Dutch Payments
Association

Response PSR and PSD3

The Dutch Payments Association

We represent around 50 members that are payment services providers active on the Dutch market: credit institutions, payment institutions and electronic money institutions. We organise and coordinate collective and non-competitive tasks in the national payment ecosystem for our members and ensure that stakeholders of the payments infrastructure are at the table. Our responsibilities lie in the areas of infrastructure, standards, and shared product features. We aim for an optimally efficient, secure, reliable, and accessible payment system. As such we have a keen interest in ensuring that the legislation of the payments domain is of the highest quality and is well-aligned with the infrastructure.

The Dutch payments market

The payments market in the Netherlands can be characterised as efficient and innovative: every Dutch person experiences the convenience of iDEAL and a payment request such as Tikkie or Betaalverzoek. Some facts about the Dutch payments market:

- In 2022 a total of 8.1 billion transactions were made in the Netherlands with cash, debit and credit cards, and iDEAL;
- Approximately 4 billion SEPA credit transfers and direct debits are made annually; individual credit transfers have almost completely migrated to instant payments since 2019;
- We increasingly pay contactless; only one in ten debit card payments only involves inserting the debit card into the terminal.

Payment Services Regulation

The Payment Services Regulation (‘PSR’) and Directive on payment services and electronic money services (‘PSD3’) are important legislations for the payments market. The DPA welcomes the PSR, but also sees the need to amend the proposal on several parts. This paper provides an executive, non-exhaustive summary of our main concerns in early December 2023.

1) Strong customer authentication
2) Open Banking
3) Data protection
4) Correct assignment of liability
5) Miscellaneous

Our extensive response to both proposals can be found here (PSR) and here (PSD3).

Strong customer authentication should be consistent and tech neutral

Outsourcing agreements for the application of SCA (art. 87)

Payment service providers (PSPs) rely on manufacturers of smartphones, such as Apple and Samsung, that produce phones with device features like face-ID or fingerprint reading, for the performance of the inherence factor. Art. 87 describes that PSPs should enter into outsourcing agreement with its technical service provider, in case that technical service provider is providing and verifying the elements of strong customer authentication.

We are concerned that these smartphone manufacturers would be viewed as 'technical service providers' and are therefore subject to outsourcing agreements with every PSP that decides to use such features for authentication purposes. This would result in thousands of contracts, without a clear benefit:

- 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;
- These contractual agreements are likely subject to auditing under the EBA outsourcing guidelines.
    - We are concerned that only large PSPs are interesting for smartphone manufacturers to enter into contractual agreements with. Smaller PSPs won't be attractive, due to the burden on smartphone manufacturers to let these PSPs conduct audit controls and a lack of (financial) incentives for the smartphone manufacturers. This affects the competitive position of these PSPs.

Accessibility requirements (art. 88)

Article 88 in the PSR describes accessibility requirements regarding SCA. Importantly, every consumer should be able to perform SCA, therefore Dutch PSPs offer a variety of SCA methods to their customers. However, art. 88(2) goes beyond this requirement. According to the proposal:

1) **The specific situation of all customers should be catered for.**

- This proposal may suggest that payment service providers will be required to offer tailormade individual solutions to a large and heterogeneous group of individuals with (temporary) disabilities. This is unfortunately not feasible and would entail a very large financial and operational burden.
- It seems to be in contradiction with or stricter than the requirements of the European Accessibility Act ('EAA').
- This requirement is in conflict with GDPR, as it could force PSPs to register the specific needs of customers resulting from their disabilities, which possibly include sensitive personal data.

2) **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 and more. The smartphone is the preferred option for many users that depend on these accessibility functions. From the viewpoint of usability and convenience, smartphones provide better security and authentication than most other devices.

Liability technical service providers and scheme operators for failure to support application of SCA

We are concerned that art. 58 of the PSR will introduce a new liability framework for technical services providers and operators of payment schemes with significant unintended consequences. The article 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. This will result in changes to business models, increased costs (which will invariably be passed on to consumers) or rendering certain services commercially.

SCA for direct debit and MIT mandates

Art. 85(5) and (6) require the application of SCA for the initial 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.

Transactions that are not initiated by the payer are not subject to SCA

We would like to receive clarity whether transactions that are not initiated by the payer are fully out of scope of the SCA obligation, or whether they are exempt from the obligation subject to the exemption criteria of Article 85(11) and the RTS of Article 89.

Moreover, according to recital (108) Merchant Initiated Transactions (MITs) and Mail Orders or Telephone Orders (MOTOs) are (partially) exempted from the SCA obligation. We would like to receive clarity whether MITs and MOTOs fall under the exemption of art. 85(2).

We would like 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.

Transaction risk analysis (TRA) and SCA

The current calculation method does not consider liability - meaning that every PSP's fraud rate is impacted by all unauthorised/fraudulent remote transactions. All fraud is allocated to all issuers, explained by EBA in Q&A question 2019_4702. Issuers are therefore incentivized to follow a maximum 3DS/SCA approach and not honour any acquirer TRA exemptions. This makes acquirer TRA redundant, despite significant investment from acquirers. This undermines the whole incentive of effective acquirer fraud management. A shift in calculation approach would instead re-incentivize acquirer TRA for all PSP.

Amendments

Art nr.	Current Text	Proposed Amendment
87	*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.*	*A payer payment service provider ~~shall~~ may at its request 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.*
	Justification: This article requires all PSPs in Europe to enter into outsourcing agreements with smartphone manufacturers, which leads to millions of contracts without a clear benefit. PSPs decide whether a phone offers enough security based on relevant international security standards and device specification documentation, it does not need an outsourcing agreement for this. Moreover, smaller PSPs possibly lack negotiating power to enter into outsourcing agreements with smartphone manufacturers. As a consequence, these PSPs are not able to use that specific smartphone for the application of SCA. This effects the competitive position of smaller PSPs.	

Art nr.	Current Text	Proposed Amendment
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 services providers shall develop a diversity of means for application of strong customer authentication to cater for the specific situation of all their customers.*	*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.~~*
	Justification: While it is important that SCA does not rely on a single means of authentication, the Regulation should be technological neutral and therefore not explicitly refer to smartphones. The smartphone is the preferred option for many users that depend on these accessibility functions. Moreover, it is not feasible for payment service providers to cater for the needs of every single customer. Importantly, this requirement is stricter than the EAA and conflicts with GDPR, as it could force PSPs to register the specific needs of customers resulting from their disabilities, which possibly includes sensitive personal data.	

Art nr.	Current Text	Proposed Amendment
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.*	*~~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.~~*
	Justification: This article 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. It creates a new liability framework with significant unintended consequences. 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. This will result in changes to business models, increased costs (which will invariably be passed on to consumers) or rendering certain services commercially.	

Open Banking - Efficient interface requirements

PSD2 accelerated open banking, which allows licensed third party providers (TPPs) to provide account information services (AIS) and payment initiation services (PIS). After explicit consent from the consumers, third parties can for instance provide a categorized overview of the consumer's expenses or initiate payments. To allow third parties to provide these services, PSD2 requires banks to provide i) a dedicated interface to access the consumer's data and ii) a fallback interface in case the dedicated interface is unavailable (unless a bank was exempted from such obligation by its Competent Authority).

Dedicated interface

In the Netherlands, banks offer high-quality dedicated interfaces. However, in other countries third-parties often have to rely on so-called screen-scraping techniques to access consumer's data, due to a below par quality of the dedicated interface. This is risky for consumers because they have to share security credentials such as log-in codes with third parties, exposing them to risks such as the unauthorised (re-)use of credentials. The third parties don't identify themselves vis-à-vis the bank, but instead use the consumers credentials. Banks are therefore not aware that third parties try to reach a payment account. To protect consumers, screen-scraping is prohibited, described in recital (61).

Fallback interface

PSD2 offers a possibility to obtain an exemption for the fallback interface, but in reality these requirements are tedious to fulfil in the Netherlands and tend to shift over time following contemporary viewpoints. Therefore, in practice, banks were required to maintain two interfaces which resulted in high initial investments and operational costs. We therefore strongly support the removal of the obligation to permanently maintain a fallback interface, described in art. 35(2) PSR. As an alternative, art. 38(2) in the PSR requires ASPSPs to offer without delay an effective alternative solution when the dedicated interface is unavailable.

Art. 38(2) article is very cumbersome and confusing:

- It suggest to use the customer interface as fallback interface, which reintroduces and legitimises the prohibited practise of access by third parties using screen scraping technologies without identifying themselves vis-à-vis the ASPSP, despite recital (61) that prohibits this practice.
- It contradicts with art. 35(2), as banks in practice will still have to maintain a permanent fallback to comply with art. 38(2). Banks will not use the customer interface as fallback option.
- Moreover, unavailability of the dedicated interface for most (Dutch) banks almost always means that the customer interface is also unavailable.

Focus on dedicated interface

We propose to start focusing on high-quality dedicated interfaces, banning all alternative (fallback) interfaces except in very special circumstances that are previously defined. To ensure high quality interfaces, we suggest the following:

- Provide clear guidelines for the dedicated interface, including availability requirements such as the minimum level of up-time. Reference could for instance be made to "Regeling Oversight goede werking betalingsverkeer" that requires an uptime of 99,88%.
- Ensure strict supervision and enforcement on the performance of the dedicated interface.
- No obligation for a fallback interface.

Data parity

Art. 36(4) requires ASPSPs to ensure that the dedicated interface allows PISPs to initiate several types of transactions, such as "place and revoke direct debits" and "initiate payments to multiple beneficiaries". These services are often not offered in the consumer's interface and therefore violates the data parity principle. This principle, described in art. 37(2) and (3), entails that the dedicated interface is to offer payment services that are also offered directly in the customer interface. We strongly recommend sticking to this principle, meaning that ASPSPs only have to offer services to the TPP that are also offered directly to the PSU. Otherwise, banks are obliged to offer services in the dedicated interface that are not directly offered to the customer.

Provision payment information to PISPs

When certain information regarding a payment transaction is not immediately available after receipt of the payment order, the ASPSP shall sent the information to the PISP immediately when it becomes available. It is unclear how 'immediately' should be interpreted and how ASPSPs should send this information to PISPs. This service requires push payment from the ASPSP to the. This is not (by default) supported in the dedicated interface and, importantly, are a value-added premium service. The service could be offered via a premium scheme or via a bilateral agreement. Alternatively, the PISP should be able to do a payment status call at an ASPSP to retrieve the (final) payment status.

Limitation API calls account information service providers

To avoid that the dedicated interface would be overloaded, the RTS of PSD2 allows for a maximum of four API calls per 24 hour when the payment service user is not actively requesting information. The PSR removes this limit in art. 41(2). This proposal sets incredibly high standards on the systems' scalability. We are concerned that the dedicated interface will be overloaded by API-calls and therefore suggest to insert a clause that allows the ASPSPs to perform rate-limiting when the dedicated interface is almost overloaded.

No sharing of private consumer data before authentication

Art. 36(2)(d) describes that the PISP should receive IBAN and account holder name before initiation of the payment. We recommend to provide this type of data after authentication has been performed, for customer protection purposes (fraud prevention and privacy). Only after authentication the payment account data or confirmation can be (safely) provided. The PISP should however receive the data before the payment is executed for screening purposes. Moreover, the PISP should be able to cancel execution of the payment based on the verification. Art. 36(2)(d) and 36(4)(g) should be amended accordingly. Requiring this information before initiation of a payment is not right.

Confirmation of funds

The requirement for ASPSPs to offer the standalone service "confirmation on the availability of funds" (art. 65 PSD2) has been removed. However, this service now has to be offered in the dedicated interface to payment initiation services providers, as described in art. 36(5)(a). We recommend removing this functionality. The available funds should be visible for the consumer, who determines to initiate the transaction. The PISP does not need to have access to the availability of funds.

Prohibited obstacles

- **Art. 44(1)(a) is not an obstacle.** Credentials issued by ASPSPs to PSUs should only be shared with the TPP if necessary. Such provision is related to screen-scraping without proper identification by the TPP, which could harm the PSU.
- **Addition to obstacle art. 44(1)(h)**: ASPSPs should not enforce SCA in a PISP flow in a different manner than such ASPSP requires via its customer interface.

Amendments

Art nr.	Current Text	Proposed Amendment
36(2)(d)	*see, prior to initiation of the payment in the case of payment initiation service providers, the unique identifier of the account, the associated names of the account holder and the currencies as available to the payment service user.*	*see, prior to ~~initiation~~ execution but after authentication of the payment in the case of payment initiation service providers, the unique identifier of the account, the associated names of the account holder and the currencies as available to the payment service user.*

	Justification: For consumer's privacy and fraud prevention purposes, the PISP should not receive the unique identifier and associated names of the account holder before initiation of the payment. This would entail that the PISP receives this information without authentication of the customer. The information should only be provided after the customer has been authenticated, but before execution of the payment to allow the PISP to take the necessary steps if needed.	
Art nr. 36(4)(g)	**Current Text** *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*	**Proposed Amendment** *verify the name of the account holder before the payment is ~~initiated~~ executed and regardless of whether the name of the account holder is available via the direct interface*
	Justification: The PISP should be able to very the name of the account holder before the payment is executed, to comply with screening requirements. However, it should only be possible to receive the name of the account holder after authentication has been performed, to protect the customer's privacy and for fraud purposes.	
Art nr. 36(4)	**Current Text** *Account servicing payment service providers shall ensure that the dedicated interface allows payment initiation service providers, at a minimum, to: […]*	**Proposed Amendment** *Account servicing payment service providers shall ensure that the dedicated interface allows payment initiation service providers, provided that this is offered in the customer interface, ~~at a minimum~~, to: […]*
	Justification: The data parity principle shall apply to this article. This implies that account servicing payments service providers shall only be obliged to include services in the dedicated interface that are also offered directly in the customer interface. Otherwise, banks are obliged to offer services that are not directly offered to the customer.	
Art nr. 36(5)(a)	**Current Text** *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;*	**Proposed Amendment** *~~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;~~*
	Justification: Credentials issued by ASPSPs to PSUs should only be shared with the TPP if necessary. Such provision is related to screen-scraping without proper identification by the TPP, which could harm the PSU.	
Art nr. 38(2)	**Current Text** *In case of unavailability of the dedicated interface, account servicing payment service providers shall inform payment service providers making use of the dedicated interface of measures taken to restore the interface and of the time estimated necessary for the problem to be resolved. 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.*	**Proposed Amendment** *In case of unavailability of the dedicated interface, account servicing payment service providers shall inform payment service providers making use of the dedicated interface of measures taken to restore the interface and of the time estimated necessary for the problem to be resolved. ~~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.~~*
	Justification: This proposed solution is very cumbersome, confusing and contradicts with art. 35(2). It seems that a permanent fallback must still be maintained because it otherwise is not possible to offer "without delay an effective alternative solution". Moreover, the example proposed in art. 38(2) seems to reintroduce and legitimise the prohibited practise of access by third parties using screen scraping technologies without identifying themselves vis-à-vis the ASPSP (despite	

	recital (61)). Screen scraping entails that consumers provide their security credentials (such as log-in codes) to third-parties, which potentially exposes consumers to large risks.	
Art nr. 40	**Current Text** *For the purposes of point (b), where some or all of the information referred to in that point is unavailable immediately after receipt of the payment order, the account servicing payment service provider shall ensure that any information about the execution of the payment order is made available to the payment initiation service provider immediately after that information becomes available to the account servicing payment service provider.*	**Proposed Amendment** *For the purposes of point (b), where some or all of the information referred to in that point is unavailable immediately after receipt of the payment order.~~, the account servicing payment service provider shall ensure that any information about the execution of the payment order is made available to the payment initiation service provider immediately after that information becomes available to the account servicing payment service provider.~~ The payment initiation service provider could make a payment status call to retrieve the (final) payment status.*
	Justification: This service requires push payment from the ASPSP to the. This is not (by default) supported in the dedicated interface and, importantly, are a value-added premium service. The service could be offered via a premium scheme or via a bilateral agreement. As an alternative, the PISP should be able to do a payment status call at an ASPSP to retrieve the (final) payment status.	
Art nr. 41(2)	**Current Text** *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.*	**Proposed Amendment** *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 account servicing payment service provider is allowed to perform rate-limiting when the dedicated interface as a result of the information requests from account information service provider overloads.*
	Justification: Providing account information service providers unlimited access to the dedicated interface could overload the interface. This will result in unavailability of the dedicated interface, affecting all third-party providers. Art. 41(2) should take this into account and contain a clause.	
Art nr. 44(1)(a)	**Current Text** *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;*	**Proposed Amendment** ~~*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;*~~
	Justification: Credentials issued by ASPSPs to PSUs should only be shared with the TPP if necessary. Such provision is related to screen-scraping without proper identification by the TPP, which could harm the PSU.	
Art nr. 44(1)(h)	**Current Text** *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*	**Proposed Amendment** *requiring that strong customer authentication is applied more times or in a different manner 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*
	Justification: ASPSPs should not enforce SCA in a PISP flow in a different manner than such ASPSP requires via its customer interface.	

Open Banking – Permission dashboard

Art. 43 describes the requirement for banks to provide an overview of third party providers (TPPs) that have access to a consumer's payment account, a so-called permission dashboard. This provision is welcomed by the Dutch payments community as it increases consumer's trust and control in open banking. 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.

Importantly, ASPSPs are not part of the PSU – TPP relationship. The PSU provides consent (under PSD2) and permission (under PSR) to a TPP when using its services. Since ASPSPs are not part of the PSU – TPP relationship, they are not in the position to "monitor and manage" permissions, as described in art. 43(1). 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. We therefore propose to amend art. 43(1) accordingly.

Moreover, art. 43 contains several requirements for the dashboard are unfeasible in practice:

- The obligation to provide the **name of the TPP** to which access has been granted, will very often mean that the name of the license-as-a-service will be provided, instead of the actual party that provides the service. Many third-party providers use a license-as-a-service (Laas) provider to connect with bank APIs across Europe, described in recital (26). It is desirable to also include the commercial name of the unlicensed party who is using the customer's data that interacts with the PSU. This party is recognized by the customer. Moreover, when several unlicensed service providers use the same Laas provider and the PSU would like to withdraw permission for one specific service, it is unclear for the PSU which permission it should withdraw as the dashboard will show the name of the Laas provider for each service. Importantly, when a third party without a license uses an aggregator to access a customer's data and provide the services, it is desirable to include the name of this party. Only mentioning the name of the aggregator is mildly informative (if at all) to the PSU and surely not transparent.
- It is **unclear** whether **purpose of the permission** refers to the PSU (i.e., purpose of the 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. Moreover, there's no clear benefit in providing this information to the PSU. When an AISP directly offers a service to the PSU, the purpose of the service is clear.
- **Obligation to offer consumers the possibility to re-establish previously withdrawn access via the dashboard.** This entails that banks inform third parties about the re-establishment, which is operationally not feasible. As TPPs don't have access to the dashboard they would be unaware of any changes. Re-establishment should therefore be performed via the TPP, just as the initial permission was given.
- **Obligation to provide in real-time to the TPP changes made by the consumer in the dashboard.** This would result in operational costs for banks, while there is no demand from TPPs in such a service. A TPP will find out a permission has been withdrawn as soon as an API-call did not go through, which likely will be within a short time-frame. A separate service is therefore unnecessary.

Amendments

Art nr.	Current Text	Proposed Amendment
43(1)	*The account servicing payment service provider shall provide the payment service user with a dashboard, integrated into its user interface, to monitor*	*The account servicing payment service provider shall provide the payment service user with a dashboard, integrated into its user interface, to monitor and manage*

	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.	*the ~~permissions~~ authorised access the payment service user has given for the purpose of account information services or payment initiation services covering multiple or recurrent payments.*
	Justification: ASPSPs are not part of the relationship between the payment service user and the third party provider. Therefore, they are not in the position to "monitor and manage" permissions. They can however provide their customers insight in the (third) parties that had authorised access to specific payment accounts.	
Art nr. 43(2)(a)(i)	**Current Text** *the name of the account information service provider or payment initiation service provider to which access has been granted;*	**Proposed Amendment** *the name of the account information service provider or payment initiation service provider to which access has been granted, and, if applicable, the commercial name of the service provider that ultimately provides the service via a license-as-a-service party;*
	Justification: We suggest to add the obligation to provide the commercial name of the service provider that ultimately provides the service to the customer. In the case a third party without a license uses an aggregator to access a customer's data, it is desirable to include the commercial name of both the licensed party and the unlicensed party who is the Asset User that ultimately provides the service. Only mentioning the name of the aggregator is mildly informative (if at all) to the PSU, as this is not the party that interacts with the PSU. The license-as-a-service provider should indicate the unlicensed party that makes the API-call.	
Art nr. 43(2)(a)(iii)	**Current Text** *The purpose of the permission;*	**Proposed Amendment** *~~The purpose of the permission;~~*
	Justification: It is unclear whether **purpose of the permission** refers to the PSU (i.e., purpose of the 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. Moreover, there's no clear benefit in providing this information to the PSU.	
Art nr. 43(2)(c)	**Current Text** *allow the payment service user to re-establish any data access withdrawn;*	**Proposed Amendment** *~~allow the payment service user to re-establish any data access withdrawn;~~*
	Justification: This entails that banks inform third parties about the re-establishment, which is operationally not feasible. As TPPs don't have access to the dashboard they would be unaware of any changes. Re-establishment should therefore be performed via the TPP, just as the initial permission was given.	
Art nr. 43(4)	**Current Text** *The account servicing payment service provider and the account information service or payment initiation service provider to which permission has been granted shall cooperate to make information available to the payment service user via the dashboard in real-time. For the purposes of paragraph 2 points (a), (b), (c) and (e):*	**Proposed Amendment** *The account servicing payment service provider and the account information service or payment initiation service provider to which permission has been granted shall cooperate to make information available to the payment service user via the dashboard ~~in real-time~~. For the purposes of paragraph 2 points (a), (b), (c) and (e):*
	Justification: This would result in operational costs for banks, while there is no demand from TPPs in such a service. A TPP will find out a permission has been withdrawn as soon as an API-call did not go through, which likely will be within a short time-frame. A separate service is therefore unnecessary.	

Correct assignment of responsibilities

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

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

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

The definition could lead to problems in art. 40(b) and art. 75(1), that both refer to term “execution of a payment transaction”.

Amendment

Art nr.	Current Text	Proposed Amendment
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;*	*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;*
	Justification: This article requires the payer’s bank should inform the payment initiation service provider whether the transaction arrived at the payee’s payment account. The payer’s bank is unable to provide this information.	

Art nr.	Current Text	Proposed Amendment
75(1)	*Where a payment order is placed directly by the payer, the payer’s payment service provider shall, without prejudice to Article 54, Article 74(2) and (3), and Article 79, be liable to the payer for correct execution of the payment transaction, 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.*	*Where a payment order is placed directly by the payer, the payer’s payment service provider shall, without prejudice to Article 54, Article 74(2) and (3), and Article 79, be liable to the payer for correct execution of the payment transaction, 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.*
	Justification: The article clarifies that the payer’s bank is not liable to the payee, when it can prove that the transaction amount arrived at the payee’s bank. This liability should be extended to the payer. In its current form, art. 75(1) holds the payer’s bank liable for a part of the transaction that is out of its control.	

Data protection

Sensitive payment data

Currently, it is unclear what is understood as sensitive payment data and what is not.

- Art. 44(2) and recital (67) aim to describe that name and account number of the account owner are not seen as sensitive payment data. However, art. 44(2) is poorly formulated leading to unclarity.
- It is unclear what data does fall in scope of sensitive payment data. Art. 46(2)(a) and 47(2)(a) require account information service provider (AISP) and payment initiation service providers (PISP) to not request or store sensitive payment data. This provides an open-ended obligation to not store any data apart from the name and account number. We would like to receive clarification what would be deemed as sensitive payment data that for instance a AISP or PISP cannot store. Reference could for instance be made to the indicative list on p.7 of the ECB 'Assessment Guide For The Security Of Internet Payments'.

Processing of data

It would be useful to refer to the grounds on which personal data or silent party data can be processed in recital (97). In practice, concerns arise as to what the legal obligation is.

- For the processing of personal data, this could be "legal obligation", "contract between data user and PSP" or "legitimate interest".
- For the processing of silent party data this could be "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.

We suggest art. 80 to include a general statement that the processing of data in the context of the PSR will be processed in line with the GDPR. Additionally, the article should explicitly refer to the substantial public interest mentioned in recital 98.

Data protection

All personal data processed in the context of the PSR needs to abide by Regulation (EU)2016/679, not only personal data that qualifies as special categories of data or data relating to criminal offences. Moreover, to effectively combat fraud it is necessary that personal data is processed and shared. The processing of such data is prohibited unless provided by law (article 10 GDPR). Each Member State has its own rules on the processing of such data and those are not uniform. It is therefore important to refer to art. 10 of the GDPR.

Importantly, we do recommend to make a distinction in Article 80 when it comes to the processing of special categories of personal data (SCPD). There is a difference between personal data that, on the one hand, is processed as such to deduce specific information such as any of the categories of data outlined under Art. 9(1) (e.g. medical devices used to assess the medical situation of persons), and on the other hand, personal data which is not used for their inherent characteristics but which are part of the set to be processed. In the first case, processing has to be intentionally undertaken by the controller with the purpose element in mind and here, controllers would apply the conditions under Art. 9 GDPR and, in the case of PSR, the requirements under paragraphs a and b of Art. 80. However, if financial transaction data are not processed in order to infer SCPD, Article 9(1) GDPR nor Art. 80(a) and (b) should apply. This is important to clarify in the article because it can have significant operational consequences for banks, particularly as additional technical measures need to be taken.

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

Amendments

Art nr.	Current Text	Proposed Amendment
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.*	*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.*
	Justification: To clarify that name and account number of the account owner are not regarded as sensitive payment data.	

Art nr.	Current Text	Proposed Amendment
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;* *organizational measures, including training on processing special categories of data, limiting access to special categories of data and recording such access.*	*Personal data shall be processed in compliance with Regulation (EU) 2016/679. Payment systems and payment service providers shall be allowed to process special categories of personal data and personal data relating to criminal offences as referred to in Article 9(1) and Article 10 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, to the extent that these allow for the proper execution and processing of payments, 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;* *organizational measures, including training on processing special categories of data and personal data relating to criminal offences, limiting access to these data to the extent necessary as to allow compliance with obligations under this Regulation and allow fraud data sharing as referred to in article 83 of this Regulation ~~special categories of data~~ and recording such access.*
	Justification: All personal data processed in the context of the PSR needs to abide by Regulation (EU)2016/679, not only personal data that qualifies as special categories of data or data relating to criminal offences. This addition clarifies this point. To effectively combat fraud it is necessary that personal data is processed and shared. These data may contain personal data that qualify as data relating to criminal offences (for example, the suspicion that a client is involved in fraud may qualify as "personal data relating to criminal offences"). The processing of such data is prohibited unless provided by law (article 10 GDPR). Each Member State has its own rules on the processing of such data and those are not uniform. The inclusion of art. 10 GDPR is necessary to 1) provide for a uniform exception that allows the processing including safeguards as per article 10 GDPR and 2) avoid fragmentation.	

	The “extent necessary for the provision of payment services” raises doubts as to in which situations the measures under a) and b) should apply. In the execution of payments, payment service providers process data that directly or indirectly qualify as special categories of data. This is for instance the case with payments to a religious institution. These type of payments should not be subject to the specific conditions under art. 80 a) and b). The measures could however apply to possible further processing of such categories of data. If the proposed text is maintained, the measures proposed could significantly impact the execution of payments on the request of the payer to a payee. The measures can be implemented to the extent they are not blocking the proper execution of payments. Clarification is however necessary regarding the meaning of “recording such access”.

Miscellaneous including amendments

Limits and blocking of the use of the payment instrument

Art. 51(1) describes that PSPs shall not unilaterally increase the spending limits agreed with their payment service users. It is currently unclear what 'spending limits' refers to. This could for instance be the maximum daily spending limit or transaction limit for credit transfers, but also the maximum contactless limit. **We strongly recommend ensuring that PSPs can amend the spending limit for contactless payments unilaterally** (for instance in circumstances like COVID-19, inflation, or in relation to security threats) with the option for the customer to determine their 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.

Unclarity regarding the irrevocability of a payment order

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

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

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

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

Remove 'central bank money' from "funds" definition

We noticed a proposed change in the definition of "Funds" in art. 3(30) 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 legal framework of such digital currency must be finalized, and the technical set-up and infrastructure must be final to accurately assess and allocate regulatory obligations and liabilities. **The definition of 'Funds' should therefore be kept to the current definition under PSD2.**

Information on currency conversion charges – art. 20(c)(v)

PSPs process cross-currency transactions for clients such as individuals and corporates, for example a euro to U.S. dollar transaction. PSPs use real-time foreign exchange (FX) rates to execute these transactions. It uses reliable market sources such as Reuters or Bloomberg for these rates.

FX rate sources should not be limited to the ECB

When expressing the charges for currency conversion services, such as with cross-currency transactions, art. 20(c)(v) requires PSPs to limit themselves to the FX rate issued by the relevant central bank. The ECB only publishes FX rates on a daily basis instead of in real-time. This can have a significant impact on the reported charges, as exchange rates vary throughout the day. The real-time market rate that a PSP uses for the currency conversion usually comes from an independent provided different than the ECB. This rate could be significantly different compared to the FX rate published by the central bank. As a result, the estimated charges provided to the customer are not representative. PSPs should therefore not be limited to one single source (i.e. the relevant central bank) when expressing the charges for FX reference rates. Instead, PSPs should be able to continue using other reliable sources available in the market. These sources are fully independent and publish real-time FX rates.

Estimated charges to be expressed as percentage mark-up or fixed mark-up

The current article requires PSPs to express the estimated charges as a percentage mark-up over the foreign FX rate published by the relevant central bank. Some PSPs express their charges as a total mark-up (as an absolute figure) on the FX rate. This method achieves the same goal as a percentage mark-up: visibility for the PSU. PSPs should therefore be allowed to express the estimated charges as (i) percentage mark-up or (ii) total mark-up.

Amendment

Art nr.	Current Text	Proposed Amendment
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.*	*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.~~*
	Justification: It is currently unclear what 'spending limits' refers to. This could for instance be the maximum daily spending limit or transaction limit for credit transfers, but also the maximum contactless limit. We strongly recommend ensuring that PSPs can amend the spending limit for contactless payments unilaterally (for instance in circumstances like COVID-19, inflation, or in relation to security threats) with the option for the customer to determine their 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.	

Art nr.	Current Text	Proposed Amendment
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.*	*Consent may be withdrawn by the payer at any time, but no later than at the moment of irrevocability in accordance with Article 66. Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorised.*
	Justification: The two amendments made to art. 49(7) compared to its PSD2 predecessor lead to confusion on the exact relation between art. 49(7) and 66(1) in PSR. Art. 66(1) states that a PSU shall not revoke a payment order once it has been received by the payer's PSP, while art. 49(7) states that the PSU can withdraw permission to execute a payment transaction at any time. As explained, execution of a payment transaction only ends when the funds have arrived at the payee's payment account. Due to the use of the new term "execution of a payment transaction" in art. 49(7), no transaction is final anymore. For instance, in the current wording of art. 49(7), the payer could revoke a payment when the funds were credited to the beneficiary's PSP but not to the payee yet. Given the above-described issues, we suggest to stick to PSD2 art. 64(3).	

Art nr. **3(30)**	**Current Text** *'funds' means central bank money issued for retail use, scriptural money and electronic money;*	**Proposed Amendment** ~~*'funds' means central bank money issued for retail use, scriptural money and electronic money;*~~ *'funds' means banknotes and coins, scriptural money or electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC;*
	Justification: 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 legal framework of such digital currency must be finalized, and the technical set-up and infrastructure must be final to accurately assess and allocate regulatory obligations and liabilities. **The definition of 'Funds' should therefore be kept to the current definition under PSD2.**	
Art nr. **20(c)(v)**	**Current Text** *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;*	**Proposed Amendment** *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 or another reliable provider, or as a total mark-up;*
	Justification: Allowing a PSP to only express charges relative to the reference rate issued by the relevant central bank, will lead to unrepresentative estimated charges. PSPs should therefore not be limited to one single source (i.e. the relevant central bank) for FX reference rates and should be able to continue using other reliable sources available in the market. These sources are fully independent and publish real-time FX rates, whereas the ECB only publishes FX rates on a daily basis. The current article requires PSPs to express the estimated charges as a percentage mark-up over the foreign FX rate published by the relevant central bank. Some PSPs express their charges as a total mark-up (as an absolute figure) on the FX rate. This method achieves the same goal as a percentage mark-up: visibility for the PSU. PSPs should therefore be allowed to express the estimated charges as (i) percentage mark-up or (ii) total mark-up.	

Miscellaneous (2)

Permission and explicit consent

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. Clarification and confirmation of its contractual nature as opposed to the term explicit consent in the GDPR would help the market.

For art. 46(1)(b) and 47(1)(a) we suggest to stick to the term ‘consent’ as was used in PSD2.

Unclarity regarding references to PSP or PSU

- **Reference to ‘payment service provider’ (PSP) is sometimes unclear** as it could be both the payer’s PSP or payee’s PSP, which in turn can be either the ASPSP or the PISP. Similar to PSD2, several articles mention ‘the PSP’ without specifying *which* PSP is meant and the responsibility of this PSP.
- **Reference to ‘payment service user’ (PSU) is sometimes unclear** as for PISPs it could be both the payer or payee, depending on the use-case. When acting as a PSP, the PISP has a contract with the merchants (payee) and that’s the PSU. On an accounting platform, the payer is however the PSU for the PISP. This leads to unclarities in art. 46(1)(b) and art. 54(2). The latter article is aimed at the PSU being a consumer and not a legal entity such as a merchant.

This resulted in a lot of confusion in PSD2, **we therefore would recommend preventing this issue from reoccurring in PSR.**

Funds blocked when the transaction amount is not known in advance

Art. 61(2) requires the payer’s PSP to ensure that the amount of the funds blocked for a transaction where the amount is not known in advance is reasonable compared to what can be expected. In the Netherlands the acquirers set the appropriate level for fund reservations, for instance for petrol payments. The acquirers inform the payer’s PSP on this appropriate level. The payer’s PSP cannot be responsible for the appropriateness of this level.

Termination framework contract

We would like to raise concerns on art. 23, relating to termination of the framework contract. There is lack of detail on the application of the proposals.

- It is unclear, pursuant to the commentary in Recital 49, as to whether technical services would also be subject to the requirements on the termination notice period, similar to the payment services. For instance whether a 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.

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.

- 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.
- 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 as to whether these potential unintended consequences have been considered.

PSD3

Transitional provisions

The transitional requirements are currently unclear for payment- and electronic money institutions with a PSD2 or EMD2 license that continue to be active under PSD3, which could have a significant impact on these licensed parties. **We would like to stress the importance of a simplified re-authorisation process for pre-existing institutions to minimise the burden on these firms.**

It is not clear what information would be required for a license under PSD3, i.e., whether it would require a full application or only to provide the additional information new to PSD3 i.e. a wind-down plan, details on security and operational resilience under DORA.

In addition, when existing payment institutions wish to apply for an e-money license, we would welcome the possibility for a simplified procedure, rather than the firm having to apply for a full permission. This would help to realise the full benefits of a streamlined merged regime and promote competition in payments and e-money markets.

Safeguarding requirements

Art. 9(1)(b) describes the requirement when a payment institution holds the funds and has not yet by the end of the business day following the day when the funds have been received delivered those funds to the payee. This article has unfortunately not changed compared to its predecessor in PSD2 and therefore still leads to confusion regarding what a PSP may or may not do. We are in doubt between two interpretations:

- A PSP is unable to hold the funds it has collected from a payer, and to which the payee is the beneficiary, in a customer account foundation ('stichting derdengelden rekening' in Dutch) as a risk mitigation tool in order to offset its own financial exposure for chargebacks due to the payer; or
- Does it simply mean that the funds can be kept on a non-customer account foundation for 1 day before it must be moved to a customer account foundation.

We would like to ask for clarification.

Outsourcing operational functions

Art. 22(1) requires payment institutions to notify the competent authority when it uses outsourcing functions of payment or electronic money services, while the Dutch central bank only requires to be notified of critical or significant outsourcing. This is a discrepancy. We therefore recommend to refer to the EBA Outsourcing Guidelines.