included in the definition) is unclear. We would welcome a definition for "placement of a payment order".

Art. 30(8): Execution of a payment transaction: ***means the process starting once the initiation of a payment transaction is completed and ending once the funds placed, withdrawn, or transferred are available to the payee.***
This definition concerns the phase after the initiation of a transaction has been completed. In the current definition, the execution phase ends with the transaction amount being credited to the beneficiary's account. The payer's bank has no influence on this last part of the execution, as this is performed by the beneficiary's bank (after receiving the funds from the payer's bank).
The current definition could cause problems in relation to the liability of the payer's bank:

- **Art. 40(b)**: *immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider*.
    - Given the definition of "execution of a payment transaction", should the bank of the payer inform the PISP whether the transaction arrived at the payee's payment account? We recommend to amend this to:
      "*immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider ~~regarding the execution of the payment transaction~~ to the payment initiation service provider*."
- **Art. 75(1)**: *"[…] unless it can prove to the payer and, where relevant, to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction in accordance with Article 69(1). In that case, the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction. […]"*
    - From the current definition it seems that the payer's PSP is still liable to the payer, this has not been clarified in this article. We would recommend removing "to the payee".

We recommend adding a definition of “authorisation”, to avoid ambiguity or misinterpretation. This is more extensively explained in our response to art. 55(1). Under PSD2 it means that in the absence of consent, a payment transaction shall be considered to be unauthorised. We propose the following: *“authorisation means the expression of the consent for the execution of a payment transaction given by a payer to his payment service provider, through the process and in the form agreed between the payer and his payment service provider.”*

Art. 3(30): *Funds means banknotes and coins, digital euro when established by EU regulation, [digital forms of Member States official currencies available to natural and legal persons], scriptural money and electronic money;*

The Commission has introduced the Digital Euro (‘D€’) into PSR by amending the definition of ‘Funds’. Through this amendment, payment transactions in D€ are governed integrally by PSR. However, transactions involving D€ cannot be treated integrally the same as regular ‘commercial’ euro transactions as they involve the ECB in many capacities, including that of PSP. Upon legal adoption of the D€, the ECB shall be responsible for its design and the technical infrastructure. There is currently no clarity on these matters. Neither on the operation of the European Identity Wallet for authentication, which means a fundamental change to authentication as currently known under PSD2. What is clear, is that banks will neither have control over such infrastructure nor of the use of the European identity wallet to facilitate payment transaction involving the D€. Furthermore, the insertion of ‘issued for retail use’ in the definition of ‘Funds’ raises too many questions.

Before applying PSR to any EU digital central bank money, the legal framework of such digital currency must be finalized, and the technical set-up and infrastructure must be final to accurately assess and regulatory allocate obligations and liabilities. At that time, PSR should be amended to properly define to what D€ payment transactions it applies from a segment perspective. It is a fundamental change to shift from the PSD/PSD2 design principle ‘applying to all payment transactions’, to applying to all payment transactions for ‘retail use’ because of any future introduction of the D€; and clearly allocate liability to the ECB and central banks as PSP in relation to D€ transactions, especially in relation to liability for defective and unauthorised transactions as the commercial banks are not the PSP for these transactions.

The current introduction of the D€ in PSR is too premature, it will create a lot of legal uncertainty and it should be avoided that commercial banks will have unnecessary debate with their supervisory authorities. That is not in the interest of any party in the ecosystem and could even hamper the uptake of the D€. We recommend excluding digital central bank money from the definition of ‘Funds’.

Chapter 3 - Framework contracts

Article 20 - Information and conditions

Art. 20(c)(v): ***The payment service provider shall provide the following information and conditions to the payment service user:***

(c) on charges, interest and exchanges:

(v) where applicable, the estimated charges for currency conversion services in relation to a credit transfer expressed as a percentage mark-up over the latest available applicable foreign exchange reference rate issued by the relevant central bank;

We strongly believe that PSPs should not be limited to one single source and should be able to continue using other reliable sources available in the market, such as Reuters or Bloomberg. Moreover, so as such sources are fully independent and publish real-time FX rates whereas the ECB only publishes FX rates daily, which could have a significant negative impact on customers in case of high-value transactions. Several customer groups demand and have grown accustomed to real-time FX rates to mitigate currency risk.

Art. 20(e): ***The payment service provider shall provide the following information and conditions to the payment service user: (e) on safeguards and corrective measures:***

(v) how and within what period of time the payment service user is to notify the payment service provider, and the police in case of impersonation fraud referred to in Article 59, of any unauthorised or incorrectly initiated or executed payment transaction or of any authorised credit transfer made following an incorrect application of the name and unique identifier matching verification service or impersonation fraud, in accordance with Article 54;

Art.20(e)(v) mentions *"impersonation fraud"*, this should be clarified by using *"bank-employee-impersonation fraud"*.

(vi) the payment service provider's liability for unauthorised payment transactions in accordance with Article 56, for the incorrect application of the name and unique identifier matching verification service in accordance with Article 57, and for impersonation fraud in accordance with Article 59;

Article 23 – Termination

We would like to raise concerns on Article 23, relating to termination of the framework contract. There is lack of detail on the application of the proposals. Article 23 outlines that where payment services are offered jointly with technical services, such technical services should be subject to requirements on termination fees (i.e., no termination fees can be charged for cancellation of the contract by the PSU after 6 months).

It is unclear, pursuant to the commentary in Recital 49, as to whether such technical services would also be subject to the requirements on the termination notice period i.e., PSU can terminate terminal hire contract upon 1 months' notice. Equally, whilst no termination fees can be applied after 6 months, it is unclear whether PSPs would still be able to bill PSUs for the remaining period of their terminal hire contract, should the PSU terminate it before the end of the contract term. For example,

if a PSU has a 12-month contract for technical services with a PSU and cancels at 6 months, is the PSP permitted to charge the PSU for the remaining 6 months for which they were contracted? We would welcome clarity from the Commission on these points.

Whilst we understand that the proposals aim to give PSUs greater mobility and choice, and thereby increase competition amongst PSPs in the market, it is unclear whether the Commission has conducted an impact assessment (there is no reference to its Impact Assessment Report) or considered the potential unintended consequences. For example, the proposals may have the potential to reduce competition and choice for merchants, as PSPs who cannot viably implement such provisions may exit the market or may disincentive acquirers from offering terminals. Equally, the proposals may lead to PSPs being incentivised to levy additional charges to PSUs to recover costs borne by these proposals. This could have knock-on commercial impacts on merchants. We would welcome clarity from the Commission as to whether these potential unintended consequences have been considered.

Article 27 - Scope

Art. 27(1): ***Where the payment service user is not a consumer, the payment service user and the payment service provider may agree that Article 28(1), Article 49(7), and Articles 55, 60, 62, 63, 66, 75 and 76 do not apply in whole or in part. The payment service user and the payment service provider may also agree on time limits that are different from those laid down in Article 54***

Clients with international trade rely heavily on the ability to make payments that guarantee that the full amount reaches the beneficiary. This is only possible if you have the OUR cost option at your disposal. Then correspondent banks are not allowed to deduct any costs. Starting with PSD2 and continued in the PSR-proposal, payments in non-EEA currencies are in the scope of the PSR (e.g., USD from NL to DE). These payments must be sent with the SHA cost option, which means that it is not always possible for the full amount to reach the beneficiary. Intermediary financial institutions that are not bound by PSD2 will deduct costs from the principal. For example, a dollar payment always goes through a correspondent in the United States, and they are not bound by the PSR. They will withhold an amount from the principal when processing a payment with the SHA cost option. As a result, customers run into problems, such as an important cargo that remains at customs because the full amount of tax has not been paid.

Therefore, we suggest allowing PSPs to be able to agree with their business customers to not apply article 28(2) and add article 28(2) to the other articles mentioned in this art. 27(1).

Chapter 3 - Account information services and payment initiation services

Article 35 - Provision of dedicated access interfaces

***Art. 35(5)*: Account servicing payment service providers shall publish on their website quarterly statistics on the availability and performance of their dedicated interface. The performance of […], and by the number and transaction volume of the successful payment initiation requests over the total number and transaction volume of the total number of payment initiation requests.**

We kindly refer to the currently available statistics on availability and performance of dedicated interfaces, which are the average response times and error rates of the interface. These are mentioned in the EBA Guidelines on the conditions to benefit from an exemption from the contingency mechanism under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC), Guidelines 2.2, 2.3 and 2.4. Experience from the Dutch market provides evidence that the current EBA Guidelines on the availability and performance of dedicated interfaces are sufficient and reach their goal. These guidelines only refer to "request" and not "payment transaction volume." We strongly recommend sticking to the EBA guidelines on AIS- and PIS-API requests and not add payment transaction volume to the availability and performance statistics. Moreover, statistics on payment transaction volume is information in the competitive/commercial space and therefore ASPSPs should not be required to share this.

Instead, we propose to uniformly enforce the EBA requirements throughout the Member States, as National Competent Authorities ('NCA')s in some Member States do not strictly enforce these requirements. Stricter enforcement of these requirements is necessary.

Article 36 - Requirements regarding dedicated data access interfaces

We support having strict requirements for dedicated interfaces to ensure their quality as this will result in TPPs having to rely less (or preferably not anymore) on using fallback interfaces or screen scraping. It would also be helpful if ASPSPs were provided with guidelines on how they should ensure the API connections are created fast and frictionless.

Art. 36(4)(g): *Account servicing payment service providers shall ensure that the dedicated interface allows payment initiation service providers, at a minimum, to: (g) verify the name of the account holder before the payment is initiated and regardless of whether the name of the account holder is available via the direct interface.*

Art. 36(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 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

processed solely based on the unique identifier of the payment account. Additional information (such as described in these sub-articles) is not needed. We do however understand the need for the above-mentioned account data for automated refunding purposes by the payee. But then this account data is only necessary after the execution of the payment and not prior to the initiation of a payment

Moreover, the ASPSP is not able to comply with the requirements laid down in art. 36(2)(d) and 36(4)(g) for one-off direct 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 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 conversion rates of TPPs.
Moreover, it is unclear what purpose additional payment account data serves to a PIS-only PISP that 'only' initiates a payment. As explained, this data is not necessary to execute a payment transaction.

ASPSP should be able to provide additional payment account data (by means of 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 where after SCA the payment is directly executed by the ASPSP.

Art. 36(4): ***Account servicing payment service providers shall ensure that the dedicated interface allows payment initiation service providers, at a minimum, to:***

Article 36(4) requires ASPSPs to ensure that the dedicated interface allows PISPs to initiate several types of transactions, such as direct debit, single payments, and future dated payments. This way prescribed however, violates in our view the data parity principle – mentioned in art. 37 and recital 59 – that requires ASPSPs to provide TPPs access to the same payment account data that is 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.

Paragraph 4 sets details on what payment initiation functionalities the dedicated interface should offer to PISPs. We have remarks on requirements (a), (d) and (g):

(a) place and revoke a standing payment order or a direct debit

We would recommend leaving direct debit out of scope for PIS. Collecting services that entail commercial/credit risk can only be provided by the party that will incur such credit risk and the loss if the risk materializes. In case of direct debit it is the creditor PSP that will decide whether it will offer the product to the payee or not and if so, on which conditions. Recent insolvency cases have demonstrated that such losses of the payee bank pile up due to debtors massively invoking their direct debit refund rights (irrelevant of it being justified). PISP are not in the money flow, so they will not be subject to any such risk and losses. Consequently, products to be offered by PISPs shall

mainly consist of credit transfers or any other product without any commercial (refund/chargeback/recall).

Bringing this in scope would lead to serious issues at ASPSPs. Moreover – from a parity point of view – some retail ASPSPs do not offer a revoking functionality of initiated & signed direct debit batches in their current business customer online interface. Revocation is exceptional and only in rare cases (manually) processed. From data parity point of view and proportionality it should not be required to revoke a direct debit batch via a dedicated interface if this functionality is not available in the direct online customer interface. Also, it must be understood that e.g., the setting up of a SEPA Direct Debit ('SDD') mandate does not always involve the debtor bank. This is only the case when an e-Mandate is set up. Paper based SDD mandates are lodged with the Payee.

(d) initiate payments to multiple beneficiaries

We would like to have more clarity on what this service exactly entails. Does this refer to 'signing a basket of multiple payments to different payees' where each individual payment results in a debit on the payment account?

(g) verify the name of the account holder before the payment is initiated and regardless of whether the name of the account holder is available via the direct interface;

Providing any payer details before the payer is involved in the transaction at ASPSP side is unacceptable from a GDPR perspective. Please note that in case of card transactions the collecting PSP will also not receive any such details upfront. There is no valid reason why a PISP should be in a different position.

Art. 36(5)(a): ***Account servicing payment service providers shall ensure that the dedicated interface provides to payment initiation service providers: (a) the immediate confirmation, upon request, in a simple 'yes' or 'no' format, of whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer.***

We recommend removing this sub-article from the proposal. It has been confirmed by participants active in the Dutch market that Confirmation of Availability of Funds is not required for payment initiation service providers. ASPSPs however would need to implement this service in the PIS-flow (instead of offering it as a standalone service, as in PSD2 art. 65) which would result in significant implementation costs for both ASPSPs and PISPs and without clear demand for the feature.

Art. 36(5)(b): ***ASPSPs shall ensure that the dedicated interface provides to payment initiation service providers:***

(a) the immediate confirmation, upon request, in a simple 'yes' or 'no' format, whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer;

While the requirement for ASPSPs to offer the service of confirmation on the availability of funds (CAF) (art. 65 PSD2) has been removed, it seems that this service now has been incorporated into art. 36(5)(b). We recommend removing this functionality. The available funds should be visible for the

PSU, who determines to initiate the transaction. The availability of funds however is not needed for the PISP.

(b) the confirmation from the account servicing payment service provider that the payment will be executed the information available to the account servicing payment service provider, any pre-existing payment orders that might affect the full execution of the payment order being placed.

We assume that from a parity point of view this information is the same as in the direct online customer payment interface of an ASPSP and in case of a CAF request of a PISP funds reservations is not required by an ASPSP. This clause seems to suggest that an ASPSP may give a guarantee to the PISP, which is *not* the case. The PSU shall have the ultimate say in which payment it may want to perform, such guarantee may give a wrong perception to the PISP. Furthermore, bankruptcy laws may prevent an ASPSP to execute a payment order to which an ASPSP may have given a confirmation before having knowledge of a bankruptcy. A PISP can only have clarity on the status of a payment through the payment having received the status 'final'. Any confirmation the PISP gives to its client (being the PSU or a merchant) shall be for the account of the PISP.

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

Art. 37(1): ***Without prejudice to Article 36, account servicing payment service providers shall ensure that their dedicated interface referred to in Article 35(1) offers at all times at least the same level of availability and performance, including technical and IT support, as the interfaces that account servicing payment service providers make available to the payment service user for directly accessing its payment account online.***

We understand what the Commission would like to achieve with article 37. However, we would suggest starting to treat the dedicated open banking interface as a fully-fledged and mature interface with its own specificities, instead of continuously comparing the interface to the customer interface. The two interfaces are different, which the following example also shows. In certain circumstances, if the direct online customer interface is unavailable, AISPs/PISPs can still execute their account information and payment initiation requests via the dedicated interface.

Art. 37(2): ***Account servicing payment service providers shall provide account information services providers with at least the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data.***

This provision seems to have been copied directly from the RTS SCA & CSC, art. 36(1)(a). We have come to understand that in the interpretation of the European Banking Authority, who have provided the sector guidance on this issue, this obligation cannot result in dedicated interfaces that effectively were to provide AISPs with less information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information. We would most welcome a confirmation of such interpretation.

Art. 37(3): ***Account servicing payment service providers shall provide payment initiation service providers with at least the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the payment service user. That information shall be***

provided immediately after receipt of the payment order and on an ongoing basis until the payment is final.

Article 37(3) as well as art. 36(4)(f) and art. (40)(b) state that ASPSPs must immediately after receipt of the payment order from a PISP, provide or make available all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction to the PISP. As clarified in article 40, where some or all the information is unavailable immediately after receipt of the payment order, the information shall be sent to the PISP when it becomes available. It is unclear how 'immediately' should be interpreted and how ASPSPs should send this information to PISPs. It is unclear how to comply with this requirement when the ASPSP's dedicated interface is temporarily unavailable. We would like to point out that push notifications for this type of service is not (by default) supported in the direct customer online interface of an ASPSP.

In our view, the PISP should be able to do a payment status call at an ASPSP to retrieve the (final) payment status. However, payment push notifications from the ASPSP to a PISP are a value-added services (premium) service and ASPSPs should be able to receive compensation from PISPs for this service. This premium service should be made available to the TPP via a bilateral contractual agreement or multilateral contractual arrangement (e.g., a scheme).

Article 38 - Contingency measures for an unavailable dedicated interface

As a general comment, every contingency measure should focus on a solution that is available immediately. TPPs rely on the dedicated interface. In case a proper alternative is not immediately available in case of unavailability, TPPs are unable to provide their services.

Art. 38 (2): ***[…] During the period of unavailability, account servicing payment service providers shall offer to account information and payment initiation service providers without delay 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, to access payment account data.***

We strongly support the removal of the obligation to permanently maintain a fallback interface, as mentioned in art. 35(2). However, we notice that whereas the Commission is clear in its intention to let the market use dedicated interfaces only (PSD2 Review Report, COM (2023) 365/2, section 3.1), the PSR is rather ambiguous in art. 38, whether and how precisely a fallback mechanism should be offered. Art. 38 may be read as if a permanent fallback must still be offered, and/or 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)). We therefore would like to receive more clarification here. It is worth mentioning that in practice unavailability of the dedicated interface for most (Dutch) ASPSPs almost always means that the direct customer interface is also unavailable. Even more, in certain circumstances AISPs/PISPs can still do account information & payment initiation requests via the dedicated interface once a customer/PSU has given his permission/mandate, if the direct online customer interface is unavailable. From this point of view, it is disproportionate to have a fallback interface in place.

Art. 38(6): ***In cases where account servicing payment service providers are obliged to allow account information service providers or payment initiation service providers to access the***

interface that account servicing payment service providers use for authentication and communication with their users, account servicing payment service providers shall immediately make available any technical specifications needed by account information service providers or payment initiation service providers to adequately connect to the interface that the account servicing payment service provider uses for authentication and communication with its users.

The entire process which must be followed when the dedicated interface of an ASPSP is unavailable seems very cumbersome especially in the case when an ASPSP provides technical specifications to a TPP to connect to the interface only after the dedicated interface is down. It requires the TPPs time and resources to implement these specifications and hence downtime of their services (to customers of that ASPSP). Under these circumstances it would be more effective to share the technical specification beforehand to TPPs to integrate. However, we are in favour of robust dedicated interfaces without any fallback mechanisms based on the (ordinary) online customer interfaces as seems to be suggested in this provision.

Article 41 - Obligations of account servicing payment service providers regarding account information services

Art. 41(2): ***Account servicing payment service providers shall allow account information service providers to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service whether or not the payment service user is actively requesting such information.***

The RTS on SCA and CSC limited the number of times an AISP could retrieve account information when the PSU is not active to four. Art. 41(2) removes this limitation. Removal of this limitation will result in a significant increase in API calls, which could overload the ASPSP's infrastructure. We therefore suggest obliging AISPs (particularly license-as-a-service providers) to implement account rate limiting plans, to limit the API calls. This is to the benefit of ASPSPs as well as AISPs and would ensure business continuity. ASPSPs should receive the right to implement a similar plan to specific AISPs overloading the infrastructure and give this AISP reasonable time to take measures when continuity is at stake. In the meantime, ASPSPs may block or limit the API calls of the applicable AISP involved for the sake of all other AISPs and their users.

Article 43 - Data access management by payment service users

The proposal in art. 43 for a "permission dashboard" to provide PSUs with an overview is generally welcomed by the Dutch payments community but it needs some amendments in wording to serve its purpose and function properly. We think the executability of the article increases if the PSR would indicate or define (for example in art. 3) what is to be considered "ongoing permission" in this respect. The RTS on SCA and CSC suggests cases "where the PSU is not actively requesting" access or granting permissions.

Art. 43(1): ***The account servicing payment service provider shall provide the payment service user with a dashboard, integrated into its user interface, to monitor and manage the permissions the payment service user has given for the purpose of account information services or payment initiation services covering multiple or recurrent payments.***

It is well established from PSD2 that PSUs have the right to make use of the services of TPPs whereas the PSUs consent to the retrieval of account information by an AISP from a payment account held at and serviced by an ASPSP. The same logic applies to PISPs. In other words, a consent, or now: "permission", is supposed to have been granted by a PSU to a TPP. 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 insight in 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 authorised access the payment service user has given for the purpose of account information services or payment initiation services covering multiple or recurrent payments."*

Art. 43(2)(a)(iii): ***The dashboard shall provide the payment service user with an overview of each ongoing permission given for the purposes of account information services or payment initiation services, including:***

(iii) the purpose of the permission.

We strongly advocate to remove from art. 43(2)(a) sub (iii) "purpose of the permission". It is unclear whether purpose refers to the PSU (i.e., purpose of permission provided) or the service offered by the TPP (i.e., purpose of the service). In both cases, it is not for the ASPSP to know and the ASPSP should not be involved.

In our opinion, when an AISP is directly offering a service to the end-user (PSU), the purpose of the service is clear and there is no need to explicitly mention the purpose of the permission in a dashboard. In this case, the name of the AISP (part of the dashboard as described in art. 43(2)(a)(i)) is sufficient.

In the case a third party without a license uses an aggregator (a business model also known as license as a service) to access a customer's data, it is desirable to include the name of the unlicensed party who is using the customer's data. Only mentioning the name of the aggregator is mildly informative (if at all) to the PSU but surely not transparent.

(v) the categories of data being shared.

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 article were to be deleted.

Art. 43(2)(c): ***The dashboard shall allow the payment service user to re-establish any data access withdrawn***

We assume that this re-establishment may be performed in the same way as how the initial permission was established, i.e., via the AISP or PISP, since these TPPs have no access to the dashboard and would be unaware of changes Practice from the Dutch market shows this is perfectly feasible and with good customer journeys outside a dashboard. 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): ***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.***

This functionality is in our view and experience not necessary. There is no demand from TPPs to receive real-time updates on changes made to permissions and importantly the TPP will find out a permission has been withdrawn as soon as an API-call does not go through. We therefore suggest removing this article.

Article 44 - Prohibited obstacles to data access

Art. 44(1): ***Account servicing payment service providers shall ensure that their dedicated interface does not create obstacles to the provision of payment initiation and account information services. Prohibited articles shall include the following:***

Art. 44(1)(a): ***preventing the use by payment initiation services providers or account information services providers of the credentials issued by account servicing payment service providers to their payment services users***

If for the proper functioning of the API it is not necessary to share the credentials, then these should not be shared with a TPP. Such provision is related to screen-scraping without proper identification by the TPP, of which we would disapprove. Explained in recital (61) this is not allowed and we therefore suggest removing this obstacle. Art. 44(1)(a) therefore cannot be regarded as an obstacle and should be removed from the list.

Art. 44(1)(h): ***requiring that strong customer authentication is applied more times in comparison with the strong customer authentication as required by the account servicing payment service provider when the payment service user is directly accessing their payment account or initiating a payment with the account servicing payment services provider***

In addition to this obstacle, we would like to add that ASPSPs should also not enforce SCA in a PISP flow in a different manner than such ASPSP requires from its own PSU. The type of SCA applied in a PISP flow should not be a more burdensome form of SCA. Similar to what is mentioned in (j), but not quite.

Moreover, certain banks impose a higher level of SCA than other banks. For example, some banks require consumers to authenticate via a scanner, while consumers do not always carry a scanner with them. Consequently, the payment initiation transaction is impossible for the consumer to execute. We propose to also have parity when it comes to strong customer authentication methods.

Art. 44(1)(k): ***imposing that the user be automatically redirected, at the stage of authentication, to the account servicing payment service provider's web page address when this is the sole method of carrying out the authentication of the payment services user that is supported by an account servicing payment service provider***

We understand this as follows, if an ASPSP is offering a mobile banking app as an SCA token to her customers (PSU), the ASPSP should also be able to offer:

- app-to-app redirection; and
- web-to-app redirection (possibly with mobile banking app as pure SCA token and subsequent completion of redirect via web).

Importantly, we do expect this to be technologically neutral, in the sense that instead of so-called native mobile banking app redirect screens a PSP may also offer 'angular' redirect screens in the mobile banking app. After all, it is all about an optimal customer journey.

Art. 44(2): ***For the activities of payment initiation services and account information services the name and the account number of the account owner shall not constitute sensitive payment data.***

We would like to propose an amendment for art. 44(2), as its current wording is unclear, open to interpretation and not fully consistent with recital (67) of PSR and the definition of sensitive payment data in PSD2. Recital (67) mentions: *"[…] it is appropriate to specify that, for the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data."* We therefore propose the following amendment:

"For the activities of payment initiation services and account information services the name and the account number of the account owner shall not be regarded as ~~constitute~~ sensitive payment data."

Chapter 4 Authorisation of payment transactions

Article 45 - Use of the customer interface by account information service providers and payment initiation service providers

Art. 45(2)(d): ***Where an account information service provider or a payment initiation service provider accesses payment account data via an interface that the account servicing payment service provider makes […], the account information service provider or the payment initiation service provider shall at all times: (d) log the data that are accessed through the interface operated by the account servicing payment service provider for its payment service users, and provide, upon request and without undue delay, the log files to the competent authority. Logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.***

For the purpose of point (d), logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.

We would like to receive clarification whether these logs would include personal data. If so, then a retention period of 3 years is not long enough. In the Netherlands, transaction data is usually stored for a period of 7 years from the date of transaction (art. 52 Wet Rijksbelastingen/Dutch General Tax Act), therefore these cannot be deleted before such a time.

Article 46 - Specific obligations of payment initiation service providers

Art. 46(1)(b): ***Payment initiation service providers shall: (b) provide services only where based on the payment service user's permission, in accordance with Article 49.***

We suggest keeping the term 'consent' as used in PSD2 and refrain from using the term 'permission'. There is no GDPR interplay in relation to this clause.

In relation to our comment on article 4(1), we would also like to receive clarification on the definition of PSU in this context, more specifically clarification needs to be given who the PSU is in relation to who. For the PSP it would be the payee, while for the PISP it would be the payer, based on how art. 46 is drafted.

Art. 46(2)(a): ***Payment initiation service providers shall not: (a) store sensitive payment data of the payment service user***

The definition of sensitive payment data is very broad and provides an open-ended obligation to not store any data. As both the name and account number are excluded from sensitive payment data, we would like to receive clarification what would be deemed as sensitive payment data that the PISP cannot store. The ECB 'Assessment Guide For The Security Of Internet Payments' published in February 2014 an indicative list of what can be considered as sensitive payment data (page 7). It could be useful to refer to this report to provide more clarity.

Article 47 - Specific obligations of and other provisions concerning account information service providers

Article 47(1)(a): ***provide services only where based on the payment service user's permission, in accordance with Article 49.***

We suggest keeping the term 'consent' as used in PSD2 and refrain from using the term 'permission'. There is no GDPR interplay in relation to this clause.

Article 49 - Authorisation of payment transactions

Article 49(2): ***Access to a payment account for the purpose of account information services or payment initiation services by payment service providers shall be authorised only if the payment service user has given its permission to the account information services provider or, respectively, to the payment initiation service provider, to access the payment account and the relevant data in that account.***

While chapter 4 'authorisation of payment transactions' is focused on the execution of a transaction, this sub-article mainly focuses on account information. Moreover, this article might (incorrectly) imply that the authentication is performed by the PISP for payment initiation services. We would suggest making it clear that the PISP relies on the ASPSP for authentication, as described in art. 86(2).

Art. 49(7): ***The payment service user may withdraw permission to execute a payment transaction or to access a payment account for the purpose of payment initiation services or***

account information services may be withdrawn by the payment service user at any time. The payment service user may also withdraw permission to execute a series of payment transactions, in which case any future payment transaction shall be considered to be unauthorised.

We suggest completely removing this sub-article from the proposal, as art. 66 “Irrevocability of a payment order” covers revocation, in art. 49(7) created confusion which adversely impacts the finality of a payment transaction and consequently the financial certainty to all actors in the ecosystem.

Importantly, art. 49(7) refers to a new definition ”execute a payment transaction”. *The PSU may withdraw permission to execute a payment transaction […] at any time*. The definition of “execution of a payment transaction” is “*the process starting once the initiation of a payment transaction is completed and ending once the funds placed, withdrawn, or transferred are available to the payee*”. In the current wording of this article, no transaction is final anymore. Therefore, the definition “to execute a payment transaction” should be replaced. 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.

Secondly, the reference to art. 66 (art. 80 in PSD2) has been removed, which results in confusion on the exact relation between art. 49(7)) and art. 66. We suggest maintaining this reference as per PSD2. Lastly, the first sentence of art. 49(7) is incorrectly formulated as ”withdrawn” is mentioned twice which causes confusion.

Given that art. 66 covers both revocation and irrevocability – which makes art. 49(7) redundant – in combination with all the above-described issues in art. 49(7) leads to the suggestion to remove art. 49(7) completely. It does not serve any purpose.

Article 50 - Discrepancies between the name and unique identifier of a payee in case of credit transfers

We are in favour of offering a confirmation of payee (CoP) service both for instant credit transfers as well as ordinary credit transfers and note that PSUs in the Netherlands much appreciate it. Most ASPSPs in the Netherlands already offer CoP on both ‘rails’ to their consumers free of charge. Our experience is that CoP has proven to be a good measure for the payer to prevent misdirected payments and recognize and help prevent certain types of fraud, such as invoice fraud. The check protects customers without compromising beneficiaries' privacy. Unfortunately, this measure is less effective for other types of fraud and online scams. Importantly, the implementation of a CoP solution that can communicate with PSPs and service providers across Europe requires complex technical solutions. We suggest strongly aligning these timelines with the timelines to be used for CoP in light of the Instant Payments Regulation.

Art. 50(1): ***In case of credit transfers, the payment service provider of the payee shall, free of charge, at the request of the payment service provider of the payer, verify whether or not the unique identifier and the name of the payee as provided by the payer match, and shall communicate the outcome of this verification to the payment service provider of the payer. Where the unique identifier and the name of the payee do not match, the payment service***

provider of the payer shall notify the payer of any such discrepancy detected and shall inform the payer of the degree of that discrepancy.

It is currently unclear whether payment initiation service providers (PISPs) are seen as 'payment service provider of the payer' and therefore fall in scope of art. 50(1) and are obliged to offer confirmation of payee to the payer. Some of our members indicate that art. 50(1) in conjunction with art. 50(2) confirm that PISPs are in scope. However, we would recommend to clearly indicate which payment service providers fall in scope of this sub-article, to avoid future discussions between market participants. To ensure quality, we also welcome a clear delineation of responsibilities between the chain parties.

Art. 50(1) implies that the PSP must inform the payee about the "degree of discrepancy". We advocate aligning the verification results between those of Instant Payments and those of the PSR. It is for everyone's benefit that how the customer is informed, is similar, regardless of the payment type.

Art. 50(4): ***Payment service providers shall ensure that payment service users have the right to opt out from being offered the service referred to in paragraph 1 and shall inform their payment service users of the means to express such opt-out right. Payment service providers shall ensure that payment service users that initially opted out from receiving the service referred to in paragraph 1, have the right to opt in to receive that service.***

We advocate for the removal of the opt-out function for CoP from the proposal for two reasons:

1. The opt-out function would *decrease* consumer protection;
2. There will be *no demand* for an opt-out function if CoP is – or must be – offered free of charge.

Both the European Parliament and the Council share this view and made amendments to the Commission's proposal on instant payments regarding the requirement to offer CoP, to ensure that PSPs are not required to offer an opt-out function when CoP is offered for free.

It is important to note that only the *payer* can make use of an opt-out function for CoP, and not the *payee*, as clarified by the European Data Protection Supervisor. More importantly, we fear that in general an opt-out function will decrease the efficacy of a CoP service. A fraudster could simply ask the payer to use the opt-out function and bypass verification. This seriously reduces the effectiveness of CoP as a consumer protection measure.

Art. 50(5): ***Payment service providers shall inform their payment service users that authorising a transaction despite a detected and notified discrepancy or that opting out from receiving the service referred to in paragraph 1 may lead to transferring the funds to a payment account not held by the payee indicated by the payer. Payment service providers shall provide that information at the same time as the notification of discrepancies or when the payment service user opts out from receiving the service referred to in paragraph 1.***

This implies that every time a PSP informs the PSU of a discrepancy, the PSP must inform the PSU about the implications. We wonder whether providing a PSU such a notification each time would be effective, it might end up like a cookie pop-up in a browser (i.e., simply click on "accept").

Art. 50(6): ***The service referred to in paragraph 1 shall be provided with respect to payment orders placed through electronic payment initiation channels and through non-electronic payment orders involving a real-time interaction between the payer and the payment service provider of the payer.***

We welcome the proposal by the Commission to mandate CoP for (i) electronic payment initiation channels and (ii) non-electronic payment orders that have real-time client interaction which allows for an efficient follow-up. We recommend extending the requirement of "real-time client interaction" also to CoP for electronic payment initiation channels, to ensure an efficient follow-up. A confirmation of payee service for corporate batch and bulk payments, however, is not feasible since there is no real-time interaction with the payer.

In most cases, a payer (i.e., corporate) cannot immediately respond (i.e., execute or withdraw a payment order) when CoP reports a close match or no match, since bulk transactions could be processed outside of business hours. This could negatively affect the business of corporates. In any case, pre-agreed terms and instructions between the ASPSP and the corporate PSU submitting the batch/bulk payments on how to handle, and deal with, CoP outcomes in a non-real time context will be required to avoid problems. This service should therefore be left to corporates and ASPSPs, who are in the position to determine the requirements.

Lastly, we would like to suggest defining "non-electronic payment orders" to avoid confusion.

Art. 50(7): ***The matching service referred to in paragraph 1 shall not be required where the payer did not input himself the unique identifier and the name of the payee.***

We welcome this proposal, as it clarifies that CoP is not required for point-of-sale and e-commerce payments. This would only disturb the customer journey. We however suggest specifying this article in more detail, for two reasons:

1. Clarify which use-cases are in scope of this article meant to avoid unintended consequences and future discussions. For instance, a credit transfer to a payee who the payer saved in his/her address book could be in scope of this article, as the payer did not input the unique identifier and name;
2. The current text can cause a troublesome situation for fraud cases where the customer is giving access via Remote Access Tooling and did not input himself. Better to describe for which payment types this does not apply (e.g., MIT or CNP). Rewrite paragraph 7 from: "*The matching service referred to in paragraph 1 shall not be required where the payer did not input himself the unique identifier and the name of the payee."* To: *"The matching service referred to in paragraph 1 shall not be required for payment types where the payer is unable to input himself the unique identifier and the name of the payee.*

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

Art. 51(1): ***Where a specific payment instrument is used for the purposes of giving permission, the payer and the payer's payment service provider may agree on spending limits for payment transactions executed through that payment instrument. Payment service***

providers shall not unilaterally increase the spending limits agreed with their payment service users.

We strongly advocate for the removal of the last sentence. 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. Or to decrease to combat fraud. Requesting each PSU's permission will result in an operational disaster.

Article 54 - Notification and rectification of unauthorised, authorised or incorrectly executed payment transactions

Art. 54(1): ***The payment service provider shall only rectify any unauthorised, incorrectly executed payment transaction or authorised payment transaction where the payment service user notifies the payment service provider in accordance with Articles 57 and 59 without undue delay after becoming aware of any such transaction giving rise to a claim, including a claim under Article 75, and no later than 13 months after the debit date.***
The time limits for notification laid down in the first subparagraph shall not apply where the payment service provider has failed to provide or make available the information on the payment transaction in accordance with Title II.

To reduce fraud and to stop fraudsters as soon as possible, it is vital that PSR introduces an obligation for payers (and payees) to check the PSP's transaction information on any unauthorised transaction within a specific and short timeframe after receipt of this information or that information being available. We would suggest a maximum timeframe of two weeks.

Art. 54(2): ***Where a payment initiation service provider is involved, the payment service user shall obtain rectification from the account servicing payment service provider pursuant to paragraph 1 of this Article, without prejudice to Article 56(4) and Article 75(1).***

This article led to unclarity in PSD2 and unfortunately has not been amended in PSR. The article is aimed at the PSU being a consumer, not a legal entity. However, in the case of a PSP, the PSU is a merchant (and not a consumer). We therefore would like to receive clarity on how this article should be interpreted and how the consumer should notify the PSP if there is no contact. Is it meant to be construed as the consumer reaches out to the merchant and the merchant reaches out to the PSP? Throughout the text, it remains unclear who the PSU is.

Article 55 - Notification and rectification of unauthorised, authorised or incorrectly executed payment transactions

Art. 55(1): ***Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the burden shall be on the payment service provider accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.***

Compared to its PSD2 equivalent (art. 72), in the title the word “authentication” has been changed to “authorisation“. Also, in paragraph 1 and 2, authentication has been changed to “authorisation”. The Commission considers that, with social engineering, the difference between authorized and non-authorized transactions is becoming more blurred and complex to apply in practice. We have to strongly disagree here.

Using social engineering techniques, scammers manipulate victims into authorising transactions. At the moment of the authorisation, the customer *intends* to conduct the transaction and only afterwards the person realizes 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.

Under PSD2 in the absence of consent, a payment transaction shall be considered to be unauthorised. To avoid ambiguities, we advise adding the following definition of authorisation in the PSR under article 3: *“definitions: “the expression of the permission given by a payer to his payment service provider, through the process and in the form agreed between the payer and his payment service provider”*.

Of course, this does not solve the problem that criminals manipulate consumers into authorising a transaction. In practice, we even see victims in the Netherlands reading scripts from criminals to PSPs to allow payment to go through. It is extremely difficult, and in most cases impossible for a PSP to determine if the payer is manipulated into authorizing a transaction. PSPs do not have, or want, the means to determine the consumer’s intent because this would come with major privacy implications for consumers and slows down payment transactions due to additional checks. It would also mean that payments are no longer final because every customer can say that he was tricked into making a transaction and did not intend to make the payment. This is undesirable.

Article 56 – Payment service provider’s liability for unauthorised payment transactions

Although this Article does not differ very much from Article 73 PSD2, we suggest some additions and changes. We suggest adding the situation of gross negligence also in Paragraph 1 and 2 to make it clearer that when the payer acted with gross negligence, the payer also gets information from his PSP that he gets the amount refunded, because there was not gross negligence, or that he gets a justification for the refusion by the PSP. Please see our suggestions below.

Art. 56(2): *Where the payer’s payment service provider had reasonable grounds for suspecting fraud committed by the payer it shall, within 10 business days after noting or being notified of the transaction, either refund the payer the amount of the unauthorised payment transaction if it has concluded, after further investigation, that no fraud has been committed by the payer, or provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 90 to 94 if the payer does not accept the reasons provided*.

Where the payer's payment service provider had reasonable grounds for suspecting fraud committed by the payer, please add "or the payer has acted in gross negligence", the payer's payment service provider shall, after noting or being notified of the transaction, do either of the following:

a) refund the payer the amount of the unauthorised payment transaction if the payer's payment service provider has concluded, after further investigation, that no fraud has been committed by the payer or the payer did not act with gross negligence.
b) provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the payer does not accept the reasons provided."

When the PSP has reasonable grounds for suspecting fraud committed by the payer, it is important for the PSP to have the ability to require the payer to report the crime to the police. False reports are punishable and therefore raise the threshold for fraudsters to make false reimbursement claims. Given the limited capacity of the police, this regularly takes several weeks in practice. The ability to require a police report corresponds to recital 80: *"As soon as the consumer becomes aware that he or she has been a victim of that type of spoofing fraud, the consumer should without undue delay report the incident to the police, preferably via online complaint procedures, where made available by the police, and to his or her payment service provider, providing every necessary supporting evidence. No refund should be granted where those procedural conditions are not fulfilled."*
Hence, it is in line with the response of Com. McGuiness[2].

Art. 56(2): *Where the payer's payment service provider had reasonable grounds for suspecting fraud committed by the payer, the payer's payment service provider shall, within 10 business days after noting or being notified of the transaction, do either of the following […].*

We want to be able to contribute to the detection of criminals and thorough investigations are needed for this. A time limit on these investigations is undesirable, as fraudulent payers have every interest in delaying the investigations. In other words, such time limits will tend to increase the chance of successful fraud cases. Therefore, we suggest removing the maximum of 10 working days in the article.

Article 57 - Payment service provider's liability for incorrect application of the matching verification service

If this article aims to protect consumers for fraud next to protecting for errors, it should be added to this article that the PSP should receive the police report from the payment service user. The police report is necessary for multiple reasons: (1) for the investigation of the PSP on the fraud, (2) that no false claims based on this Article will be made by payment service users and (3) that the police will trace the scammers and the prosecutor can prosecute the scammers.

We support that this article places partial responsibility on acquiring PSPs in deterring fraud through the matching verification service. This will help deter fraud.

[2] Com. McGuiness Review PSD2. Ares (2023)3672906

The liability within the process of the CoP is unclearly assigned. To avoid liability, banks will have to be able to prove that: they offered the CoP, that the execution was correct, that the customer ignored the outcome, that the customer turned off the CoP etc. This is going to create an additional administrative burden for PSPs.

Art. 57(1): ***The payer shall not bear any financial losses for any authorised credit transfer where the payment service provider of the payer failed, in breach of Article 50(1), to notify the payer of a detected discrepancy between the unique identifier and the name of the payee provided by the payer.***

Art. 57(2): ***Within 10 business days after noting or being notified of a credit transfer transaction executed in the circumstances referred to in paragraph 1, the payment service provider shall do either of the following:***

(a) refund the payer the full amount of the authorised credit transfer; […].

We would like to receive clarity on what the PSP must refund and see alignment between art. 57(1) and 57(2): *"full amount of the credit transfer"* and paragraph 2: *"full amount of the authorised credit transfer"*.

Art. 57(3): ***Where the payment service provider of the payee is responsible for the breach of Article 50(1) committed by the payment service provider of the payer, the payment service provider of the payee shall refund the financial damage incurred by the payment service provider of the payer.***

As discussed in Article 50, Article 57 contains an unclear division of liability: paragraph 3 is very unclear. When is the PSP of the payee liable and for which part? It is also unclear when a PISP is in the chain. Who is liable then? Or suppose both PSPs use a go-between: who is responsible for (what) mistakes made by this service provider? Suppose a payee PSP cannot deliver due to (internet) failure involving force majeure. For that the payer PSP is not responsible, but liable for a compensation fraud amount? The above scenarios will possibly lead to legal finger pointing if no clarity is provided. The division of liability within this article should be clearer and more complete (addressing the intermediary in this model).

Article 58 - Liability of technical service providers and of operators of payment schemes for failure to support the application of strong customer authentication

Art. 58: ***Technical service providers and operators of payment schemes that either provide services to the payee, or to the payment service provider of the payee or of the payer, shall be liable for any financial damage caused to the payee, to the payment service provider of the payee or of the payer for their failure, within the remit of their contractual relationship, to provide the services that are necessary to enable the application of strong customer authentication.***

We are concerned that Article 58 of the PSR will introduce a new liability framework for technical services providers and operators of payment schemes with significant unintended consequences.

Article 58 unnecessarily interferes with how PSPs procure services from third parties and how parties allocate risk and liability under their contracts based on the services being provided. If this new framework is implemented, third parties (including small Fintechs supplying services to PSPs) will be exposed to unlimited liability to PSPs, large merchants, and consumers in Europe, resulting in changes to business models, increased costs (which will invariably be passed on to consumers) or rendering certain services commercially.

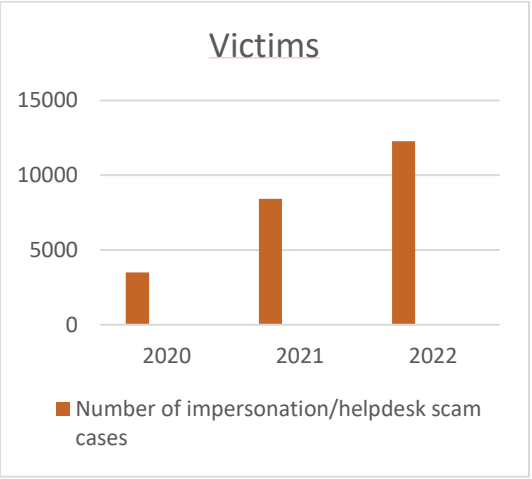
Article 59 - Payment service provider's liability for impersonation fraud

This is a whole new article. In PSD2 only non-authorised transactions needed to be compensated by the PSP. Now, bank-employee-impersonation fraud, one specific scam, must be compensated by the PSP.

Online scams have increased in recent years. In 2022, 8% of the Dutch population became a victim of such practices. Online scams can have severe negative consequences on victims, and not just financially. Scams erode societal trust and feeling of safety, impacting victim's overall well-being and trust in other persons and digital society. 42% of the victims lost trust in society and 22% of the victims indicated that they feel less safe.[3]

Online scams rely on social engineering, a technique that is used to manipulate and deceive individuals into transferring money. Banks are limited in preventing online scams, as the manipulation happens *outside* the payment system where banks cannot detect the crime. Therefore, we strongly advocate to exclude online scams from the PSR.

A liability shift does not reduce bank-employee impersonation scams. In 2020, Dutch banks decided to compensate damages caused by 'bank-employee impersonation scam' out of leniency. The Dutch example shows that placing liability on banks does not decrease bank-employee impersonation fraud. See the figures below.



Source: Dutch Banking Association (https://www.nvb.nl/english/), internal, 2022/2023

[3] Research on online safety and crime 2022, Statistics Netherlands (CBS)

Bank-employee-impersonation fraud is difficult for banks to recognise because the consumer is misled by the criminal into transferring money itself and banks do not know the consumer's intention. Measures such as strong authentication and detection cannot prevent social engineering.

Fraud damage should not be carried by banks. The far-reaching developments in artificial intelligence ('A.I.') give criminals unlimited opportunities to carry out impersonation scams. The first cases of impersonation scams where the criminal has deployed A.I. are already known in Europe (voice cloning). We strongly recommend the Commission to investigate the threats and risks of A.I. in light of impersonations scams before implementing measures such as reimbursements.

Furthermore, reimbursements increase the risk of moral hazard and first party fraud. The only solution is far-reaching cooperation with partners in the scam chain, and precisely that is hindered by placing all liability on the banks. Reimbursements reduce the incentives and pressure on other actors in the chain to help solve the problem. It also reduces incentives for prevention. As online fraud is a cross-sectoral problem, it is of vital importance to break with the current singular approach, meaning closer and more efficient cooperation.

Criminals have been active for a long time before a transaction is made. They start their criminal journey at the beginning of the fraud chain with social media platforms, online services, and communication channels. Criminals gather detailed information about their victims and reach out to the victims through communication channels and platforms. We must focus on preventing fraud and detecting criminals in the beginning of the chain. An obligation for providers of electronic communications (such as telecommunication providers, ISPs, Remote Access Tool providers, etc.) to cooperate and prevent fraud is a good first step, but they can take more preventive and detection measures. What responsibility do they have and how will this be established? This remains unclear in the PSR.

Cooperation across national borders is necessary. In the Netherlands we see an increase in foreign cash-outs; about 40-50% of the victim's money goes to PSPs abroad. Most of these "cash-outs" take place at certain Fintechs. Cooperation among regulators is necessary to stop this cash-out trend. We are not in favor of legislation in this area because it does not solve the major *social* problem. In case this liability will remain in the PSR then we propose the amendments:

- The word "Bank-Employee" must be added in the title of this article*: "Payment service provider's liability for bank-employee-impersonation fraud".* This makes it very clear that the victim's bank has to be impersonated in order for this article to be applicable.
- An addition to this article is preferable, that the PSP of the consumer that became victim of bank-employee-impersonation scams and compensates the consumer, takes over the claim the consumer has on the beneficiary of the money the client transferred the money to via the authorised transaction, directly. Please add the following paragraph: *"Where the payment service provider has refunded the consumer according to paragraph 1, the claim of the*

consumer against the beneficiary shall by operation of law, be transferred to the payment service provider which has refunded the consumer.“

- To reduce the risk of a false claim, a paragraph needs to be added mandating the victim to comply to the investigation and to provide all relevant information to proof on how the impersonation happened: *“Under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider. Additionally, the consumer has to provide some form of evidence that there has been impersonation of an employee of his/her bank, and the customer must adequately assist the bank in the investigation of the impersonation fraud.”*

Art 59(1): ***Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer’s payment service provider using the name or e-mail address or telephone number of that payment service provider unlawfully and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider.***

We recommend adjusting that ‘social engineering’ should always be involved. Otherwise the mere mention of a bank employee's name by criminals is sufficient for compensation. If the customer is called by another organization, he/she can suffice with just saying that it was the bank and still receive compensation, which means that as a bank you also must pay compensation for police impersonation scams. We propose the following change in Article 59(1):

“Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer’s payment service provider using the name or e-mail address or telephone number of that payment service provider unlawfully and that ~~manipulation~~ social engineering gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, reported the fraud to the police and notified its payment service provider.”

Art. 59(2): ***Within 10 business days after noting or being notified of the fraudulent authorised payment transaction, the payment service provider shall do either of the following: […]***

This article misses a very relevant condition: To become eligible for compensation, the victim must report the crime to the police. A police report is necessary for multiple reasons:
(1) For the investigation of the PSP on the fraud;
(2) that no false claims based on bank-employee-impersonation scams will be done by consumers; and
(3) that the police will trace the scammers and the prosecutor can prosecute the scammers.
The underlined words need to be added in paragraph 2: “*Within 10 business days after noting or being notified of the fraudulent authorised payment transaction and having received the detailed police report, the payment service provider shall do either of the following …”*

Art. 59(5): ***Where informed by a payment service provider of the occurrence of the type of fraud as referred to in paragraph 1, electronic communications services providers shall***

cooperate closely with payment service providers and act swiftly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC, including with regard to calling line identification and electronic mail address.

This article establishes an obligation for electronic communications services providers to cooperate with PSPs. It would help clearing doubts in the future if in this article explicit reference is made to the need to share data in the context of such cooperation between PSPS and electronic communication services providers. In addition, a reference should be included in the relevant article that should be added in the PSR that will provide for the processing of data that may qualify as personal data relating to criminal offences.

We welcome adding other relevant partners that are involved in the fraud chain of the bank-employee-impersonation scams, such as the police, the public prosecutor's office, Big Tech, Internet Service Providers, social media platforms and webshops. We would like to see a description of the responsibilities of electronic communications services.

Article 61 - Payment transactions where the transaction amount is not known in advance

Art. 61(1): ***Where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction and the exact future amount is not known at the moment when the payer authorizes the execution of the payment transaction, the payer's payment service provider may only block funds on the payer's payment account if the payer has given his or her permission to that precise amount of funds to be blocked.***

Article 61 seems to only refer to the context of card-based transactions. We would like to emphasize that the content of paragraph 1 would soon also apply to (premium) Open banking ("cardless") payment transactions with premium services like a payment certainty mechanism via a reservation of funds (as 'pre-authorisation mechanism'). In this case it would be a payment initiated by the payee through a PISP.

Art. 61(2): ***The amount of the funds blocked by the payer's payment service provider shall be in proportion with the amount of the payment transaction which can reasonably be expected by the payer.***

This article requires the amount of the blocked funds by the payer's PSP to be in proportion with the amount that can reasonably be expected. It is important that a requirement for the payee or payee PSP is added to this article. The payer's PSP is not able to determine the amount that can be expected.

Chapter 5 Execution of payment transactions

Article 76 - Liability in the case of payment initiation services for non-execution, defective or late execution of payment transactions

Art. 76(1): ***The burden shall be on the payment initiation service provider to prove that the payment order was received by the payer's account servicing payment service provider in accordance with Article 64 and that within its sphere of competence the payment transaction***

was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the non-execution, defective or late execution of the transaction.

A PISP has limited capabilities to store the information in its log files. We suggest clarifying which information would be sufficient.

Chapter 6 Data protection

Article 80 – Data protection

Art. 80: ***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:***

(a) technical measures to ensure compliance with the principles of purpose limitation, data minimisation and storage limitation, as laid down in Regulation (EU) 2016/679, including technical limitations on the re-use of data and use of state-of-the-art security and privacy-preserving measures, including pseudonymisation, or encryption;

(b) organizational measures, including training on processing special categories of data, limiting access to special categories of data and recording such access.

In general, we welcome sharpening technical aspects of the PSR regarding data protection. This could be done by emphasizing and providing more details on the need for data sharing and paying further attention to safeguards to the privacy of individuals. Also, a solid ground to be able to share data related to criminal offences including safeguards for individuals needs to be provided, which is a necessary requirement if fraud related data is to be shared effectively for the purposes of the PSR.

We suggest article 80 to start with a general statement that the processing of data in the context of the PSR will be processed in line with the GDPR. It may be useful to refer to the different grounds on which the processing of the data of users can be based and in line with recital 97 that data of silent parties can be processed too. See also the comments on recital 97. This article should also explicitly refer to the substantial public interest mentioned in recital 98.

See our comments on this recital.

Consideration 98 and article 80 state that special categories of data might be processed under certain circumstances. The necessity of the use of this data should be further explained in order to fulfil the requirements as formulated in e.g., ECJ, 24 February 2022 (ECLI:EU:C:2022:124). We would also like to stress that the use of special categories of data might not be enough, since also

data relating to criminal convictions and offences might be necessary in the context of the Regulation.

One of the measures mentioned as organizational measure is ‘data recording of such accesses. It is uncertain how this would work in practice. For example, if a client calls a bank regarding a specific transaction, and this transaction contains special categories of data (e.g., a cash withdrawal at a pharmacy/hospital), it would be (technically) very hard to record this kind of access.
We welcome the Commission’s proposal to remove “explicit consent” or “permission” (as in PSR) from this article. Its PSD2 equivalent art. 94(2) referred to “explicit consent” which led to a lot of confusion.

Chapter 7 Operational and security risks and authentication

Article 82 – Fraud reporting

We note that Article 82(2) and (3) PSR will harmonize the statistical reporting data and reporting templates by means of regulatory technical standards to be adopted by the Commission. The reporting data and templates under PSR may be different from the current data and templates. Is it the intention to harmonize reporting practices in line with the current EBA Guidelines on fraud reporting under PSD2, or are further changes intended? We would like to have the proportionality of the request substantiated. We would also like more insight into how the EBA uses this data.

Article 83 - Transaction monitoring mechanisms and fraud data sharing

Fraud detection is an important tool which all banks use. All professional providers whose services and systems are abused to commit the crime should be obliged to have effective fraud detection. Nevertheless, fraud detection is not the holy grail that prevents online scams from happening. The effectiveness of fraud detection for online scams is limited because criminals do not breach the payment system but manipulate victims into transferring the money to accounts held by criminals.

The authorisation and authentication are legitimate, and the transaction can therefore rarely be identified as fraudulent. This makes detecting scams, like impersonation scams, very difficult for banks. The Commission's proposal to add additional rules will have a substantial operational impact on banks. However, it does not increase the likelihood of banks identifying online scams. Focus should be on early detection of criminals by intense cooperation between all parties throughout the scam chain.

This article is about fraud monitoring in “real time”, and not about transaction monitoring, which is mostly done after the transaction is made and applies to AML/CTF. We therefore suggest replacing “transaction monitoring” in the title with “fraud monitoring”.

Art. 83(1): ***Payment service providers shall have transaction monitoring mechanisms in place that:***

(a) support the application of strong customer authentication in accordance with

Article 85;
(b) exempt the application of strong customer authentication based on the criteria under Article 85(11), subject to specified and limited conditions based on the level of risk involved, the types and details of the data assessed by the payment service provider;
(c) enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services.

We suggest amending the text as follows:

"Payment service providers shall have fraud detection in place that:

(a) *support the application of strong customer authentication in accordance with Article 85;*
(b) *(b) exempt the application of strong customer authentication based on the criteria under Article 85(11), subject to specified and limited conditions based on the level of risk involved, the types and details of the data assessed by the payment service provider;*
(c) *(c) enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services."*

It is logical that a PSP must comply with art. 85 but art. 83 (1)(a) does not need to be part of the fraud detection system. Operationally implementing this has a lot of impact while it does not add any weight to the security of the fraud detection, and it is therefore disproportionate to implement this.

Fraud detection and fraud rules should not be determined in the PSR. Given the fact that PSPs are very limited in detecting online scams, a principle-based approach would be more suited to enhance fraud monitoring then a rule-based approach. Furthermore, if the Commission aims to strengthen fraud detection, we suggest focussing on legislation that supports data sharing with parties in the scam chain. If PSPs were allowed to use more data from electronic services providers, they could strengthen their fraud detection systems and detect more online scams.

Art. 83(2): ***Transaction monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online, taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials, including the respective environmental and behavioural characteristics.***

We suggest amending this text to: "Fraud monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online. Processing shall be limited to the following data required for the purposes referred to in paragraph 1: […]."

83(2) limits the data fields that may be used during fraud monitoring. We regard this article as only applicable for fraud monitoring and not on AML/CFT related transaction monitoring, because the

limited data use as mentioned in this article is not sufficient for AML/CFT legal requirements regarding transaction monitoring. Even for fraud monitoring the data that we are allowed to use, might not be sufficient. For example, the monitoring mechanisms shall be based only on the analysis of previous payments accounts. Question is whether that would be sufficient in order have a well-functioning monitoring in place.

[…] Payment service providers 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. […]

If we interpret the above correctly, this means that we must immediately delete profiles and historical data of clients with whom the business relation was ended due to fraud. This would cause issues at a later stage in (potential) lawsuits. What if we have a dispute with the client? Or a subpoena from law enforcement? How does this relate to the 7-year retention requirement?
Our suggested text amendment would be "*Payment service providers 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.~~"*

Art. 83(3): ***To the extent necessary to comply with paragraph 1, point (c), payment service providers may exchange the unique identifier of a payee with other payment service providers who are subject to information sharing arrangements as referred to in paragraph 5, when the payment service provider has sufficient evidence to assume that there was a fraudulent payment transaction. 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. Payment service providers shall not keep unique identifiers obtained following the information exchange referred to in this paragraph and paragraph 5 for longer than it is necessary for the purposes laid down in paragraph 1, point (c).***

This article provides a possibility to share data of a payee with another PSP. We recommend for banks to be given the possibility to share information - including data of criminal nature - on fraudulent customers following the first report of fraud. Numbers must be removed in this article. Otherwise, you ensure that there will be more victims of scams and fraud if the investigation immediately shows that the client is involved in fraud or scams and the bank is not allowed to act because of the PSR.

83(3) is also an issue as we look at our Dutch warning system (PIFI) in which the requirement for two different PSUs is not incorporated. In the Netherlands, we developed a warning system for banks. When all criteria are met, banks can register fraudsters in an external reference register (EVR). The strict criteria are set up in the "Protocol Incidentenwaarschuwingssysteem Financiële Instellingen" (PIFI). And only banks in the Netherlands with a permit from the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) utilise PIFI. In case of fraud at a bank and the PIFI criteria are met, some personal data of the client is placed in the EVR. This step is designed to flag fraud risks and to

tackle crime in the financial system. The PIFI has been approved by the Dutch Data Protection Authority.

In order to avoid that the PSR would undermine current data sharing such as PIFI, the following text should be included, possibly in a new paragraph after article 83.5: *"The provisions regarding information sharing arrangements referred to in this article do not affect the validity of existing data sharing mechanisms among PSPs adopted in line with the [GDPR] and applicable Member State law".*

Furthermore, the special duty of care also applies in the Netherlands. If the bank obtains knowledge that a case of fraud has occurred, it must follow-up with adequate actions. Otherwise, the bank could be liable for damages incurred by victims of scams or fraud, even if those victims are not clients of that bank. We suggest comparing the rulings of recent years on this element.

Art. 83(6): ***The processing of personal data in accordance with paragraph 4 shall not lead to termination of the contractual relationship with the customer by the payment service provider or affect their future on-boarding by another payment service provider***

The effect of this sub-article would be that more people become victim of fraud or scams by the same account holder, while this could have been prevented. If a customer obviously is a fraudster, the PSP should be able to end the contract. The opportunities for fraudsters are unlimited if they could easily open new bank accounts without impediments. However, we acknowledge the importance and social relevance of financial inclusion and are aware of the risks for the rights and freedoms of individuals if merely on the grounds of exchanged information they could be automatically banned from obtaining bank services. Therefore, we recommend amending Article 83(6) in the PSR so that a thorough fraud investigation is needed prior to deciding to end a business relationship with a customer.

This would also be in line with recital 105 stating *"Payment fraud data shared amongst payment services providers in the context of such arrangements should not constitute grounds for withdrawal of banking services without detailed investigation."* Therefore, the text should be adequately amended. Our suggested text change would be:
"The processing of personal data in accordance with paragraph 4 shall not lead to termination of the contractual relationship with the customer by the payment service provider or affect their future on-boarding by another payment service provider unless a fraud investigation conducted by the ASPSP has taken place, showing the customers participation in the fraudulent activity."
Not being allowed to offboard a fraudster will negatively affect banks' legal obligations regarding sound and effective risk management expectations derived from the Capital Requirements Directive (CRD) and the Anti Money Laundering Directive (AMLD) and may even pose the bank at risk.

Article 84 – Payment fraud risks and trends

Art. 84(1): ***Payment service providers shall alert their customers via all appropriate means and media when new forms of payment fraud emerge, taking into account the needs of their most vulnerable groups of customers. Payment service providers shall give their customers clear indications on how to identify fraudulent attempts and warn them as to the necessary actions and precautions to be taken to avoid falling victim of fraudulent actions targeting them. Payment service providers shall inform their customers of where they can report fraudulent actions and rapidly obtain fraud related information.***

This article could potentially impact interbank fraud awareness campaigns, we would therefore like to receive clarification if awareness campaigns could also run through banking associations. Moreover, we would like to understand what "all appropriate means and media" mean.

Article 85 - Strong customer authentication

Art. 85(2): ***Payment transactions that are not initiated by the payer but by the payee only shall not be subject to strong customer authentication to the extent that those transactions are initiated without any interaction or involvement of the payer***

This sub-article states that "transactions that are not initiated by the payer" are in principle not subject to the SCA obligation. Are such transactions fully out of scope of the SCA obligation, or are they exempt from the obligation subject to the exemption criteria of Article 82(11) and the RTS of Article 89 PSR?

Moreover, recital (108) states that merchant-initiated transactions (MITs) and Mail Orders or Telephone Orders (MOTOs) may be (partially) exempted from the SCA obligation. Is it correct that these types of orders should be categorized as "transactions that are not initiated by the payer," which are out of scope/exempt from SCA under Article 85(2) PSR?

We also want to point out that by giving MITs a legal basis, an enormous number of transactions will become 'payee-initiated' and thus lack SCA as a fraud prevention means. This can only work if SCA step-up can be performed in case of a suspicion of fraud and consequently shift liability.

Art. 85(3)-(5): ***Related to payee initiated transactions***

We assume this applies not only for card-based transactions but also in the near future for (premium) Open Banking payment services (covering multiple deferred/dynamic future dated or dynamic/variable recurring payments): once a setup of a 'mandate / permission' has been authenticated with SCA, SCA for payment initiations thereafter on the basis of such a mandate is not mandatory/required.

Art. 85(5): ***Where the mandate of the payer to the payee to place payment orders for transactions referred to in paragraph 3 is provided through a remote channel with the involvement of the payment service provider, the setting up of such a mandate shall be subject to strong customer authentication***

Art. 85(6): ***For direct debits, where the mandate given by the payer to the payee to initiate one or several direct debit transactions is provided through a remote channel with the direct involvement of a payment service provider in the setting up of such a mandate, strong customer authentication shall be applied.***

Paragraphs 5 and 6 require the application of SCA for giving a mandate for direct debits and other payee-initiated payment transactions. We expect that requiring SCA will be too impractical. This will cause most mandates that merchants will collect, to be invalid. It is advisable to stipulate a more flexible method for acquiring a mandate. For example, by using a simple form of an electronic signature that proves the identity of the payer and the payer's confirmation of the mandate. And the customer protection of the payment account holders is still guaranteed if the payer seems not authorized to establish a mandate on the applicable payment account and the risk of liability of the involved payer's PSP (debtor bank / ASPSP) will not be increased.

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

The article regulates that only authentication of the customer via the PISP/AISP may be requested the first time it is used, unless the PSP has "reasonable grounds to suspect fraud." This makes detecting fraud more difficult because PSPs will have less data-points to base the fraud detection on compared to current PIS payments. This also has implications for fraud investigations.

Moreover, we are not sure to what extent the reliance of PISPs/AISPs on SCA performed by the PSP changes the relationship between the PSP and PISPs/AISPs, respectively.
Does this require the exchange of any (additional) information with PISPs/AISPs regarding the SCA process?

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

A payer payment service provider shall enter into an outsourcing agreement with its technical service provider in case that technical service provider is providing and verifying the elements of strong customer authentication. A payer's payment service provider shall, under such agreement, retain full liability for any failure to apply strong customer authentication and have the right to audit and control security provisions.

We are concerned this article may lead to the interpretation that PSPs may need to enter into outsourcing agreements with several companies while this would not serve any purpose. PSPs can decide whether a company provides enough security. We therefore would like to ask for a clear definition of a technical service provider, 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 should be viewed as 'technical service providers' and therefore – according to this current article – subject to outsourcing agreements with every PSP that decides to use such features for authentication 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. Nowadays, PSPs can decide whether a particular phone offers secure enough device features to be used for authentication purposes based on relevant international security standards and device specification documentation.

Moreover, as described in art. 87, PSPs keep full liability for any failure to apply SCA. From this perspective, it is unclear *why* an outsourcing agreement would be needed.

Article 88 - Accessibility requirements regarding strong customer authentication

Art. 88(2): ***Payment services providers shall not make the performance of strong customer authentication dependant on the exclusive use of a single means of authentication and shall not make the performance of strong customer authentication depend, explicitly or implicitly, on the possession of a smartphone. Payment service providers shall develop a diversity of means for application of strong customer authentication to cater for the specific situation of all their customers.***

We propose to amend the text as follows:

"Payment services providers shall not make the performance of strong customer authentication dependant on the exclusive use of a single means of authentication ~~and shall not make the performance of strong customer authentication depend, explicitly or implicitly, on the possession of a smartphone. Payment services providers shall develop a diversity of means for application of strong customer authentication to cater for the specific situation of all their customers."~~

Our proposal is based on the following 2 arguments:

1. **According to the proposal, strong customer authentication shall not be dependent on the possession of a smartphone**. We would like to emphasize that the smartphone has become an indispensable tool in promoting the accessibility to and usability of banking services. For accessibility, smartphones offer multiple functions such as contrast options, dark mode, zoom functions, magnifiers, setting font sizes, voice over functions, connecting to refreshable braille displays, sensory alerts, voice control, dictation functions, guides access, etc. Contrary to other devices, these functions work "out of the box," the user does not need to install additional software or devices.

   The smartphone is the preferred option for many users that depend on these accessibility functions. From the viewpoint of usability, smartphones provide better security and authentication than most other devices. The practice of device binding (binding a device to a certain person through a thorough identification process) thereby confirming the possession of the smartphone, does not occur with other devices. Authentication mechanisms such fingerprints, facial recognition or other biometric systems offer protection against 'shouldering'[4].

[4] Obtaining the PIN-code or password by looking over the user's shoulder

2. **According to the proposal the specific situation of all customers should be catered for.** This is unfortunately not possible, entails a very large financial and operational burden to PSPs and seems to be in contradiction with or stricter than the requirements from the European Accessibility Act (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.

It would be advisable to continue this path and not include additional requirements like the phrase *"… to cater for the specific situation of all their customers"*. It could result in a whole catalogue of (operational) procedures having to be catered for, as this is a whole new concept. Furthermore, as mentioned before, this could conflict with the GDPR. The only requirements should be the four accessibility principles: perceivability, operability, understandability, and robustness.

Perceivability, means that information and user interface components must be presentable to users in ways they can perceive; operability, means that user interface components and navigation must be operable; understandability, means that information and the operation of the user interface must be understandable; and robustness, means that content must be robust enough to be interpreted reliably by a wide variety of user agents, including assistive technologies.

Article 89 - Regulatory technical standards on authentication, communication and transaction monitoring mechanisms

Art. 89(1)(ii): ***Regarding the exemption from the application of strong customer authentication for payment transactions, methodologies and models to implement transaction risk analysis.***
We do understand the limitations regarding the transaction risk analysis (TRA) tiers within the current framework. Guidelines are useful and necessary; however, these must be practical and executable. Clear definitions and guidelines about what is in and out of scope of TRA are critical for success in executing it properly.

SCA and fraud reduction
In relation to acquirer TRA, we use this opportunity to also advocate for changes regarding the entity fraud rate calculations. The current EAA calculation method does not consider liability - meaning that every PSP's fraud rate is impacted by all unauthorised/fraudulent remote transactions. As all fraud is allocated to all issuers, acquirer TRA is redundant (despite significant investment from acquirers). This undermines the whole incentive of effective acquirer fraud management in the EAA. Issuers are instead currently incentivized to follow a maximum 3DS/SCA approach and not honor any acquirer TRA exemptions. A shift in calculation approach would instead re-incentivize acquirer TRA for all PSPs.

Article 107 – More favourable refund rights and stricter fraud prevention measures

Art. 107(1): ***Member States or payment service providers may grant payment service users more favourable refund rights in relation to authorised credit transfers as referred to in Articles 57 and 59 and provide for stricter fraud prevention measures that go beyond those set out in Article 83(1) and Article 84.***

Member States can give payment service users more favourable refund rights in relation to authorized credit transfers as referred to in Articles 57 and 59 and provide for stricter fraud prevention measures that go beyond those set out in Article 83(1) and Article 84. When Member States will do this, they must notify the Commission when the Regulation is into force. Any subsequent amendments on this must be notified to the Commission without delay. This Clause does not contribute to the harmonization that PSR strives to accomplish. If you decide to make a regulation, why create the space to deviate nationally? If this article remains, differences will continue to apply to all PSPs in the respective Member States. By adding this Member State option, it creates differences in Member State legislation once again. A level playing field is still not achievable with this article.

***

This concludes the comments and suggestions from the Dutch Payments Association.