Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0209 (COD)
2023/0210 (COD)

Brussels, 28 April 2025

WK 5345/2025 INIT

LIMITE

EF
ECOFIN
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Consolidation PSD/PSR Presidency questionnaire following WP on 4/04. Ddl 14 April 2025. Replies from 22 MS

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
Presidency Discussion Note: Discussion on fraud-related issues in the Payment Services Regulation (authorisation, liability, burden of proof, gross negligence) (WK 4230/2025 INIT)	
Q1. Could Member States accept the proposed wording of Recital 69a and Article 49 PSR?	DK (MS reply): We can accept the proposed wording of Recital 69a and Article 49 PSR. It is not, however, entirely clear to us what is meant by "a contribution" in "Authorisation is based on an intention or a contribution in fact". DE (MS reply): We strongly welcome the implementation of Option 1 and the respective changes made in Rec. 69a and Art. 49. We request only one change: In Recital 69a "initiated or modified" should be replaced by "carried out". The insertion in Rec. 69a that a modification of a payment transaction by a third party leads to the transaction being unauthorised will blur the line between authorised and unauthorised payment transactions. Example: A payment transaction was initiated by the PSU and modified by a third party. As (obligatory) SCA is required (e.g. push-Tan) the PSU will be asked to confirm the (then) modified

PUBLIC

Question	MS reply
	payment transaction. If the PSU proceeds to confirm the modified transaction, the transaction needs to be considered authorised with regard to Article 49, however, this would be not clear according to the wording "initiated or modified". For this reason, we suggest the more general term "carry out". CZ (MS reply): In recital 69a we would like to ask what is meant by modified by a third party. The word "modified" is also only in the recital but not in Article 49. We prefer deleting this word as it seems redundant. In general, the consent of the payer includes the specific amount and the specific payee (with the exception of direct debits etc.). Therefore, it is not clear what the purpose of "modification" concept is and why it has been inserted in the text. Regarding paragraph 67 of Article 49 - *consent may be withdrawn at any time*. We ask for clarification in the recital that irrevocability (Article 66 PSR) applies once the order is already in the system, similar to PSD2. In this respect the consent may not be withdrawn or at least the withdrawal is without effect. See the wording of PSD2: Article 64 (3) *Consent may be withdrawn by the payer at any time,* ***but no later than at the moment of irrevocability in accordance with Article 80****. 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.* CY (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We do not oppose the proposed wording of Article 49 PSR and Recital 69a PSR, subject to the proposed changes mentioned in the answers below. BG (MS reply): We agree with the Presidency's proposed wording in Recital 69a and in Article 49 PSR. BE (MS reply): BE: Following the approach chosen by Member States, we understand that fraudulent payment transactions based on social engineering would not be considered as unauthorised. Under the current wording of PSR as suggested by the Presidency, in the event of fraud based on social engineering, the transaction will be considered authorised, which means that the PSU will have no refund's right in accordance with Article 56. Therefore, the PSU will have to bear all the financial losses resulting from the fraudulent transaction. We expressed in the past that if such approach were chosen, we should amend liability's provisions to strengthen the consumer protection, in order to avoid victims of social engineering fraud being left without any solution. We mention in particular the need to extend the scope of Article 59. In practice, a very large number of frauds are the result of social engineering (in particular "payee impersonation fraud") and this is

Question	MS reply
	increasing rapidly with new technology and AI. The risk is entirely incurred by the PSU. It is therefore important to include in PSR compensatory measures that could strike the right balance between consumer protection and PSP's accountability in fraud prevention. It is also very important in this context to ensure that the only fact that the payment transaction has been authenticated is in itself not sufficient to prove the authorisation. We understand that the word "not necessarily" is now included in Article 55 (2). During CWP in February, we expressed serious concerns about this wording insofar as it implies that in some cases, the only authentication could still be sufficient to prove the authorisation. In our understanding, it is important that, in any case, the PSP takes into account all the factual circumstances when assessing the authorisation process. Regarding recital 69a and Article 49, we do not disagree with the Presidency's proposal but we have the following remark. Firstly, we regret that the definition of what should be considered as unauthorised payment transaction is only included in a recital and not in Article 49. In our view, not having this definition in Article 49 could

Question	MS reply
	undermine the legal power of such principle. Moreover, in its current wording, Article 49 is verry similar to the wording of the PSD2. However, PSD2 is unclear as regards the notion of authorised and unauthorised payment transaction. We see an added value in clarifying the notion of unauthorised payment transaction in Article 49 PSR insofar as it would help to eliminate the current confusion in PSD2 in this respect. A second paragraph should be included in Article 49, stating that a payment transaction shall not be deemed as authorised where the transaction was carried out by a third party who is acting without the consent of the payment service user. However, the example related to the third party using security credential fraudulently obtained could be left to the recital. Secondly, we have some concerns regarding the word "modified" in Recital 69a. We are not sur which cases are covered in this sentence. See Q1.1. AT (MS reply): **AT:** In line with our support for the previously discussed option 1, we support the proposed wording for Art 49 PSR on authorization. ES

PUBLIC

PUBLIC

Question	MS reply
	(MS reply): ES has from the start positioned itself in favour of option 2. The presidency proposes as compromise some caveats to option 1 following the majority of MSs. ES is favourable to any caveats that aims at improving consumer protection so in this sense, we could accept the proposal. However, we note, that as a downside, it makes more complex the Regulation. SK (MS reply): We can support proposed wording. SI (MS reply): We supported **Option 1** which was proposed in the PRY non-paper on fraud-related issues prepared for the 21 February CWP on the issue of authorisation. Option 1 namely suggested to revert to the European Commission's version of Article 49(1) (with the word permission replaced by the word **consent**) and clarify that a transaction must be both **initiated and authenticated** by the payer in order to be considered authorized. We agree with adding more examples in Recital 69a PSR and we support its wording. However, we prefer to keep the second paragraph in Article 49 PSR rather than moving it to the Recitals. Therefore, we do not support the proposed wording of Article 49 PSR; instead we support the wording

Question	MS reply
	proposed in the PRY non-paper on fraud-related issues, prepared for the 21 February CWP on the issue of authorisation, as Option 1. SE (MS reply): We strongly prefer option 2 but accept the direction chosen by the Council. We welcome the suggested clarification that all payment transactions fraudulently initiated or modified by a third party should be defined as unauthorised. PT (MS reply): Despite supporting the chosen approach of moving forward with Option 1, PT does not agree with the deletion of Article 49(2) as proposed in the February CWP. NL (MS reply): We welcome the approach of option 1 for moving forward on the issue of authorisation. Therefore we support the wording of recital 69a and article 49 PSR. LV (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We were in favor of Option 2, for the sake of a compromise we can support what has been proposed. Regarding Recital 69 - Theoretically we support, but in practice this point could be difficult to apply in cases where the payer is tricked into entering his data in authentication tool (for example, Smart-ID) or accept the payment transaction by himself LU (MS reply): OK. LT (MS reply): There are no clear and justifiable reasons as to why para. 2 of Article 49 was moved to Recitals. We would like to emphasize that the question of authorisation and its clear delineation that is free from ambiguities is of paramount importance not only for PSUs protection but also for fraud prevention itself. Ambiguities and obscurities leave the door open for misinterpretations and/or interpretations of the text that are disadvantageous to PSUs, hence, give no incentive to invest more in effective prevention in the first place to eliminate the risk of liability burden. Also, notions in Recitals do not have the same legal effect as notions in the legal text itself. Although mutual agreements on the definition might hard to reach, the final decisions should not be rushed in as it will predetermine the future of regulatory framework for fraud prevention in payment services and the level of consumer protection. If the legal text of Article 49 is not altered to make the clear delineation of authorised-unauthorised payment transaction, PSPs who follow only the narrow formal approach towards this question, will continue this practice even after PSR comes into force. We are in favor of Option 1 as proposed in discussion note for the 21 February CWP and the definition of authorisation should remain in Article 49. IT

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	(MS reply): IT.We support the clarification in R(69a) regarding cases where a payment order is modified by a third party. In our view, the Presidency's proposal helps to clarify the distinction between authorised and unauthorised transactions. However, we have the following observations. In our understanding, the scopes of Art. 49 and of Art. 59 are complementary: either Art. 49 applies or Art. 59 applies, but not both. As pointed out before, Option 1 was not our preferred course of action, because, from an Italian perspective: (i) On the one hand, it could lead to a partial regression in the PSU's protection, in certain cases where the PSU initiates the transaction directly, but is mistaken about the consequences of its actions, due to the fraud of a third party (who is not impersonating a PSP and therefore Art. 59 does not apply). See for example scenario 4 of the DE non-paper. (ii) On the other hand, art. 59 could extend the PSP's liability to certain frauds related to the "underlying reasons" of the transaction (for example, if the fraudster pretends to be the PSP to offer the PSU a fake investment). However, in our view, the Presidency's proposal, from a practical point of view, is an acceptable step forward, as it clarifies how the most common scenario (i.e. the fraudster obtains the PSU's credentials) should be handled. Moreover, it moves away from the strictest interpretation of the "objective theory" (whereby "authorization" equals to "authentication") toward a more balanced approach. We highlight that Art. 49(7) allows the PSU to withdraw consent for a payment transaction "at any time". This provision is not aligned with Art. 66 (Irrevocability of a payment order). Following the current art. 64(3) PSD2, we propose the following wording for Art. 49(7): "*7. The payment service*

Question	MS reply
	user may withdraw consent ~~*permission*~~ *to execute a payment transaction or to access a payment account for the purpose of payment initiation services*, ***at any time but no later than at the moment of irrevocability in accordance with Article 66. The payment service user may withdraw consent to access a payment account for the purpose of*** ~~***or***~~ *account information services* ~~***may be withdrawn by the payment service user***~~ *at any time. The payment service user may also withdraw consent permission to execute a series of payment transactions, in which case any future payment transaction shall be considered to be unauthorised.*". Finally, we strongly reiterate the need to introduce **clearer procedural rules** for PSPs when assessing PSUs' refund request. Currently, Article 56 only addresses cases where the payer is suspected of fraud and does not cover other possible (and far more common) reasons for refusing reimbursement of an unauthorized transaction, such as "gross negligence". In other words, Article 56 does not talk with Article 60. For the sake of clarity, we underline that in our national experience (and thus not under a strictly "objective" approach), Art. 73 and Art. 74 PSD2 have led to a situation where the PSP refunds, within one business day, the full amount, but such refund is made "under reserve" ("salvo buon fine"). At a later stage (sometime after months) the PSP debits the PSU again, if it concludes (unilaterally) that there has been gross negligence on the part of the PSU. (After that, the PSU is free to bring the matter to the Courts or to an ADR scheme). This approach is consistent with the European Commission's response to Q&A No. 223 here (albeit in the context of PSD1). Due to this lack of clear rules, a preliminary reference has been raised by a Polish Court (C-70/25 [Tukowiecka]) regarding the interpretation of Art. 73 and 74 PSD2. The key question is whether a PSP may refuse the reimbursement of an unauthorized transaction on the grounds that the PSU was grossly negligent or – as proposed by the national court – whether the

Question	MS reply
	PSP must first reimburse the PSU and then refer the matter to a court. If the national court's interpretation were to be upheld by the CJEU, it could have an extremely significant impact on the application of the PSD2 across multiple MSs, where the PSP can debit the PSU again if "gross negligence" is established at a later stage. **The existence of such widely divergent interpretations on an issue with significant implications for the implementation of PSD2 (a decade after its adoption) clearly highlights the need for a more detailed and coherent legal framework**. This need is even more pressing given the innovations that the PSR will introduce. In our view, **it is essential that the PSR clarifies that PSPs are able to independently assess whether the PSU was grossly negligent and, on that basis, deny the refund request**. If PSPs were required to refund the PSU at T+1 (except when there is a suspicion of fraud by the PSU, which is and should be a very rare occurrence) but were then unable to recover the funds in case of gross negligence, unless they initiated court proceedings (which would be economically unfeasible for low value transactions and on such a massive scale), the resulting framework would be quite dysfunctional. In practice, the substantive rules governing the PSU's liability would be unenforceable. While the proposed approach may be seen as less PSU-friendly, we believe that there are important counterbalances, including: the role of the NCAs, which are required to monitor the PSPs' complaint resolution procedures (art. 94); the PSU ability to refer disputes to an ADR body (art. 95), a faster and more cost-effective remedy; the fact that the burden of proof falls on the PSP in any case. To achieve these objectives, we believe there are two main approaches that could be considered: 1. **Proposal 1 - T+1 only for non-compliance with SCA**: one

Question	MS reply
	approach would be to recognize that the T+1 rule is better suited for a stricter application of "objective theory", which requires simpler and more automatable controls (roughly, compliance with SCA). Under a non-strictly objective approach, the PSP should have time to make a more complex assessments of the relevant circumstances. Accordingly, the T+1 rule could be limited to cases where SCA was not applied. 2. **Proposal 2 - T+1 plus reclaim by the PSP:** another approach would be to maintain the T+1 rule, in order to ensure that the reimbursement is prompt and to prevent PSPs from using the time needed to collect and assess information as a means to delay (or effectively deny) the refund. However, if the T+1 rule is retained, it should be made clear that the PSP has the right to debit the payer's account again in cases where it subsequently determines that the refund was unjustified. Find our proposals below, with the changes from the original EC proposal highlighted. We remain fully open to discussing alternative suggestions. ***PROPOSAL 1* - T+1 only for non-compliance with SCA** *Article 56* ***Payment service provider's liability for unauthorised payment transactions*** 1. Without prejudice to Article 54, in the case of an unauthorised payment transaction: (a) **if payer's payment service provider has failed to fulfil the obligation to require strong customer authentication set out in Article 85 or an exemption from the application of strong customer authentication has been applied**, the payer's payment service provider shall refund the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the unauthorised

PUBLIC

Question	MS reply
	transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud committed by the payer and communicates those grounds to the relevant national authority in writing; (b) **unless it has refunded the payer according to point (a), the payer's payment service provider, within XX business days after noting or being notified of the unauthorised transaction, shall refund the payer the amount of the unauthorised payment transaction 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, 91, 93, 94 and 95 if the payer does not accept the justification provided.** 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:~~ ~~(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;~~ ~~(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.~~ 3. **[NO CHANGE]** 4. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund**, in accordance with paragraph 1,** ~~immediately, and in any event no later than by the end of the following business day,~~ the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. 5. **[NO CHANGE]** 6. **[NO CHANGE]**

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	PROPOSAL 2 **- T+1 plus reclaim by the PSP** *Article 56* ***Payment service provider's liability for unauthorised payment transactions*** 1. Without prejudice to Article 54, in the case of an unauthorised payment transaction, the payer's payment service provider shall refund the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the unauthorised transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud committed by the payer and communicates those grounds to the relevant national authority in writing. 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 **XX** ~~10~~ business days 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; (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. **2a. If the payer's payment service provider has refunded the payer in accordance with paragraph 1, and subsequently obtains evidence, pursuant to Article 55, that that the payment transaction was authorised by the payer, or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52, or that any other reasons exist for the payer to be held liable for the payment transaction, the payer's payment service provider can recover from the payer the amount refunded and, where applicable, debit that amount**

PUBLIC

Question	MS reply
	directly from the payer's payment account, no later than XX business days after the refund took place. **The payment service provider shall provide to the payer, on a durable medium, a justification for its decision 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.** 3. **[NO CHANGE]** 4. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund, **in accordance with paragraph 1 and without prejudice to paragraph 2a,** ~~immediately, and in any event no later than by the end of the following business day,~~ the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. 5. **[NO CHANGE]** 6. **[NO CHANGE]** IE (MS reply): See below. HR (MS reply): We express our support for the direction of this proposal based on option 1. FR (MS reply):

PUBLIC

Question	MS reply
	We don't oppose to the drafting but it should be made very clear in Article 49 PSR that a payment transaction subject to SCA shouldn't be deemed authorised by nature. In Recital 69a, we find important to keep a reference to manipulation fraud in relation to the definition of authorisation. We propose to insert a drafting suggestion in Recital 69a. (69a) Authorisation is based on an intention or a contribution in fact. If the payment service user uses its security credentials in a responsible manner when executing a payment transaction, the validity and authenticity of the authorisation will be easier to assess. The set of payment transactions can be divided into two distinct categories, those that are considered authorised and those that are not, called unauthorised. The payment transaction operates as a process and requires the active participation and approval of the payment service user. A payment transaction or a series of payment transactions should be assessed as authorised only if the payer has given its consent for the execution of the payment transaction in a manner agreed on between the payer and the account servicing payment service provider. It should not be deemed to be authorised where the transaction was initiated or modified by a third party

Question	MS reply
	who is acting without the consent of the payment service user, ***or by a third party who manipulated it***, e.g. where the third party is using the personal security credentials of the payment service user fraudulently obtained, ***or under manipulation***. In Article 49(7) PSR, we reiterate that for matter of legal certainty, it should be precised that consent of the PSU to execute a payment transaction may be withdrawn by the payer at any time, "*but no later than the moment of irrevocability in accordance with Article 66 [PSR]*". This reference was in Article 64 (3) PSD2 and we see no reason to have a different drafting in Article 49(7) PSR. Otherwise, it would open the possibility for a PSU to withdraw its consent including after the moment of irrevocability of the payment order, which would lead to significant difficulties and increased legal uncertainty. FI (MS reply): FI: Although we would have preferred defining transactions in which PSUs have the right to refund through a general provision, we think the provision and the recital are heading in the right direction. We support clarifying that payment transactions fraudulently initiated or modified by a third party should be deemed as unauthorised.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	EL (MS reply): **EL:** We agree with the drafting suggestion in recital 69a and in Article 49 as they capture Option 1 of the Presidency's suggestions and at the same time clarifying that scams conducted after altering a payment order (i.e. through means of man-in-the-middle/browser) shall be considered unauthorized. In order for a transaction to be considered authorized, it needs to be both initiated and authenticated by the payer.
Q1.1. Do Member States agree to replace the word 'modified' with the phrase 'carried out' in Recital 69a, as proposed during the CWP meeting?	DK (MS reply): We do not agree. Modified catches the situation where a PSU has authorised a payment but the payment is modified (e.g. the amount is increased) by the fraudster. "Caried out" would basically mean the same as initiated. DE (MS reply): We suggest to replace the entire wording "initiated or modified" by "carried out" as "to carry out" already includes the initiation. CZ (MS reply):

PUBLIC

Question	MS reply
	CZ shares the view that the reference to "transaction was modified" in the recital 69a is misleading. However, we cannot support the wording "transaction was initiated or modified carried out by a third party who is acting without the consent…" as the transaction is executed (carried out) in any case (authorized or not) by PSP not by fraudster. We prefer deleting the word "modified". Moreover, the issue of "man-in-the-middle" is partially covered by Article 60 (1) PSR: the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment. CY (MS reply): We agree to replace the word 'modified' with the phrase 'carried out' in Recital 69a. BG (MS reply): We agree with the proposal to replace the word 'modified' with the phrase 'carried out' in Recital 69a. BE (MS reply): BE: we are not sure what "modified" means in this proposal. During the CWP, we suggested to add some examples of what should be mean by

PUBLIC

Question	MS reply
	"where the transaction was initiated or *modified* by a third party who is acting without the consent of the payment service user". But we can also support the replacement of the word "modified" by "carried out". AT (MS reply): **AT**: Regarding Recital 69a, we ask to replace the words "**initiated or modified**" by the words "**carried out**". ES (MS reply): yes SK (MS reply): We support the replacement. SI (MS reply): Yes. SE (MS reply):

Question	MS reply
	No, we support 'modified'. Cases where the payment transaction has been altered along the way should be deemed as unauthorised. 'Carried out' would narrow the scope even further in an unacceptable way. PT (MS reply): PT does not oppose the suggested replacement. NL (MS reply): Yes. LV (MS reply): We agree. LU (MS reply): We have a preference to replace "initiated or modified" by "carried out" to ensure legal clarity of the text. LT (MS reply): Yes. IT (MS reply): IT.We would prefer the word "modified".

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	IE (MS reply): We support replacing the words “initiated or modified” by “carried out” because the current wording blurs the line between authorised and unauthorised payment transactions, and we prefer a well-defined, clear and balanced authorisation concept. HR (MS reply): We do not agree with the addition of the text "or modified" nor with replacing it with the phrase "carried out" in the context of the unauthorised payment transaction in recital 69a because it brings ambiguity in the distinction between authorised and unauthorised transactions. We agree with the text presented in the previous proposal for WP held on 21 February stipulating that the transaction shall not be deemed as authorised where it was initiated by a third party using the personal security credentials of the payment service user fraudulently obtained. FR (MS reply): The word “*modified”* is ambiguous. We struggle to find to which cases it would be applicable. FI

PUBLIC

Question	MS reply
	(MS reply): FI: No. We prefer the use of the word 'modified'. We understand this expression as referring to, for example, cases where the fraudster, during the initiation phase, modifies the payment order by changing the name of the payee. Such cases would not necessarily always be 'initiated' *per se* (as per the definition under Article 3(6) PSR) by a third party although in principle they should be treated similarly to cases where the fraudster initiates the transaction. EL (MS reply): EL: We agree
Q1.2. Do Member States agree that paragraph 2 of Article 49 PSR should be retained (and not moved to Recital 69a)?	DE (MS reply): GER prefers the current proposal with Art. 49(2) being deleted and transferred to Rec. 69a PSR, especially since the Rec. contains a clarifying example. At the same time, if a majority of MS opts for a retention of para. 2 in Art. 49, GER could show flexibility. In that case, the same as with the wording in Rec. 69a applies: the wording "initiated or modified" would have to be replaced by "carried out". CZ (MS reply):

PUBLIC

Question	MS reply
	We disagree, we want to keep it in the recital. CY (MS reply): We do not object retaining paragraph 2 under Article 49 PSR. BG (MS reply): We believe that paragraph 2 should remain as part of Recital 69a. BE (MS reply): BE: see Q1. We believe that a second paragraph should be included in Article 49, stating that a payment transaction shall not be deemed as authorised where the transaction was carried out by a third party who is acting without the consent of the payment service user. AT (MS reply): **AT**: We agree with the PCY's proposal to move Art 49 (2) PSR to Recital 69a. ES (MS reply): *yes*

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	SK (MS reply): We prefer the movement to the Recital. SI (MS reply): Yes, we strongly agree. SE (MS reply): Yes, this is an important clarification that should be expressed in the article. PT (MS reply): As stated in Q1, PT wishes to retain Article 49(2), which clearly highlighted that a payment transaction shall not be deemed as authorised where the transaction was initiated by a 3rd party using the personal security credentials of the PSU fraudulently obtained. In our view, a sole reference in a Recital lacks the appropriate legal safeguarding the provision should carry, especially, taking into consideration, that it embodies a change in approach of the current PSD2 framework. Moreover, we deem it worthwhile to underscore this specific reference following the general conditions described in Article 49(1).

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	NL (MS reply): Yes. LV (MS reply): We agree. LU (MS reply): We have a preference to keep the wording in recital 69a. If the wording were to be removed to para 2 of article 49 PSR, it would be all the more important to replace “initiated or modified” by “carried out”. (cf previous comment). LT (MS reply): We are strongly in favor of retaining paragraph 2 of Article 49 PSR and not moving to Recitals. IT (MS reply): IT.We have no strong opinion on the issue. IE (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We agree that paragraph 2 of Article 49 PSR should be retained and not moved to recital 69a. HR (MS reply): We do not consider it necessary to retain paragraph 2 in Article 49 so we support the Presidency's proposal to move that text in Recital 69a. FR (MS reply): We would be fine with maintaining Article 49 (2) PSR and not deleting it. FI (MS reply): FI: Yes. EL (MS reply): EL: We consider that par. 2 of Article 49 should be retained.
Q2. Could Member States accept the wording of Recitals 79 and 80a and Article 59(1) PSR or would Member States be in favour of referring to bank employee impersonation fraud in more general terms, without specifying different elements of fraud?	DK (MS reply): We would support referring to bank employee impersonation fraud in more general terms. Although it may not be clear to us how to do this, one could imagine fraud that could be considered bank impersonation fraud which did not use the channels mentioned.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	DE (MS reply): GER is open as to the proposed changes to bank employee impersonation fraud in Rec. 79, 80a/ Art. 59 PSR: - While we support the requirement of only one element of deception, we would also be open to describe bank employee impersonation fraud in more general terms to further render the PSR future-proof. - We further support changing "without any delay" to "without undue delay". - We would also be open to the other changes made in Art. 59, including the PSU's obligation to provide information that should now be triggered only when and insofar the PSP demands the information. CZ (MS reply): **While we still propose to delete Article 59 completely**; **we do not agree with the use of the *mobile app and website* in the new proposal**. The principle of this article is that when fraudsters impersonate PSPs, and the PSU make authorised transaction, because he/she is manipulated. But how this could be done with mobile app and website? If fraudsters use fake website or fake mobile app and steal PSU credentials, this will be unauthorised transaction and it is not covered by Article 59. For real websites or real mobile apps, there is no impersonation. CY

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): We do not oppose the proposed wording of Recitals 79 and 80a. We are open to further explore cases where a consumer is manipulated by a third party pretending to be an employee of the PSU's PSP, using a name, email address, telephone number of the person pretending to be a bank employee, which may slightly differ from the original version of the name/email/telephone number due to impersonation evolving over time. BG (MS reply): We agree with the Presidency's proposed wording in Recitals 79 and 80a and in Article 59 PSR. BE (MS reply): BE: Regarding Article 59, we understand the need to strike a right balance between the consumer protection and the PSP's liability. However, given the approach chosen in Article 49, we see a need to strengthen the consumer protection offered in Article 59. We advocate for a extension of the scope of Article 59 to other impersonation frauds, at least to fraud where the fraudster pretend to be acting on behalf of a public entity or

PUBLIC

Question	MS reply
	(national) authority. Consumers are particularly vulnerable to a threat that appears to emanate from a public authority. This type of impersonation fraud undermines public confidence in public institutions, and involves significant financial losses. Some Member States argued that PSPs should not have to bear such liability because they cannot prevent such frauds and do not have any control over it. However, we underline that PSPs should have in place robust fraud prevention mechanisms. In this sense, PSPs have a certain power of action and should therefore bear a liability where they fail to fulfil their obligations to have strong fraud prevention mechanisms in place in accordance with PSR. Regarding the Presidency drafting suggestion on the elements of bank-employee impersonation fraud, we agree. Given the approach chosen in Article 49, we are ready to consider amendments aimed at extending the scope of Article 59. Regarding the option of specifying or not the elements of bank-employee impersonation fraud, it could be considered to make the reference to bank-employee impersonation fraud in general terms in Article 59 and to have the different elements as examples in a recital. In this sense, we could prevent the risk of confusion and the provision would be futureproof.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	AT (MS reply): **AT**: We **do not** support the extension of the scope of Art 59 (1) **to websites and mobile applications** (as stipulated in Art 59 (1) and Recitals 79 and 80a). The reason is that this extension concern scenarios in which PSPs have no control over misuse of communication elements. We support the obligation for consumers to provide supporting evidence. However, the information that "can be reasonably expected" from the user should be clarified. ES (MS reply): From the start, ES has been in favour of exploring the recognition of going beyond bank impersonation to other types of impersonation, provided these are directly linked to a payment transaction, with the double objective of, on one side, improving , consumer protection, and on the other side, enhance cooperation between PSPs and Telcos As regards whether bank impersonation should be drafted in a more generic way than that proposed by the presidency, we deem this would be very difficult to implement in practice, provide legal uncertainty and would lead to numerous litigation cases. Following this we consider that the amendments made by the

Question	MS reply
	presidency under Article 59 (including website and mobile application of the bank and not requiring both the name and telephone of the PSP in order to be considered bank impersonation) are adequate and sufficient. SK (MS reply): We support the wording in general, however the sentence I very long and simplification would be welcomed. Using the name of PSP should not be enough to be stipulate bank employee fraud. Name should be used in combination with e-mail address or phone number. We would prefer to be more general on the possible communication channels that can be used as there may be other chat functions or future solutions. SI (MS reply): In general, we agree with the approach taken. We would, however, like to repeat our suggestion to replace the term "consumer" with a boarder term "payment service user" to offer equal protection to both natural and legal persons. Our concern are in particular natural persons performing business activities as well as small enterprises, as we have seen from practical experience that also these are vulnerable to bank impersonation fraud. Furthermore, any legal entity can fall victim to bank impersonation fraud.

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	SE (MS reply): We would prefer referring to bank employee impersonation fraud in article 59 in more general terms, in order to future proof the provision. In general, we would prefer to widen the scope of article 59 to other types of impersonation fraud. We can however accept the current scope for the sake of compromise, **but we are <u>not</u> willing to accept a narrower scope than this**. It is therefore imperative that the current wording 'or' is kept when listing different elements of impersonation fraud, instead of using 'and'. Furthermore, we welcome the amendments to the requirements on PSUs to inform the PSP of fraud 'without undue delay', 'upon request' and 'when becoming aware of the fraud'. We strongly support these amendments. PT (MS reply): PT tends to favour a precise approach specifying the different elements of fraud that should be accounted for to trigger the liability shift. This enhanced predictability and certainty avoids excessive negative spillovers on PSP's activity relating with a broader, and more subjective interpretation of this shift, that could stimulate over recurrence.

PUBLIC

Question	MS reply
	However, we disagree with the new suggestion of reverting back to the sole appropriation of the PSP's name to guarantee a liability shift. In our view, this appears to create a difficult and unbalanced expectation for PSP to effectively mitigate such cases, considering the easiness for fraudsters to refer solely to the name of the PSP in an attack. Please consider the following adjustment to Article 59(1), which should also be extended to Recitals 79 and 80a: *"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* ***accompanied by either the*** ~~***or***~~ *e-mail address,* ~~***or***~~ *telephone number,* ~~***or***~~ *website or mobile application of that payment service provider unlawfully and that manipulation gave rise (...)"* Moreover, we understand that the Council is interpreting the mention to the impersonation of the PSP's website or mobile application to include, besides the actual ones provided by the PSP, also the "fake" ones, created by fraudsters to mirror the real channels. To fully specify this is the case, we would welcome the introduction of a clarification in Recital 80a. Please consider the following adjustment: *"(80a) Cases of bank employee impersonation (spoofing) fraud affect the good repute of the bank financial entity, of the banking financial sector as a whole and may cause significant financial damages to Union consumers,*

PUBLIC

Question	MS reply
	affecting their trust in electronic payments and in the banking financial system. A good-faith consumer who has been the victim of such manipulated transactions, namely 'spoofing' fraud where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name ***accompanied by either the*** ~~,~~ *e-mail address, telephone number, website or mobile application should therefore be entitled to a refund of the full amount of the fraudulent payment transaction from the payment service provider on a shared-damage basis, unless the payer has acted fraudulently or with 'gross negligence'.* ***When concerning the payment service provider's website or mobile application, the refund right shall encompass both an appropriation of these channels by the fraudster, as well as fraudulently created versions of the website or mobile application that mirror the contents of the real ones.*** *As soon as the consumer becomes aware that he or she has been a victim of that type of spoofing fraud manipulation (...)"* NL (MS reply): We suggest adding the following words to Recital 79:

PUBLIC

Question	MS reply
	"This includes not only the situation in which the third party uses the name and the actual website/email address/telephone number/application of the consumer's payment service provider, but also the situation in which the third party uses the name and a website/email address/telephone number/application that is similar to that of the consumer's payment service provider." • The current wording makes it seem that is has to be the actual website etc. which is rarely the case in fraud cases. As for recital 80a and Article 59, we still have some comments: • The phrase "and provide the payment service provider with all the relevant information requested by the payment service provider and that the payment service user can reasonably be expected to have regarding the events leading to the disputed payment transaction, providing supporting evidence" sets the bar too high, as it may provide PSPs with the opportunity to request great sets of information that the PSU is unable to provide. We therefore suggest the following wording: "and provide the payment service provider with all the relevant requested information insofar as the payment service user can reasonably be expected to have such information, considering the events leading to the disputed payment transaction".

PUBLIC

Question	MS reply
	• Furthermore, in Article 59, we believe it can be clarified that once the PSU has become aware of the fraud, the obligation to report the fraud without undue delay comes into existence (and not the other way around). This can be clarified by changing the wording of the phrase as follows: "under the condition that the payment service user, when becoming aware of the fraud, reports the fraud without undue delay to the police and its payment service provider." • We also want to delete the part that says that reporting the incident to the police should preferably be done via online complaint procedures, because it is not consumer friendly, especially taken into account that fraudsters often target the elderly. LV (MS reply): We could support a broad scope of liability to target fake websites for example. LU (MS reply): We could accept the proposed wording by the PRES with one change: the criteria of the name of the consumer should always be combined with any of the other criteria listed in article 59(1). A cumulative combination of the

Question	MS reply
	name and any other criteria is to ensure a more balanced approach in terms of incentive structure and liability between PSPs and PSUs. If a more general wording were to be introduced in part 59(1), the legal text would become less clear on PSP liability. Some redrafting of the recitals would then be warranted, especially by introducing the concept of cumulation of two criteria as a necessary condition. (cf comment in previous para). LT (MS reply): We accept. IT (MS reply): IT.In our view, the difficulties underlying the question stem from the fact that Article 59 seeks to regulate a specific type of fraud (an inherently complex and evolving challenge). A definition that is too narrow may fail to adequately protect the PSU and quickly become obsolete, while a definition that is too broad could impose liability on the PSP even in cases where such protection is unwarranted. This is one of the reasons we opposed Article 59. The proposal that merely using the PSP's "name" should be sufficient to trigger the application of Article 59 is a prime example of this challenge. In some cases, the mere use of the name may indeed deceive the PSU. However, we understand that Article 59 is intended to address more sophisticated forms of "spoofing" fraud, where the fraudster creates a highly convincing illusion by exploiting specific technological features of the communication channels. We see two possible solutions:

Question	MS reply
	A) We could clearly define the elements of the fraud to limit its scope only to particularly insidious cases. Under this approach, merely using the PSP's "name" would not be sufficient to trigger PSP liability. However, this approach risks becoming obsolete as new forms of fraud emerge. Even specifying "bank *employee* impersonation" may quickly become outdated. What if, for example, a fraudster convinces the PSU that he/she is interacting with an AI-powered banking chatbot rather than a human employee? **B)** Alternatively, we could refer to "bank impersonation fraud" in broader terms, without specifying the means or the channels used by the fraudster. This would expand the scope of Art. 59. However, the concept of "gross negligence" should serve as a safeguard against excessive PSP's liability. To this end, we should make clear that the fraudster's methods are relevant when assessing the PSU's gross negligence. For example, if the fraudster only uses the PSP's name without any additional elements to enhance credibility, the PSU should almost always be deemed grossly negligent. All thing considered, perhaps the second is the preferable and more future-proof option. Having said that, we still have several concerns regarding Article 59: - We understand that Art. 59 aims to protect the "good repute of the bank" and "trust in electronic payments" (R80a). However, there are similar fraudulent scenarios that fall outside its scope. For example, the fraudster pretends to be a policeman and convinces the PSU to move its fund to an account for "security" reasons. - We are unsure about excluding PSUs who are not consumers. In all other cases, the PSR guarantees the same default level of protection to both consumers and non-consumers. Article 27 already allows that, when the PSU is not a consumer, the PSU and the PSP may agree to exclude certain provisions on the PSP's liability. Given the

PUBLIC

Question	MS reply
	stated aim of Article 59 (see Recital 80a) and the fact that enterprises are also frequently targeted by bank impersonation fraud, we see no clear justification for excluding non-consumers from the scope of Article 59. - The application of Art. 59 is unclear in many cases: - what if the the consumer holds accounts with multiple PSPs? - what if the impersonation occurs through channels not covered by Art. 59? - what if the fraudster uses a name very similar, but not identical, to that of the PSP, or a convincing abbreviation different from the commonly used one? The same concern applies to email addresses, telephone numbers, websites, etc. that closely resemble, but do not exactly match, those of the PSP. Would such cases fall within the scope of Article 59, or would they be excluded based on a strict interpretation? This ambiguity raises concerns about potential loopholes. We are not sure that such distinctions should determine whether a "fraudulent authorized" transaction is deemed worthy of protection. Moreover, Art. 59 could potentially be used to extend the PSP's liability to certain cases of fraud on the "underlying reasons"/ APP fraud, a result we do not support. For example, fake investment scams. We could therefore clarify, for example in a Recital, that if the PSU knowingly authorizes a payment transaction but is mistaken about the underlying circumstances of the payment (whether due to fraud or not), the transaction should still be considered authorised, even in case of impersonation fraud. Regarding the proposed Recital (80a) we would like to clarify the following points: - The Recital refers to "*a shared-damage basis, unless the payer has acted fraudulently or with gross negligence*". In our understanding, Art. 59 stipulates that liability for "fraudulent authorized transactions" falls either on the PSP or the PSU, depending on the

Question	MS reply
	circumstances. We do not see any "shared damages" in this context; - the Recital concludes with the following statement: "*Without prejudice to the right of customers to bring action in courts, the rules of refunds based on shared compensation between the payer and the payment service provider can only be considered as a temporary (preliminary) way*". If the purpose of this statement is to clarify that the final decision on the liability rests with the Courts (if the matter is brought before them), we think that the reference to a "temporary (preliminary) way" could be misleading. First, this clarification is superfluous, as it applies to any dispute between a PSP and a PSU. Also, the refund should be considered definitive, unless it is contested by either party. Find below our **drafting proposal for Art. 59**. We suggest the following amendments: - adding the phrase "*Without prejudice to Article 56* […]" to further clarify the relationship between the two articles; - extending the scope to include all payers, not just consumers; - referring to "bank impersonation fraud" in broader terms, for the reasons outlined above; - amending paragraph (2)(b) to reflect that the PSP may refuse a refund for reasons other than fraud or gross negligence (e.g., if the payer has not reported the fraud to the police). We also propose adding the following at the end of the proposed Recital (80a), for the reasons outlined above: "*However, the payment service provider should not be held liable when the fraud concerns the underlying purpose of the payment transaction, for example when a fraudster, posing as a bank employee, convinces the customer to transfer large sums of money for a non-existent investment opportunity*".

Question	MS reply
	We remain fully open to discussing alternative suggestions. **Article 59 [Payment service provider's liability for impersonation fraud]** 1. **Without prejudice to Article 56, w~~W~~**here a payment services user **~~who is a consumer~~** was manipulated by a third party pretending to be **~~an employee of~~** the **payment services user~~ consumer~~**'s payment service provider **~~using the name and/or e-mail address or name and telephone number or website or mobile application of that payment service provider unlawfully~~** and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the **payer~~ consumer~~** the full amount of the fraudulent authorised payment transaction under the condition that the **payer~~ consumer~~** has, without undue ~~any~~ delay, reported the fraud to the police and notified its payment service provider when becoming aware of the fraud, providing the payment service provider with all the relevant information requested by the payment service provider and that the payment service user can reasonably be expected to have regarding the events leading to the disputed payment transaction ~~providing supporting evidence available to the consumer~~. 2. Within **XX~~10~~** business days after noting or being notified of the fraudulent authorised payment transaction, the payment service provider shall do either of the following: (a) refund the **payer~~ consumer~~** the amount of the fraudulent authorised payment transaction; (b) **~~where the payment service provider has reasonable grounds to suspect a fraud or a gross negligence by the consumer,~~** provide a justification for refusing the refund and indicate to the consumer the bodies to which the consumer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the consumer

Question	MS reply
	does not accept the reasons provided. 3. Paragraph 1 shall not apply if the **payer** ~~**consumer**~~ has acted fraudulently**, with intent** or with gross negligence. 4. The burden shall be on the payment service provider of the consumer to prove that the **payer** ~~**consumer**~~ acted fraudulently**,** ~~**or**~~ with **intent or with** gross negligence. 5. **[duty of cooperation for ECSPs] [moved to the proposed Art. 59a] […]** IE (MS reply): The use of a name only is not sufficient to hold a PSP liable for the fraud and oblige it to refund the consumer the full amount of the fraudulent transaction. HR (MS reply): We do not agree with the proposal for Article 59(1) to revert to only one of the given elements in the fraud to be considered as bank employee impersonation fraud. In our opinion, it is not sufficient to hold the PSP liable for the fraud where fraudster uses only the PSP's name because we believe that there is no possibility for the PSP to take any preventive measure in such a case. In practice it is possible that the fraudster calls a PSU saying that he or she is a bank employee, so using just PSP's name without combining it with the other element should not be sufficient. FR

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): The wording of Article 59(1) PSR is too favorable for the PSP in our view, when specifying "*all relevant information requested*" as it could give leeway to divergent approaches. That's why we would like to delete such mention. 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 ~~and~~ or e-mail address or ~~name and~~ telephone number or website or mobile application 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 undue ~~any~~ delay, reported the fraud to the police and notified its payment service provider when becoming aware of the fraud, providing the payment service provider with all the relevant information ~~***requested by the payment service provider and that***~~ the payment service user can reasonably be expected to have regarding the events leading to the disputed payment transaction ~~providing supporting evidence available to the consumer.~~ FI (MS reply): FI: We support the suggested amendment of "without *any* delay" to "without *undue* delay" and only requiring the PSU to provide the PSP with

PUBLIC

Question	MS reply
	such information that it can reasonably be expected to have under Article 59(1). Although we also support other amendments suggested under Article 59(1), we are not entirely sure whether ***fake*** websites and mobile applications would be within the scope of the current wording, even though the intention seems to be to include them. We would appreciate clarification on this in the text. One way to tackle this issue, which we could also support, would be to refer to bank employee impersonation fraud in more general terms. EL (MS reply): **EL:** Yes we agree with the drafting suggestions in recitals 79 and 80a of as they reflect points we proposed in earlier rounds of comments . For article 59(1), we agree with the drafting modifications to include "website or mobile application" in order to make clear that this type of fraud is related to PSP impersonation when the user is scammed by means of spoofing.
Q3. Would Member States be in favour of shifting the obligation to report fraud to the police from the PSU to the PSP?	DK (MS reply): While we realise we are in the minority, we think there could be some merit in shifting the obligation to the PSP, which is the professional part, and which can see fraud

PUBLIC

Question	MS reply
	patterns and connections between various frauds that the PSU can-not. We remain unconvinced that there should be a commitment to report to the police in all cases. We believe there could be instances, where this would only lead to administrative burdens on both sides, but where the police is unable (due to resources or other constraints) to act on the report. In this case, it could be added "where deemed relevant by the PSP. DE (MS reply): We do not support shifting the obligation to report fraud to the police onto the PSPs for several reasons: - As the PSU is the victim of the fraud, the PSU is in possession of all relevant information and therefore better equipped to report the fraud to the police. - Furthermore, an obligation to report the fraud to the police might prevent a dishonest claim for compensation on the part of the PSU as it is a higher burden to make a false report to the police. CZ (MS reply):

Question	MS reply
	No, we do not agree with shifting the obligation to PSP it up to payer decide if the matter should be dealt by the police and in relevant cases banks are already obliged to do so by national law. CY (MS reply): We are of the view that the obligation to report fraud to the police by the PSU should not shift to the PSP. We would be open to exploring the possibility of requiring PSPs to assist PSUs and to inform PSUs of their obligation to report such fraud to the police. BG (MS reply): We are not in favour of shifting the obligation to report fraud to the police from the PSU to the PSP. BE (MS reply): BE: we do not have a strong position but we can see a logic in shifting the obligation from the PSU to the PSP since it relates to PSP's identity impersonation. Moreover, according to Article 59, it is for the PSP to bear

Question	MS reply
	the financial losses and, if any, to attempt to recover the funds. Therefore, we can support the shift of the obligation from the PSU to the PSP. AT (MS reply): **AT**: No, we do not support shifting of the obligation to report fraud to the police from the user to the service provider. As explained by the Commission in the CWP on 4. April 2025 such a shift could be unsound from a legal perspective. We could show some openness towards an obligation of the PSPs to help the PSU to provide the required evidence as suggested by several MS in the CWP. ES (MS reply): No, we deem essential that the requirements to all parties are balanced, and PSUs should act diligently when dealing with fraud. Reporting to the police is a preventive measure that should be on the side of the PSU. SK (MS reply): We believe the reporting obligation should not be a precondition for the claim. If maintained, then obligation should stay with PSU. SI

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): We would not be in favour of shifting the obligation to report fraud to the police from the PSU to the PSP. As we mentioned in our previous response, we expect that the PSU will have at least some information to provide to the police (however, caution is needed here, as the provision could be too strict for the PSU). Transferring the responsibility of reporting fraud to the police on the PSP would also mean duplication of burden – first the PSU would have to gather all the relevant information and relay it to the PSP and than the PSP would have to forward the same information to the police. SE (MS reply): We find the proposal a bit far reaching. PSPs could perhaps be obliged to help PSUs report fraud to the police, especially vulnerable groups. PT (MS reply): PT disagrees with the option of transferring the obligation to report fraud to the police from the PSU to the PSP, given the legal challenges and complexity it appears to create. The PSU, being the fraud victim, is better positioned to fully report the case to the criminal authorities, but we do not oppose to the introduction of a duty to the PSP collaborate with the PSU to report fraud to the police.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	NL (MS reply): We are not in favour of shifting the obligation to report the fraud to the PSP. We think that this would be difficult to put into practice. However, to improve the position of the PSU, we suggest adding that the PSP should assist the PSU in reporting the fraud if needed. LV (MS reply): This could create an unnecessary burden for credit institutions, and there may be situations where both the bank and the victim report at the same time, which would create an administrative burden for the police to assess whether several cases are included in one situation. In our view, it should be maintained that the PSU itself makes the referral rather than the PSP doing so, the PSP only if the damage is caused by the PSU rather than it being a classic fraudulent transaction LU (MS reply): No.

PUBLIC

Question	MS reply
	However, in order to take into account financial inclusion concerns, we could be open to some wording that a PSP, on request of a PSU, could help a PSU in its obligation to report fraud to the police. LT (MS reply): No - in fact, shifting this obligation to the PSP might actually contradict the requirements laid down in criminal procedure laws stating that the victim of a certain offence or crime must report it to the police himself/herself to give police the legal basis for starting the investigation. IT (MS reply): IT.We strongly oppose the proposal to shift the obligation to report fraud to the police from the PSU to the PSP. As stated in previous rounds of comments, we were already unsure about introducing a general duty to report all frauds to the police, because it could be overly burdensome for both the PSU and the police, while offering little added value in most cases. However, we acknowledge that a reporting obligation (particularly in cases such as those covered by Article 59) could have certain advantages: (i) the PSU would be required to disclose the factual circumstances surrounding the fraud; (ii) reporting fraud to the police enhances credibility and seriousness, as making false statements to the police may constitute a criminal offense. This could encourage the PSU to provide a full and accurate account, reducing the risk of omitting details that might indicate gross negligence. These advantages would be lost if the obligation were shifted to the PSP.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	IE (MS reply): We are of the view that the obligation should be on PSUs to report fraud to the police. We would suggest some examples of "*all the relevant information*" within a Recital. HR (MS reply): We disagree with the proposal of shifting the obligation to report fraud to the police from the PSU to the PSP. We propose to keep the provision that obliges PSU to report the incident to the police, as such a requirement gives additional weight to the case and we believe that it can reduce the number of frauds committed by PSUs themselves. FR (MS reply): We would like to delete such obligation to report fraud to the police, whether it is carried out by the PSU or by the PSP. Reporting a fraud to police is not and should not be a matter of civil liability. Furthermore, it could pose significant difficulties for most vulnerable parts of the population. FI (MS reply):

PUBLIC

Question	MS reply
	FI: No. However, given that especially vulnerable consumers may have difficulties in reporting the fraud to the police in a timely manner, we suggest considering an obligation for the PSP to assist the PSU in the reporting. Furthermore, we suggest changing the order in Article 59 and recital 80a so that the PSU's obligation to notify its PSP is mentioned first, followed by the obligation to report the fraud to the police. This would better reflect the urgency of informing the PSP before reporting to the police. Nevertheless, whether the PSU first informs its PSP or reports the fraud to the police should not affect the PSU's right to refund. EL (MS reply): **EL:** We believe that the obligation to report fraud to the police should remain to the PSU as he/she has the information to claim a fraud. We propose that support by the PSP shall be required instead, in order to have a complete report including the sequence of events that led to fraud i.e. the registration of a device that only the PSP knows that took place and the PSU is not aware of.
Q4. Could Member States accept the wording of Article 60(1) PSR?	DK (MS reply): We support all the changes, including the addition of dispute resolution bodies in article 60(1).

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	DE (MS reply): In our view, it is systematically wrong to refer to the bodies that may reduce the aforementioned liability. Dispute resolution bodies, be it courts or ADR entities, base their decisions on the applicable law. If, therefore, the substantive law provides for a reduction in liability, courts and ADR entities will apply such a provision without a need for it being expressly stated within the substantive law. The same applies for national competent authorities. We would therefore suggest the following wording: "Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, ~~national competent authorities or dispute resolution bodies, in accordance with their requisite powers, or payment service providers may reduce~~ the liability referred to in this paragraph may be reduced, thereby taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated." CZ (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	Thank you for the amendment, but the wording "*national competent authorities or dispute resolution bodies, in accordance with their requisite powers*" seems not to be sufficient. In the Czech Republic, NCA does not resolve disputes between clients and PSP. There should be an option for MS if the power is with ADR or with NCA. Also the wording requisite powers – is legally incorrect. Our proposed wording is: In accordance with **their relevant powers**. For the sake of legal clarity, we would like to add this proposed explanation to the recital: "*Member States are free to choose whether the power to reduce liability under Article 60(1), last sub-paragraph, is given to court or out-of-court bodies or NCAs.*" CY (MS reply): We have no comments for the proposed wording of Article 60(1) PSR regarding the dispute resolution bodies. BG (MS reply): We agree with the Presidency's proposed wording in Article 60(1) PSR. BE (MS reply): BE: we agree AT

Question	MS reply
	(MS reply): **AT**: We could support it. However, as pointed out by one MS in the CWP on 4 April 2025 the reference to ADR bodies is not strictly necessary as there are already existing provisions which contain the required legal basis for ADR bodies to act. ES (MS reply): Yes, we agree to include dispute resolution bodies (courts and ADR bodies) among the entities empowered to reduce the liability of the payer. SK (MS reply): Yes. SI (MS reply): We could accept the wording of Article 60(1) PSR. SE (MS reply): Yes, given that we are going with option 1. PT

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): PT agrees. NL (MS reply): Yes. LV (MS reply): We support. LU (MS reply): Ok. LT (MS reply): We accept. IT (MS reply): IT.We agree with the proposed wording of Article 60(1). IE (MS reply): We can agree with the proposed wording. HR (MS reply):

PUBLIC

Question	MS reply
	We accept the proposed wording. FR (MS reply): The proposed wording of Article 60 (1) PSR is unclear to us ("requisite powers" of dispute resolution bodies). FI (MS reply): FI: Yes. EL (MS reply): **EL:** We agree with the wording of Article 60 (1) as we have already commented in the Consolidated tables with ddl 24/3.
Q5. Do Member States agree with the proposed drafting to Recital 82 PSR? If not, please provide an alternative wording.	DK (MS reply): We are still of the firm belief that gross negligence should be a question for courts. However, we can agree with the proposed drafting to Recital 82. DE (MS reply): We could agree to the proposed changes to gross negligence in Rec. 82.

PUBLIC

Question	MS reply
	We regret that the prohibition for PSPs to set off any claims stemming from the same payment transaction against the payer's claim for refund has been withdrawn. CZ (MS reply): We can support the proposal. We suggest some other examples of gross negligence that could be considered and potentially added to the recital. - Forwarding an activation SMS, handing over an activation code, handing over a smart device or USB token, card or SIM card, including electronics. - Handing over a PIN, handing over a password, forwarding or providing a QR activation code (including showing it at the camera). - Authorising a transaction despite clear warnings from the bank about the nature of the fraud before or during the transaction entry and authorisation (e.g, the customer insists on a transaction that the banker tells him is a fraudulent formula, or the customer is shown this information by the bank in the banking system prior to authorisation). - Providing or handing over an authentication device to an an-authorised third party.

Question	MS reply
	- Repeated frauds with the same characteristics (e.g, the client again grants remote access to fraudsters despite the bank's explanation and warning after the damage is done). CY (MS reply): We agree with not providing specific examples under Recital 82 PSR, as this runs the risk of a future restriction in terms of manoeuvre of ADR or courts. We would be open to exploring the possibility of providing non-exhaustive or not legally binding circumstances. BG (MS reply): We agree with the Presidency's proposed drafting to Recital 82 PSR. BE (MS reply): BE: we welcome the deletion of the examples. In our opinion, examples could weaken the case-by-case assessment of the gross negligence and the discretion of courts and ADR bodies. Although, we notice that even the example that was in the proposal of the Commission and in PSD2 has been deleted while this one did not involve any problem.

PUBLIC

Question	MS reply
	However, regarding the list of criteria, we are concerned about the new wording proposed by the Presidency, where the most criteria has been deleted. The objective is to provide some guidance in the assessment of the gross negligence, without prejudice to the case-by-case basis, and to have a minimum harmonisation in the use of the notion of gross negligence. We fear that the current proposal will now be so reduced that the impact will be insignificant. Having such criteria, like the characteristics of the PSU, in PSR should be seen as an incentive for PSPs to take into account all the personal circumstances when assessing the gross negligence. It would also enhance a more coherent approach throughout the EU. Moreover, in the newly proposed wording, it is no longer clear that criteria are not binding. We therefore suggest to reinstate at least the following sentence : “This list is not exhaustive and does not prejudice the discretion of national courts and/or ADR entities. The circumstances as mentioned are not cumulative and are not binding.” *Drafting suggestion* [BE: we reproduced the text of the drafting suggestions made to the CWP in February, with some amendments highlighted in red]*:*

PUBLIC

Question	MS reply
	(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness that should be assessed depending on the circumstances of the case; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties~~; sharing account credentials with the person without the right of disposal, i.e. is not eligible to use the payment instrument; if the loss of a payment instrument is not reported to the payment service provider immediately after the loss is discovered; where the payment service user has ignored a clear, concrete and case-specific warning by the payment service provider about how to react in the type of fraudulent situation which then occurred and led to the damage; where the payment service user has failed to check if the elements which are dynamically linked and displayed during the strong customer authentication in accordance with Article 85 are correct~~. *When assessing the possible gross negligence on the part of the payment user, all the factual circumstances shall be taken into account. For this*

PUBLIC

Question	MS reply
	purpose, one or more of the following circumstances may be taken into account: *~~(a) payment service user's behaviour or communication with third parties, where relevant;~~* *(a~~b~~) innovativeness, complexity of the fraud, and means or strategies used by third parties to illegally take over the payment service user's personalised security credentials of payment instruments owned by the payment service user;* *~~(c) innovativeness, complexity of fraud;~~* *(b~~d~~) whether the payment service user has previously fallen victim of the same type of fraud;* *(c~~e~~) in case the fraudster's means or strategies constitute a new type of fraud, whether the payment service providers have fulfilled their obligation under Article 84, ~~with particular~~ including with regard to their most vulnerable groups of customers;* *(d~~f~~) whether the payment service user has taken adequate steps in order to properly ensure the confidentiality of their personalised security credentials ~~of the payment instruments~~;* *(e~~g~~) the known characteristics of the payment service user that might make the user more likely to fall victim to fraud~~, for example the user's age, or level of education or profession~~;*

Question	MS reply
	[comment BE: for the purpose of compromise, we propose to leave the criterion in general terms] ~~*(fh) in the event that the payment service user used its means of identification, the circumstances, whether and what the payment service user saw in its messages asking to enter its security credential that confirmed the disputed payment or where the payment service user has failed to check if the elements which are dynamically linked and regarding the amount and the payee that were displayed during the strong customer authentication in accordance with Article 85 are correct, and, where the applicable, the circumstances why the payment service user authenticated the payment without having regard to the information displayed during the authentication process;*~~ ~~*(i) whether the personalised security credentials of the payment instrument have been appropriated by third parties, while the payment service user was using the payment instrument according to its purpose;*~~ ~~*(gj) whether the payment service providers offered clear, concrete and case-specific bespoke warnings against currently used frauds methods that were brought directly to the attention of payer, that are transaction specific, and payment service providers actions, taken in order to familiarise the payment service user with the risks and methods of fraud in the electronic space, as well as the meaning and legal consequences of the*~~

PUBLIC

PUBLIC

Question	MS reply
	~~*safe misuse of identification means and payment instruments issued by the payment service user, the disclosure of their personalised security data, etc. the specificity and nature of any intervention made by the sending payment service provider in the payment flow, whether the payment service user failed to have regard to specific, directed interventions made by their payment service provdider, and whether those interventions offered a clear assessment of the probability that an intended payment was fraudulent.*~~ [comment BE: we suggest deleting the last three criteria as they are not clear] *This list is not exhaustive and does not prejudice the discretion of national courts and/or ADR entities. The circumstances as mentioned are not cumulative and are not binding.* ~~*The fact that a payment service user consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could, depending on the circumstances of the case, be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent modus operandi.*~~ AT

PUBLIC

Question	MS reply
	(MS reply): **AT:** We are open to the drafting of an open list of circumstances **if it remains sufficiently** clear that the distinction between gross and simple negligence is always **up to the national courts in the individual case** and that the list is **non-binding**. The proposed drafting seems to reflect this. ES (MS reply): We do not agree with the removal of the examples for defining gross negligence. We consider these are a useful tool and a prudent way to improve harmonization of liability distribution, since examples per se constitute gross negligence. In previous working parties, the middle ground found was to include both some examples, that constitute automatically gross negligence, and criteria for the ADR bodies and national courts to assess on a case-by-case basis. Please see our drafting proposal in the written comments to the consolidated tables. SK (MS reply):

PUBLIC

Question	MS reply
	We can show flexibility, but some non-exhaustive list of non-negligence, rather than currently drafted list of circumstances for consideration, could be beneficial for the clarity of the text. SI (MS reply): We agree with the proposed drafting to Recital 82 PSR. SE (MS reply): **We strongly support the deletions made.** Focus should be on the need to assess gross negligence on a case-by-case basis, and we welcome that this is more clearly emphasised in the current and more concise drafting. Listing detailed examples will only obfuscate this focus and may tempt PSPs to reject a claim solely based on these examples. The fact that examples and circumstances are difficult to agree on in the Council only supports the case for leaving this to civil law entirely. We can however accept the current drafting for the sake of compromise, but would suggest not to include the circumstance of 'whether the PSU has previously fallen victim of the same type of fraud'. As we have pointed out before, fraudsters sell victims' personal details to other fraudsters, knowing they

Question	MS reply
	are vulnerable. PSUs that have previously fallen victims are therefore much more likely to be targeted again. Furthermore, it is unclear how this circumstance should be assessed. PT (MS reply): PT supports the removal, since a list of examples of 'gross negligence' in PSR itself, besides failing in being unequivocal, and be subjective to become outdated, would also pose challenges to MS due to potential variations in national laws. This inherently involves a case-by-case analysis, with the burden of proof being a crucial factor. Nevertheless, and in the aftermath of the discussion in the CWP, we recall our previous suggestion to consider mandating the EBA to describe a list of examples, not legally binding, that could provide for some guidance on what constitutes gross negligence. This approach ensures flexibility, as it is easier to change Guidelines, an aspect particularly relevant due to the constant evolution in this field. NL (MS reply): We can agree with shortening the text of this recital and providing fewer examples of gross negligence. However, we find the example of warnings by the PSP of great importance as it shows that not only the PSU, but also

PUBLIC

Question	MS reply
	the PSP has a role to fulfil in this context. We therefore propose to include the following text once again (slightly amended for readability): • Whether the payment service providers offered clear, concrete and bespoke warnings payment service user, that are transaction specific. • The specificity and nature of any intervention made by the sending payment service provider in the payment flow, and whether those interventions offered a clear assessment of the probability that an intended payment was fraudulent. LV (MS reply): We support. LU (MS reply): Ok. LT (MS reply): We agree with the elimination of the specific examples from the Recitals. However, regarding other amendments - we strongly disagree. Deleting almost all the criteria would make no improvement in the evaluation process of 'gross negligence' and would the same situation as it is up till now - unclear and open to PSPs' discretion to decide on the content of 'gross negligence'. As well as 'authorisation', 'gross negligence' is one of the crucial elements that determine the scope of PSPs' liability and, hence, the level of PSUs' protection. Even though as

PUBLIC

Question	MS reply
	some MSs state, 'gross neglicence' is a civil law notion, when it comes to PSPs' liability for unauthorised payment transactions, it becomes a question that PSPs are in power to decide upon. Therefore, the guidance on how to interpret this notion and how high or high how low the bar for 'gross negligence' should be, must be introduced in the regulation (be it in the legal text itself, or in the Recitals). Moreover, to ensure the same high level of consumer protection, this question, as well as the question of the definition of 'authorisation', must be understood and approached equally across all MSs. Suggested drafting: *(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness that should be assessed depending on the individual circumstances of the case.* *When assessing the possible gross negligence on the part of the payment user, all the factual circumstances shall be taken into account. For this purpose, one or more of the following circumstances may be taken into account:* *(a) innovativeness, complexity of the fraud, and means or strategies used by third parties to illegally take over the payment service user's personalised security credentials;* *(b) whether the payment service user has previously fallen victim of the same type of fraud;* *(c) in case of a new type of fraud, whether the payment service providers have fulfilled their obligation under Article 84, including with regard to their most vulnerable groups of customers;* *(d) whether the payment service user has taken adequate steps in order to properly ensure the confidentiality of their personalised security credentials;* *(e) the known characteristics of the payment service user that might make the user more likely to fall victim to fraud, for example the user's age, or level of education or profession;*

Question	MS reply
	(f) whether the payment service user has failed to check if the elements regarding the amount and the payee that were displayed during the strong customer authentication in accordance with Article 85 are correct, and, where the applicable, the circumstances why the payment service user authenticated the payment without having regard to the information displayed during the authentication process. *(g) whether the payment service providers offered clear, concrete and bespoke warnings to the payer and whether the payment service user failed to have regard to specific, directed interventions made by their payment service provider.* *This list is not exhaustive and does not prejudice the discretion of national courts and/or ADR entities. The circumstances as mentioned are not cumulative and are not binding.* *The fact that a payment service user consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could, depending on the circumstances of the case, be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent modus operandi.* IT (MS reply): IT.As pointed out in previous rounds of comments, in our opinion, the PSR should clarify the following: • the assessment of "gross negligence" is to be made on a case-by-case basis; • any list of criteria or examples is merely for guidance and is neither exhaustive nor mandatory; • therefore, all the relevant circumstances of the case must be taken into account, even if not explicitly mentioned in the PSR.

PUBLIC

Question	MS reply
	In our view, the current Presidency's proposal aligns with these points. IE (MS reply): Given that national law and the assessment of negligence under national law may vary from country to country we support a comprehensive and open-ended list of guidelines in the Recitals which should be aligned insofar as possible to the EBA Opinion on new types of payment fraud and possible mitigants. Such an approach would facilitate and promote uniform application across Member States. HR (MS reply): We do not agree with the proposal to delete the examples of gross negligence from recital 82. Examples in question may serve as useful guidance for better understanding of what can be considered as gross negligence. We do not see how it would affect the court's freedom to assess on case-by-case basis because competent court in any case has the freedom to decide in accordance with the national law of a Member State. We therefore strongly support retaining the examples of gross negligence in the recital 82. FR (MS reply):

PUBLIC

Question	MS reply
	On Recital 82 on gross negligence, some elements shouldn't be included in the items for defining gross negligence. Indeed, some items ignore the very nature of social engineering cases where fraudster abuse the emotional state of the victim by creating a sense of urgency and coaching the victim through the payment process. Instead, gross negligence should be assessed based on individual characteristics of vulnerability (e.g. age, education, disability, digital skills) and the situational vulnerability (e.g. degree of personalisation and sophistication of the fraud case, use of psychological pressure). (82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness that should be assessed depending on the individual circumstances of the case, ***on the individual characteristics of the payment service user (i.e. amont others age, education, disability, digital skills) or its situation vulnerability***. When assessing the possible gross negligence on the part of the payment service user, account should be taken, for example, of the innovativeness and, complexity of the fraud, the means or strategies used by third parties to illegally take over the payment service user's personalised security credentials ***such as the use of psychological pressure***; whether the payment service user has previously fallen

Question	MS reply
	victim of the same type of fraud; ~~***whether the payment service providers have complied with their obligations under Article 84, with particular including with regard to their most vulnerable groups of customers***~~; whether the payment service user has taken adequate steps in order to properly ensure the confidentiality of their personalised security credentials. FI (MS reply): FI: Yes. It is important that the concept of gross negligence is evaluated on a case-by-case basis and ultimately remains under the discretion of courts and ADR bodies. EL (MS reply): **EL:** We believe that the deleted situation lists be retained, as it provides a practical guidance on what a "significant degree of carelessness" might mean. Also, as already mentioned, we have been among the few Member States supporting a mandate for the EBA to develop Guidelines (GLs) for this purpose. On the current drafting note, we agree with factors proposed such as "whether the PSU has previously fallen victim of the same type of fraud" or "whether the PSU has taken adequate steps to properly ensure confidentially of personalized security credentials". However, there are some factors

Question	MS reply
	proposed which may not support a careless conduct by PSU. For these following factors (in red) we propose to rephrase in order to reflect PSU's perspective and not the innovativeness of the fraud method or the strategies of other parties: - the innovativeness and complexity of the fraud - the means or strategies used by third parties to illegally take over the payment service user's personalised security credentials; - whether the payment service providers have complied with fulfilled their obligations under Article 84, including with regard to their most vulnerable groups of customers We propose to replace the above with the following in blue: - "*level of PSU awareness towards innovative and complex fraud and strategies used by third party to illegally take over the PSU's credentials although payment service providers have complied and fulfilled their obligations under Article 84, including with regard to their most vulnerable groups of customers*".
Presidency Discussion Note: Discussion on electronic communications services providers (WK 4266/2025 INIT)	

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
Q1. Could Member States accept the proposed approach? If not, please provide your suggestions.	DE (MS reply): We appreciate the effort of the PCY to strengthen the role of ECSP in fraud prevention. In particular, we support the alignment of the provisions in PSR with other sectorial obligations for ECSP, e.g. under the DSA. However, given the significant role of ECSP in the fraud value chain it is important to evaluate and further develop the taken measures on an ongoing basis. Hence, we particularly support the inclusion of a review clause in Article 108 with a relatively short time horizon of two years. However, there are still some revisions of the text needed. We will provide our feedback in the course of our written comments after the working party. In particular, concerning the proposed amendments of recital 81 and Article 59a para 1, against the background of GDPR, in our opinion, we would need a more detailed and explicit provision as a legal basis for the exchange of personal data between ECSPs and PSPs (What data may be transmitted by whom to whom and under which prerequisites? Retention period? Permission for further processions? Etc). The Article 59a and the recitals should be amended accordingly.

PUBLIC

Question	MS reply
	Further, the proposed approach to Recital 81f and Article 91 PSR [Competent authorities and investigatory powers] would need further adjustments. Insofar as the proposed Recital 81f states that "competent authority [...] may require providers of public electronic communications networks or publicly available electronic communications services to block access to numbers or services", this should also be explicitly reflected in the powers under Article 91 (5) (h) PSR. Article 91 (5) (h) PSR shall enable the authorities to request third parties to implement measures. In subsections (ii) and (iii), only hosting service providers and domain registries or registrars are currently addressed by way of example. For the sake of clarity, providers of electronic communications services as defined in Article 2(4), points (a) and (b), of Directive (EU) 2018/1972, should also be included here in order to enable access blockings by public electronic communications networks and publicly available electronic communications services in a legally secure manner. The mere inclusion of providers of electronic communications services in Article 91 (5) (a) (iv) PSR is not sufficient, as this only concerns orders to provide information. We also suggest reaching a common understanding with regard to the necessary resources of the competent authorities in Article 91 (5) PSR. In

Question	MS reply
	this respect, it would be helpful to clarify that resources means financial, human and technical resources. CZ (MS reply): We thank Pl PRES for narrowing the definition of ECSPs. However, we still cannot support the new definition in Article 59a PSR. In the new definition, ECSPs fall under the providers listed in Article 2(4)(a) and (b) of the Electronic Communications Code (EEC). The introduction of measures for all providers of Internet access services covered by Article 2(4)(a) of the Code (approximately 2000 companies in the Czech Republic, many of which are SMEs) would mean the introduction of an administrative burden, which is contrary to the current strategy of the European institutions (aimed at reducing administrative burdens). Often these service providers are not even companies. Sometimes they are non-profit organisations providing internet access only to their small local community. Sometimes they don't even have full-time employees, just a few part-time enthusiasts. If this definition is maintained, there is also a risk that their obligations in the trialogues will be extended. **We therefore strongly prefer to apply the definition of ECSPs only to Article 2(4) letter (b) of the Code. The reference to Article 2(4) letter a) of the Code should be deleted. Overall, we believe that the PSR should not impose additional obligations on SMEs, as most related fraud issues occur on very large online platforms and search engines** **As a last resort, this definition should not apply to microenterprises or small or medium-sized enterprises (SMEs).**

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	On the obligation to establish dedicated channels for ECSPs [Article 59a (1) second suppara] - as it is not in the power of small ECSPs to establish communication channels with all Payment Service Providers, such a general obligation should not be imposed on them. **At the very least, the publication of a contact should be sufficient.** On recital 81f - We do not agree with this recital. There is already sufficient regulation under the EEC. On recitals 81b,c,d,e we do not see the need for these recitals to interpret the DSA Regulation and not to have a descriptive provision in the text of the PSR. We believe that this should be discussed with the Council's Legal Service, and we would welcome their views on these drafted recitals. **In general, it is not clear to us why the PSR should contain recitals whose purpose is to interpret other legal regulations.** Regarding Article 59a (2) it is not clear at all what is the legal nature of this provision. As it seems that Article 59a (2) has no legal effect and no binding nature, we suggest deleting this provision or to move it into the recitals. CY (MS reply): We are supportive of the proposals of the IE non-paper.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	BG (MS reply): We are concerned in relation to the Presidency's proposal to extend to national PSR competent authorities the power to require providers of public electronic communications networks or publicly available electronic communications services to block access to numbers or services. Such an approach would imply that national PSR competent authorities are required to supervise to some extent the work of electronic communications service providers, which goes beyond the scope of PSR/PSD3. We believe that this should remain within the scope of the relevant sectoral competent authorities. Also, we do not see merit in the proposed recitals 81b to 81f as they merely refer to other EU legal acts that would apply without prejudice to the PSR. However, if they remain in the PSR we are concerned that PSR competent authorities would be required to supervise application of certain aspects of said EU legal acts. There shall be a clear division of responsibilities between the competent authorities. Furthermore, we are of the view that the appropriate systemic place of Article 59a (1) is within Directive (EU) 2018/1972, rather than in PSR, as it imposes obligations specifically on the providers of electronic communications services. BE (MS reply):

PUBLIC

Question	MS reply
	BE: BE agrees that the introduction of Article 59a PSR is a step in the right direction. However the scope of Article 59 PSR stays very limited. We stress the possible valuable contribution of ECSP's in other types of impersonation frauds in combating and preventing fraud. At last, we question what the added (legal) value is of the new recitals 81a-f PSR since they give interpretation to another legal instrument, the DSA. AT (MS reply): **AT**: We supported the intention of the Irish non paper on electronic communication service providers (ECSPs). Having said that, we acknowledge that any involvement of ECSPs needs to have a legally sound basis. Therefore, we could show support for the PCY's proposal. As far as the IE delegation's proposal regarding the ECSP's assessment of a business' license is regarded we – as many other Member States – were wondering why this should violate fundamental or other rights of ECSPs. Such obligation would not be about blocking content but simply assessing the entitlement of certain businesses to carry out financial services. Along with most other Member States we can support a bold approach regarding ECSPs, in particular large platforms for social interactions. Concerning the proposed communication channels, we agree that the text should allow for flexibility regarding the form of these channels to ensure future proofness.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	ES (MS reply): We strongly support the inclusion of more specific cooperation requirements for ECSP. In particular, we welcome the introductions of recital 81. However, we would like to highlight that even though recital 81(f) includes the possibility that NCAs require ECSPs to block access to numbers or services in fraud scenarios, this possibility could be more preventive. For instance, Spanish domestic legislation includes the obligation to block calls and texts under certain circumstances that are usually linked to fraud, such as the use of national CLIs by international calls without roaming. Therefore, we would suggest the following wording: *National competent authorities can play an important role in combating the type of fraud referred to in this Regulation by requiring providers of electronic communications services on a case-by-case basis to block access to numbers or services once said fraud has been committed using electronic communications services and ascertained by a competent authority. If a national competent authority has ascertained the occurrence of the type of fraud referred to in this Regulation, they may require providers of public electronic communications networks or publicly available electronic*

Question	MS reply
	communications services to block access to numbers or services, in accordance with Article 97(2) of Directive 2018/1972/EU. Furthermore, sectorial regulation at the national level could be updated to allow electronic communication services providers the possibility to block calls and/or SMS where fraudulent elements are identified. SK (MS reply): We are not against stricter obligations for ECSP in principle, however, costs must be properly analysed, and the wording fine-tuned. Beside of necessity to keep in alignment with DSA, we should carefully assess the impact on ECSP. We would like to echo CZ in the stance, that current wording would influence broad range of entities, some of which are of negligible size and the costs laid on them would be non-proportionate to the benefits foreseen. Introduction of the entities under Article 2(4)(a) of ECC to the Article 59a PSR should be reconsidered. SI (MS reply): We could accept the proposed approach. SE

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): We support the proposal in 59a on the communication requirements. We do however still also support the first part of the Irish proposal, on the verification of advertisers of financial products. We still struggle to understand in what way the Irish proposal would be in conflict with the ePrivacy Directive or the no monitoring obligations of the DSA. As our Irish colleagues already made clear, the proposed measures do not focus on the content itself. Therefore, it does not require the platform to monitor the advertisement for any facts or circumstances that indicate illegal activity on the advertiser's part. The proposed measures simply require that before displaying an ad, the identity of the advertiser should be verified as an authorised financial services provider. This should rather be compared to article 30 in the DSA, requiring traceability of traders (the article states that online platform providers should obtain information on the name and payment account details of the trader, as well as its registration number with the relevant trade register). We would therefore like to ask the Presidency if the legal analysis dismissing the Irish proposal could be clarified? If there is indeed a problem, perhaps there are ways to adapt the proposal to fit the DSA better.

PUBLIC

Question	MS reply
	If not, it should be possible to motivate and exception from the general rules of the DSA when it comes to such severe organised crime as online fraud. Online fraud is quickly growing all over the world and is now competing with the illegal drug industry in terms of profits. Investment fraud is the by far most lucrative type. Given the magnitude of this problem, we really think we should seize every opportunity we can to fight these types of organised crime. This would also be in line with EUs European Internal Security Strategy, acknowledging that we need to strengthen EU's ability to fight online fraud. PT (MS reply): PT can support the introduction of new Article 59a, that foresees dedicated communication channels between PSP and ECSP, as well as the usage of notification mechanisms on part of PSP. Moreover, we cherish the blockage possibilities previewed in Recital 81f triggered by intent of the competent authority and the review clause advocated by the PRES PL. NL (MS reply): General

PUBLIC

Question	MS reply
	• These proposals (including addition of Article 59a) have been improved significantly. Positive: the single focus on impersonation fraud seems to have been left, more active (preventive) actions are included and digital platform providers are clearly positioned. • We could basically agree with the taken approach, but still propose some modifications and finetuning to both articles 59 and 59a and related recitals. • Main points of concern: the proposals still do not seem to give enough clarity on the interworking with directives 2002/58/EC and 2018/1972/EU: o regarding the scope of 2002/58/EC with regards to possible measures ECSPs can take to prevent fraud; o regarding the role of public authorities in possible mechanisms for e.g. blocking access to numbers for fraud prevention. These issues are urgent and therefore it is less appropriate to wait addressing these in the review based on Article 108. <u>Recital 81</u> • We agree with the active approach: technical/organizational measures with involvement of ECSPs should be in place to prevent future fraud,

Question	MS reply
	supported by the relationship with the NIS2 directive. We note that the scope of this recital should be better aligned with article 59a, where the scope includes all types of fraud including spoofing fraud, and includes *preventive* measures. • It is important that different ECSPs in the service chain should be distinguished, at least between Interpersonal Communication Service Providers (IPCSPs) that terminate traffic to the end-user and IPCSPs originating traffic at the side of the caller/sender (e.g. sms brokers). In certain cases the latter are in better control to effectively prevent or stop fraud at the start of the fraud chain (Know Your Customer). This should be emphasized in the recital text. • A clear legal basis for data processing is not described. See also our remarks and text suggestions to Articles 59a.1 and 83a. • A reference is made to directive 2002/58/EC but as we mentioned before, this directive is not very clear on the possible mechanism to process communications data and traffic (meta)data to prevent fraud as targeted in the PSR: o Recital 29 of that directive points to fraud consisting of unpaid access to electronic communications service, but does not mention fraud *targeted to end-users*. It would be beneficial to

PUBLIC

PUBLIC

Question	MS reply
	clarify that the scope of the directive includes both types of fraud. o Also the directive 2002/58/EC is not clear on the role of a competent authority in this mechanism, where we have the same concern as mentioned with respect to Recital 81f (again, see also our remarks and text suggestions to Articles 59a.1 and 83a). • In light of above, we propose to modify Recital 81 and add an additional recital 81g as described below: *Recital 81* *Given their obligations to safeguard the security of their services in accordance with Directive 2002/58/EC of the European Parliament and of the Council and Directive (EU) 2022/2555 of the European Parliament and of the Council, publicly available electronic communications services providers have the capacity to contribute to the collective fight against* ***fraud, including*** *'spoofing' fraud.* ***Such capacity differs between different ECSPs, dependent on their position in the electronic communications service chain.*** *Therefore, and without prejudice to those Directives, electronic communications services providers should* ***implement preventive***

PUBLIC

Question	MS reply
	and responsive measures and *cooperate with payment service providers with a view to preventing further occurrences* ***fraud including 'spoofing'*** *of that type of fraud. This cooperation could include establishing dedicated communication channels for the sharing of relevant information in order to facilitate fraud prevention and detection in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC. Furthermore, providers of electronic communication services could also assist the fight against fraud by exchanging with payment service providers fraud scenarios, trends and threats identified in relation to the use of their services, as doing so may help to improve the effectiveness of transaction monitoring mechanisms and the educational campaigns and training on fraud implemented in accordance with this Regulation and without prejudice to Directive 2002/58.* ***Recital 81g*** ***In accordance with article 15, paragraph 1, of Directive 2002/58/EC, electronic communication service providers may process communications and the related traffic data for the prevention, investigation, detection and prosecution of fraud targeted to electronic communications end-users. This may include, for example, with regard to impersonation***

Question	MS reply
	fraud, the processing of traffic data or communications data in order to prevent or end reasonably suspected fraud.
	• In accordance with article 15, paragraph 1, of Directive 2002/58/EC, electronic communication service providers may process communications and the related traffic data for the prevention, investigation, detection and prosecution of fraud targeted to electronic communications end-users. This may include, for example, with regard to impersonation fraud, the processing of traffic data or communications data in order to prevent or end reasonably suspected fraud.
	<u>Recital 81a</u>
	• No comments on the content of this recital. However, we have a strong preference that – because of its urgency - the issue mentioned under Recital 81 is solved in the current legislative proposal.
	<u>Recitals 81b, 81c, 81d, 81e</u>

PUBLIC

Question	MS reply
	• We welcome these recitals as they explain the interworking with DSA directive, no comments. <u>Recital 81f</u> • We have concerns about the described explicit role of national competent authorities as this may impact on anti-fraud measures initiated and operated by ECSPs: o The proposal seems to go beyond cases where numbers are used without or in violation of number usage rights, e.g. spoofing, where the blocking of numbers should be a possible measure to be taken by ECSPs to fulfill their legal obligations in this regard. o The involvement of competent authorities in individual cases may reduce the effectiveness of certain measures, including those based on internal traffic monitoring by ECSPs and those based on (realtime) datasharing with PSPs. o At least, and to address the previous point, there should be more clarity on how involvement of competent authorities on a "case-by-case" basis should work in practice (while not delaying detection or prevention of fraud).

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	Text proposal for modification Recital 81f: *National competent authorities can play an important role in combating the type of fraud referred to in this Regulation by requiring providers of electronic communications services on a case-by-case basis to block,* ***permanently or temporarily,*** *access to numbers or services once* ***when fraud is reasonably suspected or*** *said fraud has been committed,* *using electronic communications services and ascertained by a competent authority.* ***In such cases national competent authorities*** *If a national competent authority has ascertained the occurrence of the type of fraud referred to in this Regulation, they may,* ***ad hoc or on the basis of guidelines issued by national competent authorities,*** *require providers of public electronic communications networks or publicly available electronic communications services to block access to numbers or services in accordance with Article 97(2) of Directive 2018/1972/EU****, without prejudice to the ability for providers of electronic communications services to block access to numbers or services in cases of infringements of number usage rights.*** <u>Article 59.1 and 59.5</u>

PUBLIC

Question	MS reply
	We note that there may be a spectrum of similar names/numbers around the name/number of the concerned PSP, especially for alphanumeric identifiers, that also creates a grey area around impersonation fraud. The effectiveness of Article 59.1 (liability of PSP at impersonation fraud) would benefit if the scope of this Article would be extended with such cases. Furthermore it is unclear whether the use of the "name" of a PSP/bank in Article 59.1 may refer to: a) the use within the body of the message or call, or b) the message origin header or Calling Line Identification (CLI). We suggest to clarify this in the text of this article. Furthermore we suggest to use a more technological neutral term for "email address" e.g. *messaging address* (the same applies to the rest of the proposal) Concerning Article 59.5, we repeat our earlier wish that the required actions with regard to the ending of fraud occurrences should be specified more accurately. We note that in the above cases (name in message call body, similar name) the responsibilities and required actions from ECSPs

PUBLIC

Question	MS reply
	become more complex as these would go beyond sector-specific obligations to ECSPs (anti-spoofing measures, regulation of telephone number user rights and regulation of alphanumeric messaging addresses). However, with the creation of Article 59a.1, we suggest to reconsider keeping Article 59.5, see for this our respective consideration of Article 59a.1. <u>Article 59a.1 and 83.6</u> • We read Article 59a.1 such that is includes both preventive measures, and reactive measures to occurring types of fraud. Therefore in relation with Article 59a.1, Article 59.5 seems to have reduced added value and may act confusing as it only refers to the types of fraud specified in Article 59.1. We suggest to reconsider to keep Article 59.5 in this light. • We repeat our earlier wish that the required actions with regard to the ending of fraud occurrences by ECSPs should be specified more accurately. • We agree with the obligatory character to ECSPs of the Article 59a.1. • There is no (reference to) a legal ground for data processing/sharing needed in the context of cross-sectoral (PSPs-ECSPs) measures targeted in article 59a.1. To solve this, we propose modifications to both Article 59a.1 and Article 83.6.

Question	MS reply
	• Furthermore the provision in Article 59a.1 does not include network internal measures by ECSPs (without involvement of PSPs). This element should also be addressed, as an option, by including it in the scope of the current provision. • Text proposals for modification of these articles: *Article 59a.1* *1. For the purpose of preventing, and detecting* ***and ending*** *fraud, including that referred to in Article 59(1), providers of 'electronic communications services' as defined in Article 2(4), points (a) and (b), of Directive (EU) 2018/1972 shall have in place* ***measures, including*** *measures to ensure effective cooperation with payment service providers, having regard to the technical characteristics of each of their services.* ***Member States shall ensure that appropriate measures are in place so that providers of electronic communications services are able to share the data referred to in Article 83, paragraph 1, points f to i, with payment service providers, in accordance with Article 15(1) of Directive 2002/58/EC.*** *Article 83.6*

PUBLIC

Question	MS reply
	6. For the purposes of this Article, Member States shall ensure that appropriate measures are in place so that the payment service providers are also able to share the data referred to in paragraph 1 with the relevant national authorities ***and providers of electronic communications services****.* • We repeat one of our remarks to recital 81: The concept of dedicated communication channels needs elaboration, and be more clear about whether this would be – in line with article 59 - obligatory or not (an obligation would be appropriate in our view). <u>Article 59a.2</u> • With new insights on the role of the DSA, we step back from an earlier contribution where we stated that digital platform providers should fall in a similar way as ECSPs under article 59. Although their role should be addressed, given the relevant considerations, we do not see the added value of the specific provision in Article 59a.2. It seems to be redundant as it only repeats the concerned mechanisms as stipulated in the DSA, with as contrary effect of possibly leading to legal uncertainty. <u>Article 59a.3</u>

Question	MS reply
	• Although we understand the reasoning, we wonder how such a mandate to the EC and relevant surveillance bodies relates to the independent characters of these bodies. We suggest to also investigate alternatives, such as, instead of a legal obligation, a commitment of the EC to start such procedure. LV (MS reply): We support. LU (MS reply): We are strongly supportive of PRES proposal. We would be against the introduction of any obligation for electronic communication service providers that would not be compliant with the sectoral legislation of electronic communication service providers. LT (MS reply): We accept IT (MS reply):

PUBLIC

PUBLIC

Question	MS reply
	IT. We welcome the new provision art. 59 a and in particular the possibility for PSPs to apply to be awarded trusted flaggers status and the drawing up of voluntary code of conduct. We provide a few suggestions in relation to the actual wording. In particular: a) A better coordination with recitals 81e and 81f, which refer to NCAs' powers. However, NCAs for ECSPs are different from NCAs of the financial sector. Some of the concepts mentioned in the recitals are not developed in the articles; b) with reference to infosharing (par. 1), "any information" could be replaced with "fraud scenario, trends and threats" (referred to in rec. 81), which is more narrow; c) sectoral CERT/CSIRT could be involved in the drawing up of codes of conduct. In relation to art. 91, the provision gives investigative powers to authorities that are not competent for the financial sector. We suggest initiating contacts also with the national authorities competent for ECSPs. IE (MS reply): We are disappointed by the analysis in this Discussion Note, which suggests that our drafting includes an element of removing/blocking access to content contrary to the DSA, and we would disagree with that interpretation. As we

Question	MS reply
	have previously stated, this aspect of our proposal is focused on who is placing the advertisement rather than the content in the advertisement and contains no general monitoring obligations. Article 8 DSA states that there is no general obligation to monitor the information which providers of intermediary services **transmit or store,** nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers. If our proposal is adopted this would mean that the requirement to verify will apply **before** any content or advertisement is created, transmitted or stored. If the verification check shows that the advertiser is not authorised, and the advertiser and advertisement is rejected, there will be no content or advertisement stored or transmitted and therefore nothing to monitor. If there is nothing to monitor it would be difficult to see how the proposal breaches Article 8. If the verification check shows that the advertiser is authorised and the advertiser and advertisement is accepted there is no obligation by the service provider to monitor the information which providers of intermediary services transmit or store for the advertiser. In addition, the requirement to verify the financial regulatory status of the advertiser is not related to the seeking of facts or circumstances that indicate or speak to the illegality or legality of any activity. The proposal requires

PUBLIC

PUBLIC

Question	MS reply
	only that before an entity becomes an advertiser, the service provider receives a verification that the advertiser is an authorised financial service provider. The service provider is under no obligation to conduct any actions that seek to test or validate the illegality or legality of the advertiser's actions. We believe that we have steered a line between what needs to be done and the DSA: our proposed measure is a modest one to try and prevent a portion of fraud before it happens, building on the fact that payments are the last step in the fraud chain. We reiterate that we believe our solution would be a strong foothold to bring to trilogues, demonstrating strong action on this issue, especially with the potential for a move to much wider reimbursement from Parliament's second reading. We would also raise the question of why Articles 26 and 46 of the DSA are not referenced in the proposed recitals. Article 26 of the DSA sets requirements related to advertisements on online platforms, including a requirement for online platforms to ensure that recipients of advertisements can identify, in a clear, concise and unambiguous manner and in real time the natural or legal person on whose behalf the advertisement is presented and the natural or legal person who paid for the advertisement. Article 46 of the DSA provides the Commission with scope to facilitate the drawing up of voluntary codes of conduct of online platforms and other relevant service

PUBLIC

Question	MS reply
	providers involved in the advertising value chain in order to increase transparency for actors in the online advertising value chain. Recital 81d in the Presidency note references Article 45 of DSA on voluntary codes of conduct. Is there scope to insert another recital focusing on Article 26 and 46 of the DSA? Such a recital could draw attention to the issue of fraudulent financial services advertisements on online platforms and point to Article 26 and 46 as potential avenues through which the issue could be addressed within the framework of the DSA. However, we welcome the work being done on the dedicated communication channels. This is something we believe has the potential to make a real difference both in terms of fraud prevention and in terms of an equitable and productive relationship between PSPs and electronic communications series providers. HR (MS reply): We accept the proposed approach. FR (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	The approach proposed by the Presidency focuses on enhancing the cross-sectoral cooperation between electronic communication service providers (ECSPs) and payment service providers (PSPs). Such approach with the proposed creation of Article 59a PSR has merits. We welcome the proposal aiming at (i) ensuring that PSP could apply as trusted flaggers in the meaning of Article 22 DSA, (ii) encouraging the drawing up of a voluntary code ii) encouraging the drawing up of a voluntary code of conduct to foster prevention, enhance security and combat payment fraud and financial scams under the conditions set out in Article 45 DSA. We wonder whether it would be possible to clarify that payment fraud and financial scams as systemic risks under Articles 34 and 35 DSA through a recital for example. However, we consider that targeted obligations should be imposed to telco operators in the meaning of Article 2 point (4) *b)* of Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code on the basis of what has been implemented by several Member States including France. As an example, in France, fraud through manipulation of the payer (spoofing) has decreased since the implementation of authentication of telephone lines. In our view these targeted obligations should focus on

PUBLIC

Question	MS reply
	preventing (i) spoofing, (ii) SIM-swapping and (iii) smishing (= fraudulent SMS). FI (MS reply): FI: We thank the Presidency for its efforts to find a balanced solution that does not contradict with other legislation in the telco sector. Overall, we find the proposed approach acceptable, but we have a couple of remarks on the proposals: • Firstly, regarding Article 59a(2): we would appreciate confirmation that multilateral dedicated communication channels would fulfil the requirement, i.e., not all ECSPs should have their own communication channel, but one including multiple ECSPs is acceptable. Such a multilateral communication channel is currently being prepared in Finland. To ensure legal certainty on this, the following sentence could be added to the recital: "***or participate in a system for effective communication, or an information sharing mechanism***". We also think Article 59(2) would be better suited in a recital than in the operative part of the text. • Secondly, we suggest the following amendment to Article 91(5)(a): "*in the course of procedures to investigate potential breaches of*

PUBLIC

Question	MS reply
	this Regulation, the power to require ~~*from, inter alia, the following natural or legal persons, all information necessary to carry out that investigation*~~***, insofar as permitted by national law,*** *any person to provide information and documents which the competent authorities consider* ~~*could be relevant*~~***necessary*** *for the performance of their duties, including the following natural or legal persons*:" o The addition "*insofar as permitted by national law*" is necessary as the processing of communications data is subject to conditions under, inter alia, the ePrivacy Directive 2002/58/EC and national laws through which it has been transposed, and MSs may also have other legislation relating to the processing of such data which should be taken into account when processing such data. Furthermore, through this amendment, the wording would be aligned with the wording under Article 91(5)(e). o The amendment of "*could be relevant*" to "*necessary*" would, as the powers to obtain information concerns personal data as well, ensure consistency with Article 5(1)(c) GDPR on data minimisation. EL (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	EL: We agree with the establishment of a cooperation framework and the creation of a dedicated communication channel between PSPs and ECSPs, as well as with the possibility of designating PSPs as trusted flaggers. However, we continue to believe that it would be beneficial if obligations for ECSPs could also directly arise in connection with liability, rather than relying solely on national law. We would also prefer direct requirements in relation "verification of the advertisers of financial products" as Ireland had suggested in its non-paper. With respect to the suggested wording included in the PCY document, but we are in favor of using **"***should***"** instead of **"***could"* in Recital 81, to align the recital with the wording of the newly introduced Article 59a.
Presidency Discussion Note: Discussion on transparency on payment card schemes' fees and rules (WK 4326/2025 INIT)	LT (MS reply): We'd like to pay attention to one important aspect – that is enforcement. It is not clear how to enforce the application of such requirements and how to supervise that, as requirements are set for card schemes and not PSPs.
Q1. Do you agree that the scope of the transparency requirement should be extended to acquirers or should the concerns of Member States be addressed as a clarification in the recitals instead?	DK (MS reply): Increased transparency regarding fees is a political priority in Denmark. Hence, we are open to the idea of an EBA report as long as it is still possible to do national measures to increase transparency.

Question	MS reply
	We believe that this is essential for merchants to benefit from the Transparency and to be able to negotiate fees with acquirers. Many merchants may not be aware of a report published by the Commission as suggested in 108(3) PSR. Our understanding is that a EBA report should not preclude member states to do more in this area if needed. The suggested article 31a should as such secure the objective of a minimum harmonisation across the Union and not the objective of total harmonisation. DE (MS reply): We strongly disagree with the proposal to extend transparency requirement to acquirers. The competitive situation on the markets for acquiring services differs much from that on the markets for card schemes services. The typical merchant has the choice between different acquirers and contracts with only one of them. This gives the merchant the possibility to negotiate for low fees. In addition, regarding transparency between acquirers and merchants there is Art. 9 of the Interchange fee regulation in place ("unblending" requirement for acquirers towards merchants), i.e. possible aspects regarding acquirer-merchant transparency would be better placed there.

PUBLIC

PUBLIC

Question	MS reply
	With regard to the term 'payment service business end user', we think that a clarification in the recitals is not the best way forward. Instead, the addressees and responsible parties should be defined more clearly. "For the purposes of paragraph 1, payment card schemes shall communicate scheme rules and fees unambiguously in a transparent and consistent manner to the payment service providers issuing payment cards or providing acquiring of payment transactions ~~and to payment service business end users of the payment card scheme~~ no later than 6 ~~9~~ months prior to their implementation. Payment service providers providing acquiring of payment transactions shall forward this information to their payment service users without delay." Further, we still see the risk of tacit collusion arising from such proposal that could lead to an increase of payment card scheme fees, against the aim of the proposal. CZ (MS reply): No. The issue is already covered by Article 9 (2) of interchange fee regulation: *Acquirers shall include in their agreements with payees individually specified information on the amount of the merchant service charges, interchange fees and scheme fees applicable with respect to each*

Question	MS reply
	category and brand of payment cards, unless the payee subsequently makes a different request in writing. CY (MS reply): We do not object that the scope of the transparency requirement could be extended to acquirers. BE (MS reply): BE: We can agree to extend the scope to acquirers yet we have doubts on the direct disclosure requirements towards payment service business end-users of a payment card scheme. We consider that the reality of the business relationships should be taken into account. Payment schemes have relations with issuers and acquirers, not directly with merchants and consumers/payers. Hence any transparency requirement towards merchants and consumers/payers should be levied on their contractual counterparty, while of course ensuring that payment schemes do nothing to prevent issuers and acquirers from being fully transparent (so anticipate any Non-disclosure agreements that payment schemes force on acquirers).. AT (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	AT: As previously mentioned, we welcome our FR colleagues' intention to improve transparency regarding fees of payment card schemes. We still believe that a solution would be better placed in the Interchange Fee Regulation. Subject to this caveat, we could show openness towards a clarification in the recital that the transparency requirements also refer to acquirers if a majority of Member States favor this option. In any case, the proposal needs to be in line with the requirements under IFR. ES (MS reply): As a general comment, ES is supports the FR non paper on transparency of scheme fees. ES shares the concerns that the increase in scheme fees may potentially negatively affect the retail sector, and could agree to extend transparency requirements to acquirers since in this way we can have the complete information on how the merchant service charge is being applied. However, we do not object either if the way forward is to clarify in the recital that this only applies to scheme fees. SK (MS reply): Ideally, we would tackle this issue within IFR, however we are supportive towards FR initiative. We do support extension of the scope to the

Question	MS reply
	acquirers. We should be cautious with the introduction of new terms such as payment service business end-users, which are not yet defined in relevant legislation. Should be clarified at least in recital. SI (MS reply): We agree with extension of the scope to acquirers. SE (MS reply): Yes. Overall, we support the proposal. PT (MS reply): PT tends to support broadening the transparency requirements to also include acquirers and, consequently, encompass in the review clause (point a) an assessment of fees charged by the acquirers. Nonethless, we wonder about the necessity of mandating such requisites within the PSR, considering the obligations foreseen in Article 9(2) of Regulation (EU) 2015/751 (IFR), under which the acquirer shall provide to their PSU specified information on the amount of the merchant service charges, interchange fees and scheme fees.

PUBLIC

Question	MS reply
	Considering this provision already involves depicting scheme fees to the end user, PT believes the suggested Article 31a PSR should assure the removal of any current barriers that may be deterring the intended transparency, such as non-disclosure agreements imposed by payment card schemes. Additionally, and considering the concerns raised by various MS, we question if it would be preferable to include the provisions of the suggested Article 31a PSR instead as an amendment to IFR's Article 9. NL (MS reply): We agree that the scope should be extended to acquirers which would mean a break-down of the charged Merchant Service Charges (MSCs) into 1. scheme fees paid to the scheme by both the issuer and acquirer, 2. interchange fees paid to the issuer and 3. acquirer margin. Reporting on scheme fees only would be too narrow, we would reckon. LV (MS reply): We strongly support the need for a more in-depth assessment of the transparency of fees. We strongly support the need for clarity and transparency in the relationship with merchants; end users should be able to see those fees attributable to the payment decisions. The transparency is

PUBLIC

PUBLIC

Question	MS reply
	largely addressed through the IFR, but perhaps the PSR is the right place to regulate such information exchange information requirements between card schemes and merchants. In that case, we would also delete the option left in the IFR, so that the PSP can still bundle the fees together "*if so agreed with the client-merchant*". In practice the PSP acts from the strength positions and the client/merchant from the weakness positions, so in most cases the merchant won't get the fee transparency under the current IFR. LU (MS reply): We support the extension of transparent requirements to acquirers. However we should ensure that the transparency obligations follow the logic of business relationships of the payment ecosystem, i.e. acquirers should be transparent to merchants, whereas payment card schemes should be transparent to acquirers. LT (MS reply): Requirements for the information provided by acquirers to merchants are already in the IFR, new provisions in the PSR might overlap which could make acquiring PSP difficult to implement all the information requirements. Also, there should be no requirements for schemes to provide any information to merchants. They have no contractual relations and it would be not reasonable for

PUBLIC

Question	MS reply
	schemes to try reaching out all the merchants. Moreover, part of scheme fees are not directly attributable to merchants, e.g. annual scheme fees for PSPs. IT (MS reply): IT. As a general comment we support French proposal that was presented in the 21/02 Working Party. Regarding the possibility of extending transparency obligation to the acquirer, we underline that Regulation 2015/751 (IFR), in particular in the art. 9 and art. 12, already defines some disclosure requirements. Therefore, we believe that coordination with the aforementioned regulation is necessary, in order to avoid overlapping and unclear/duplicated obligations. In addition, coherently with what defined in art.13 of IFR, it would be important to provide clear indications about the competent authorities in charge of the supervision and enforcement of such new requirements. IE (MS reply): We are open to extending transparency requirements to acquirers and are generally supportive of making payment card scheme fees and rules more transparent and this should be done in the most efficient way. HR (MS reply): We have no comments. FR (MS reply):

PUBLIC

Question	MS reply
	The transparency of the card fees should be considered in a large way. It is therefore a good policy to envisage greater transparency also on the side of acquirers. However we should ensure that such transparency duty isn't counterproductive and does not represent extra duty for acquirers. Acquiring fees are negotiated between merchants and PSPs and there are multiple requirements in the Chapter 3 on framework contracts in the PSR, contrary to scheme fees that are unilaterally set by the card scheme and to interchange fees (that are capped only for consumer cards). That's why we think that the scope of transparency requirement shouldn't be extended to acquirers that are subject to other requirements ensuring the same goal. FI (MS reply): FI: Yes. EL (MS reply): EL: We believe that the scope of the transparency requirement should be extended to include acquirers.
Q2. Do you agree with the proposed amendments to the list of issues that should undergo the review by the Commission in 108(3)?	DK (MS reply): Yes. Denmark agrees with the proposed amendments, that is the

PUBLIC

Question	MS reply
	deletion of d) and e), and thus narrowing the scope of the review the Commission is intended to carry out. However, Denmark urges to reconsider the scope of the review even further. It would be a large task to collect and compile all of the data and information from multiple schemes, not to mention write a report. Denmark believes a report, with a narrower scope may be more useful, and less burdensome both for the schemes and for the Commission. If the larger scope of the review is preferred, then Denmark urges to reconsider how often the review should be carried out. Denmark suggests that the review is carried out every fifth year rather than every second year. Please also note by imposing the Commission to carry out the review and present a report every second year, the Commission can to a lesser degree prioritize other cases. Finally, Denmark notes, in case the transparency requirements is extended to acquirers the information to be collected is multiplied many times over.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	DE (MS reply): We share the aim of the proposal. However, we still have some concerns regarding the set-up of the proposal. In particular, we still do not understand yet, on which data basis the COM should draft the report under Article 108 PSR? In our understanding, some of the key elements of the report would rely on very granular data – e.g. regarding rebates and incentives by acquirers and issuers. How should the Commission obtain such data? To be clear, we would be very skeptical about a reporting duty to the COM including individual transaction data. CZ (MS reply): We are flexible. CY (MS reply): We have no comments for the proposed amendments to the list of issues that should undergo the review by the Commission in 108(3). BE (MS reply): BE: we agree

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	AT (MS reply): **AT**: We can show flexibility here. ES (MS reply): We would prefer a wider approach, but we do not object the proposed amendments. SK (MS reply): Support. SI (MS reply): We agree. SE (MS reply): Yes. PT (MS reply):

PUBLIC

Question	MS reply
	PT can be flexible on the suggested removal but would consider important to hear the COM's stance on this issue to fully understand possible challenges and realistic expectations on what is achievable. For us, maintaining points d) and e) would make sense from a conceptual point of view given that it may facilitate gathering relevant insights surrounding the negotiating capacity of PSP and the overall competition of the payment card scheme market, which could then feed into an eventual legislative proposal. NL (MS reply): Yes, but we still believe that these issues belong more in a future revision of the IFR than in the PSR. But when this appears not feasible, then the PSR should do. However, it is, inter alia, stated that the European Commission should report on the 'rebates and incentives' that acquirers and issuers have received from the card schemes (by key transaction category, per Member State). Please note that is quite delicate and competition-sensitive data for acquirers and issuers to provide (see also our reply to question 5). In this case, the proposed amendments to the list of issues that should undergo the review by the Commission in 108(3) should also be extended to acquirers (re. their MSCs charged to merchants). LV

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): We support (we supported FR non-paper) LU (MS reply): OK. IT (MS reply): IT. We support the inclusion of points (d) and (e) as originally presented in the French proposal. IE (MS reply): We can agree with the proposed amendments. HR (MS reply): We have no comments. FR (MS reply): We agree with the proposed amendments in Article 108 (3) PSR. We think it is important to keep items d) and e) in the forthcoming report of the Commission.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	FI (MS reply): FI: Yes. EL (MS reply): EL: It is better to keep the article as it is.
Q3. Do you consider the proposed clarification to be sufficient or is it necessary to further clarify the term 'in a transparent manner' mentioned in Article 31a(1)? If the latter, please provide drafting suggestions.	DK (MS reply): No. Denmark does not consider the proposed clarification to be sufficient. The suggested amendment implies, that the legislator leaves it to the industry (that is the schemes and possible acquirers) to reach an agreement on what is transparent and what is needed in order to secure comparability of billing categories between schemes (and in case the requirement is extended also acquires). Denmark instead suggests that the Commission after consultation and dialogue with schemes (and acquires) specifies in level 2 an overall template in which information and data should be shared with the Commission.

PUBLIC

Question	MS reply
	This will allow the Commission to further specify which requirement need to be fulfilled in order to secure comparability of billing categories between schemes etc. DE (MS reply): --- CZ (MS reply): We are flexible. CY (MS reply): We understand that if the article or recitals are too vague in this respect, enforcement of these provisions will be difficult and that disclosure should be made in a manner that allows for comparability. BE (MS reply): BE: In Belgium, we are currently working on the development of a tool allowing merchants to compare the costs of the different payment solutions. The aim is to improve transparency on the costs for merchants. Therefore,

Question	MS reply
	in our opinion, transparency implies comparability between payment card schemes. We can therefore support the presidency's drafting suggestion. AT (MS reply): **AT**: Subject to our caveat regarding the IFR as the more suitable framework for fee transparency, we believe the drafting could be a step in the right direction. ES (MS reply): Regarding the suggestion by one Member State to elaborating on what 'in a transparent manner' could mean, and on the suggestion proposed by the presidency of allowing comparability between payment card schemes, we need to be careful that allowing the referred comparability does not undermine the business secrecy on how setting up their own rules and fees. At the end, what is important, is to monitor the price trend, and not the specific detail of each fee imposed on a specific service at a specific point in time This latter information could be useful to a NCA, but maybe not for the general public. SK (MS reply):

PUBLIC

Question	MS reply
	Open to clarification. SI (MS reply): We consider the proposed clarification to be sufficient. SE (MS reply): We think the proposal is sufficient. PT (MS reply): PT agrees. NL (MS reply): We believe it should be clarified, in order to avoid misunderstandings. Maybe EBA could be mandated here to draft implementing technical standards (ITS) on what 'in a transparent manner allowing comparability of billing categories between schemes' actually comprises of. An advantage of this approach is that the EBA submits its draft IT for public consultation, in order to receive input from the involved market participants. LV

PUBLIC

PUBLIC

Question	MS reply
	(MS reply): We could agree that we need to think about a solution for transparency. LU (MS reply): OK. IT (MS reply): IT. We deem current wording ('in a transparent manner') is sufficient for Level 1 regulation. However, we propose to defer to Regulatory Technical Standards developed by EBA the definition of specific requirements in order to obtain clear and comparable information (e.g. data categories definition and level of data detail). Furthermore, RTS can also be the mode of better defining the "interplay" between PSD3/R and IFR requirements. IE (MS reply): We consider the proposed clarification to be sufficient: if more clarification is required, it may be useful for further clarity in a recital. HR (MS reply): We consider the proposed clarification to be sufficient.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	FR (MS reply): We consider important to ensure harmonisation/categorisation or standardisation of the classification of scheme fees, which goes beyond the unblended possibility given by IFR. That's why the proposed drafting on the comparability of billing categories is a good approach for us ; some standardisation in the Regulation (or in a L2 text) could be envisaged. Regarding exchange of information between payment card schemes and merchants, since scheme fees are unilaterally decided by the payment card scheme, it is logical to impose a duty of transparency on payment card schemes while also maintaining the fact that card scheme do not have a direct contractual relationship with merchants. Many possibilities could be envisaged (such as disclosure of simplified information on website,) that do not imply direct contractual relationships between schemes and merchants. Then, acquirers, via their contractual relationship and existing regulatory obligations (IFR and PSR) will provide that transparency to merchants. Such change does not require any change in business model or a change in contractual relationship at all. EL (MS reply):

PUBLIC

Question	MS reply
	EL: We consider that the term 'in a transparent manner' needs clarification
Q4. Do you agree with the amendments regarding the notification period?	DK (MS reply): No. Denmark suggested that the original notification period should be shorter than 9 months, since such a long period gave the schemes the possibility to signal their (future) prices to competitors. Denmark suggests the notification period be shortened even further e.g. 3 months. In case the scope of the transparency requirement is extended to acquirers, and the fees payees pay to acquirers, Denmark suggests the notification period should be even shorter than 3 month, however, at least one month. DE (MS reply): Shortening the notification period could decrease the risk of tacit collusion. CZ (MS reply): We're in favour of reducing it to 6 months. CY (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We have no comments regarding the change in the notification period from 9 to 6 months. BE (MS reply): BE: we agree AT (MS reply): - ES (MS reply): We have no objections to shortening the notification period set out in Article 31ª ("payment card schemes shall communicate scheme rules and fees unambiguously in a transparent and consistent manner to the payment service providers….") from 9 monts to 6 months. SK (MS reply): We agree. SI (MS reply): We agree.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	SE (MS reply): Yes. PT (MS reply): PT agrees with the newly suggested notification period but believes complimentary provisions may be included to dully assure the new expectations introduced via Article 31a PSR are dully enforced and properly supervised. NL (MS reply): Yes, we agree with the amendments regarding the notification period (shortening the period to communicate changes on scheme rules and fees from 9 to 6 months). LV (MS reply): We support. LU (MS reply): OK.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	IT (MS reply): IT. We do not oppose the proposal; a notification period of 6 months is acceptable. IE (MS reply): We can agree. HR (MS reply): We agree with the proposed amendments regarding the notification period of 6 months in Article 31a PSR. FR (MS reply): We agree with the amendments on notification period. FI (MS reply): FI: Yes. EL (MS reply): EL: We agree.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
Q5. Do you share the concerns about the report published by the Commission and are you in favour of obliging the Commission only to share this information with NCAs (instead of publishing the report)?	DK (MS reply): Yes. Denmark supports that the report should not be made public and only shared with the NCAs. The NCAs could make use of the detailed information in the NCAs' supervision and enforcement of the suggested article. Denmark pointed to the risk, that a publication of such fees, rebates and other incentives may lead to even higher prices or dampening of the competition among schemes. The Danish Competition and Consumer Authority has seen such examples in the past in other markets where publication of prices lead to higher prices. In case the scope of the transparency requirement is extended to acquirers, then the information becomes even more sensitive. DE (MS reply): This would depend on the type of data presented in the report. If the report contains competitively sensitive data, it would be preferable to share it exclusively with the NCAs. However, as argued under Q2, it is

Question	MS reply
	still not clear to us, what the data basis of the report would be. Hence, we cannot answer this question at this stage. CZ (MS reply): We don't share concerns, but we are flexible about it. CY (MS reply): We are flexible regarding the obligation of the Commission to only share this information with NCAs or to publish the report. We understand the benefits of being more transparent and are open to assessing whether certain aspects need to be treated as confidential. BE (MS reply): BE: Transparency should not be a problem for the market. However a solution as proposed by Sweden to have a public report and one for NCAs (with more sensitive data) could also be envisaged in order to ensure a right balance between enhanced transparency on scheme fees and fair competition among card schemes. AT (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	AT: Subject to our caveat regarding the IFR as the more suitable framework for fee transparency and in line with the view of most Member States, a report that is being published should exclude commercially sensitive data. ES (MS reply): We share the concerns highlighted by the Member State that publishing such detailed information on fees may lead to even higher fees and therefore dampen the competition among card schemes and we agree to the proposed approach to share this information with NCAs instead of publishing it. The NCAs would then have detailed information enabling them to supervise and enforce Article 31 a. SK (MS reply): Flexible, not against sharing only with NCAs. SI (MS reply): /

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	SE (MS reply): It is fine with us if the report is not published, if it means that more information can be shared with the NCAs. It should however be possible to publish some type of summary or conclusions. PT (MS reply): PT would welcome the publication of a COM's report to be accessed by the public, which is closely aligned with the transparency objective pretended to be introduced with these provisions. However, we would not oppose having a more detailed version of the report, or additional data sets, to be shared only with the NCA. The public at large may have access only to a report that aggregates data and does not individualise specific entities. NL (MS reply): Yes, we do share those concerns as it concerns quite competition sensitive information. However, it's not very transparent towards the market and general public if the Commission shares this information with NCAs only instead of publicly publishing the report. We would like to ask DG COMP to provide advice on this matter. LV

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	(MS reply): We can agree, as this could indeed have a significant impact on price regulation among market participants. LU (MS reply): We believe that the publicity of reports will positively contribute to the general policy objective of transparency. IT (MS reply): IT. We are in favour of making scheme fees public, which can also be published on company websites. IE (MS reply): We do not share such concerns, and we note that if a legislative proposal were to be submitted by the Commission based on Article 108 it would need to be accompanied by a report. We can support the Commission only sharing the reports with NCAs. HR (MS reply): We are in favour of obliging the Commission only to share this information with NCAs

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	FR (MS reply): Given the importance of such topic that has gained a lot of political attention, we think it is key to have a report published by Commission to ensure that all institutions (Member States, NCAs, European Parliament) have access to all necessary information in order to envisage any further regulatory action. However, topics dealing with commercial secrecy like item (a) (ii) (rebates and incentives) could be placed in a confidential version of the report only disclosed to NCAs. FI (MS reply): FI: We would favour an approach where detailed information would be shared only between authorities, and only a general-level-report would be published. This would tackle also the concern that particularly acquiring-fees would be business-sensitive information. EL (MS reply): EL: We think it is better that the report not be published; instead, the Commission should share this information with NCAs.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
Q6. Do Member States wish to include only scheme operators or also processing entities and processing fees in the transparency obligation under Article 31a PSR?	DK (MS reply): No. Denmark do not wish to include further. DE (MS reply): We tend to include only card scheme operators. In our view, processing entities don't need to be addressed, in particular, since there seems to be more (functioning) competition among processors than in the (international) card scheme market (see e.g. recent Eurosystem/ECB Report on card schemes and processors). Thus, in the sense of a lean regulation, the provision should focus on areas where there is a stronger consensus that regulatory intervention would truly be beneficial. CZ (MS reply): We don't understand the difference between scheme operators and payment card schemes. Does that mean a payment card schemes under Interchange Fee Regulation, in Article 2(16)? If you mean a subject, then it's a payment card scheme operator and we could agree on this. Otherwise, the answer is NO CY (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We have no comments. BE (MS reply): BE: no strong position here but we are ready to consider any suggestion aimed at strengthening the transparency obligation. AT (MS reply): - SK (MS reply): The broader the scope the higher level of transparency achieved. SI (MS reply): / PT (MS reply): PT conceptually agrees with the intention of also encompassing fees charged by processing entities, with the aim of ensuring a level playing field in the market by imposing transparency obligations equally to all stakeholders.

Question	MS reply
	Yet, we would advise the PRES PL to verify if the new obligations resultant from this scope expansion are not already imposed via other pieces of legislation. It is essential that these provisions do not reflect measures presently in place. On a final note, we highlight fees collected by processing entities are not directed at the final consumer, meaning the urgency for greater transparency to merchants, the intended goal of this initiative, is not the same as the other ones discussed so far. In this advanced stage of the negotiations, we would advise prioritising compliance of the put forward measures, rather than trying to further broaden its scope. LV (MS reply): Yes, we agree that processing entities and fees should be included in the transparency requirement. Without this element, the fees do not show the whole picture. LU (MS reply): In order to ensure a maximum of transparency along the whole payment eco-system, we would be open to consider scoping in processing entities and processing fees. IT

Question	MS reply
	(MS reply): IT. While we agree in general with enhancing transparency (see Q1, also with regard to coordination with IFR) and as such we are not contrary to this proposal, before answering this question the envisaged role of processing entities should be clarified, including the definition of processing entities and related activities: would they have to comply with disclosure requirements toward card schemes/acquirers or merchants? In particular, we should avoid too many layering of disclosure requirements toward merchants. We deem it necessary to know the proposed changes to Article 31a PSR before specifically assessing this proposed expansion of the scope of this Article. IE (MS reply): Processing entities and processing fees should be included – the more transparency the better for consumers and merchants. HR (MS reply): We have no comments. FR (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We are opened to include processing fees in the transparency obligations under Article 31a PSR since they are part of the unilaterally imposed scheme fees. FI (MS reply): FI: We do not have a firm view on this, but in principle it would be beneficial to extend transparency requirement to all fees charged. EL (MS reply): EL: Also, we consider that processing entities and processing fees should also be subject to the transparency obligation.
Presidency Discussion Note: Discussion on safeguarding of funds held in settlement accounts with payment systems (WK 4333/2025 INIT)	
Q1. Do Member States accept that PSU funds held in settlement accounts with designated payment systems should be considered as safeguarded for the purpose of Article 9(1) PSD3 subject to the above revised conditions included in Recital 31a and Articles 9(1a) and 9(7) PSD3?	DK (MS reply): In general, we are still sceptical towards the possibility of safe-guarding funds in settlement accounts. Funds held in settlement accounts will not be the PSU's – it will belong to the PSP. And the PSP will in most cases need to keep

PUBLIC

Question	MS reply
	additional liquidity in case of unforeseen payments (e.g. in an instant payments world). This means that in any event, funds of the PSUs will be comingled with funds of the PSP – and the safeguarding could be challenged in the case of bankruptcy. We would thus prefer that this option is dropped. We remain unconvinced that it will work when faced with the operational realities of such settlement accounts. Additionally, we have two comments on safeguarding in general. Firstly, we think it is quite important that government bonds can be used for safeguarding. Secondly, given the way the international card schemes operate, the requirement that funds cannot be commingled at any point cannot to our mind be fulfilled. The funds will be received commingled, and PIs will often receive less funds than what they owe their customers (e.g. due to charge-

PUBLIC

Question	MS reply
	backs etc). Thus, the requirement cannot be fulfilled before the funds are actively safeguarded by the PI. There should therefore be included some kind of timeframe for the safeguarding to occur. This could for instance be "as soon as possible" or "without undue delay" or another timeframe indication that could be deemed reasonably quick. We would be happy to provide a drafting suggestion in the written comments and have also done so in our comments for the consolidated PSD3 table. DE (MS reply): On the level of principle, we fully support the effort to simplify the access to and the usage of settlement accounts by Non-Bank-PSPs. However, we still do not see how the (German or European) legislator could oblige the central banks to maintain such accounts or change the chosen design as "own funds accounts" of payment/e-money institutions due to the precedence of the provisions of the ESCB Statute (Art. 17, 22) over the provisions of PSD2 (or the ZAG as national implementation law). The central banks are rather free (= "at their discretion") to open such

PUBLIC

Question	MS reply
	accounts either not at all or (a majore ad minus) only as "own funds accounts". The Eurosystem has decided not to offer "safeguarding accounts" (see https://www.ecb.europa.eu/pub/pdf/legal/ecb.leg_dec_2025_2.en.pdf). We would urge the PCY to clarify how to cope with this dispute before we agree on such proposal in the council. CZ (MS reply): We do accept that PSU funds held in settlement accounts with designated payment systems should be considered as safeguarded. Article 9 PSD3, paragraph 7, first subparagraph we think this is too extensive competence for the EBA the ECB and relevant national central banks should be included in the process of drafting RTS as it is the issue of payment systems oversight. Article 9 PSD3 is also a significant shift from Article 10 in PSD2 further analysis is needed with regard to some details (i.e. how to approach the prohibition of commingling of funds). We have a scrutiny reservation on recital 31a; especially last sentence. CY (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We have no comments. BE (MS reply): BE: Whilst we fully understand the goal of ensuring non-bank PSPs need not to use their own funds in the payment system while safeguarding separately (outside the payment system) all incoming payments in the payment system, we have concerns with this approach: • first off, it seems to hollow out the ECB decision on not providing safeguarding accounts which is thereby cimcumvented. • The impact on the Eurosystem Central Bank operators of designating settlement accounts as safeguarded seems unassessed in case of the insolvency of a particular non-bank PSP participant in the SFD-designated payment system. Would the Eurosystem CB operator be in the position of the credit institution providing safeguarded accounts when it comes to the settlement account in T2 in such a case? • the new wording of Article 9, new paragraph (1a) allows for funds from incoming payments to be considered as safeguarded. However, outgoing payments may far exceed in a given 24-hour cycle the incoming payments. Given the co-mingling prohibition, how is the non-bank PSP to solve this issue? A second settlement

Question	MS reply
	account containing own funds pertaining to the non-bank PSP? Should the CB operator be verifying this kind of set up ex-ante and on an on-going basis? Should the NCA?; a lot of questions arise We **<u>strongly disagree</u>** with this new wording in the new recital (31a) PSD3: "*Where a payment institution uses an insurance policy or some other comparable guarantee from an insurance company or a credit institution to safeguard the funds of payment service users, it should be able to use both its funds and the funds of payment service users in the same settlement account.*" In Belgian national transposition Law of 11 March 2018 (PSD2 transposition) we have considered <u>the requirement to never co-mingle as an absolute one</u>, utterly <u>regardless</u> of which method of safeguarding is afterwards employed by the non-bank PSP. The proposed text by the Presidency would destroy this key pillar of our safeguarding approach and we how an account commingling client's funds and PI's Own funds could comply with article 10 which provides that "*2. Payment institutions that provide one or more payment services, shall only hold <u>or provide to its payment service users</u> payment accounts which are used exclusively for payment transactions.* AT

PUBLIC

Question	MS reply
	(MS reply): **AT:** We are open for the proposed suggestion regarding settlement accounts as safeguards and the attached conditions. ES (MS reply): We have concerns regarding the proposal that settlement accounts with designated Payment systems should be considered as safeguarded for the purposes of Article 9 (1) and subject to the revised proposed conditions. Liquidity needs must not be in detriment of adequate safeguarding. SK (MS reply): We do accept. It is an important step towards making SFD work. SI (MS reply): / SE (MS reply): First of all, we wonder whether the proposal is to be understood as a mandatory requirement for the payment system provider to provide dual accounts to non-banks to make the separation of funds possible? Or will

Question	MS reply
	this be up to the payment systems operator to decide? We would prefer the latter. We would also like to stress the need to make sure that the proposal is aligned with national insolvency regimes, including EBA's technical standards. Secondly, we would like to comment on another part of this article (para 1, second subparagraph (b)), that is not mentioned in the discussion note. We think that it should be possible to invest funds in secure, liquid low-risk government bonds, not just assets issued by institutions. This issue has been raised by several Member States before and we think this subparagraph needs to be amended to reflect this. PT (MS reply): As previously stated, PT recalls that safeguarding accounts are distinct in nature from settlement accounts, to which most of the criteria suggested by the PRES PL will apply only for non-bank PSP. We can follow the reasoning of the proposal to try to limit the funds held in settlement accounts to the minimum necessary, but as with respect to the other ones, we do not comprehend at this time their respective value added. NL (MS reply):

PUBLIC

PUBLIC

Question	MS reply
	We have some questions about what this would entail in practice: • How does this relate to the funds that are not in the payment system? How will it be made clear to consumers that those funds are not in the same way safeguarded? • How can the Eurosystem guarantee the safety of their payment system when they are not always the ones supervising PSPs? • How does this relate to a level playing field between PSPs and banks? Since banks are not allowed to use payment systems to safeguard, not even when they deposit e-money tokens when they have a license under MiCAR. Are electronic money institutions thus offered more possibilities to safeguard than banks when using e-money? LV (MS reply): We accept that these funds should be considered safeguarded. However, there are parallel fora opinions circulation of the opposite. If the regulation specifically states this and solves all the uncertainties, and the issues with SFD and ECB are agreed upon, then definitely the preferred version is that the funds that temporarily are situated in settlement accounts within the system and are meant for payments are still considered to be safeguarded.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	LU (MS reply): We are open to this possibility. LT (MS reply): We strongly support the proposed amendments. It covers concerns raised by several MSs regarding risks, received fees and other. We once again emphasize the importance of these provisions in order to ensure the possibility for payment institutions to participate in payment systems and provide their services smoothly, and also to have a possibility to compete with other market participants. Without a proper solutions payment institutions will face a lot of risks – i.e. risk of inability to properly manage their liquidity in the payment system, operational risk when having to frequently move funds between settlement account and safeguarding accounts in credit institutions, risk to breach IPR requirements to provide instant payments. Therefore, it is of utmost importance to find a solution; and the current proposal ensures that, also covers risks, which are raised by some MSs. IT (MS reply): IT. Without prejudice to our previous comments made for the WP of last February, before providing any comments on the specificities of the proposal, we would like to express some concerns related to the compatibility of para. 1a of Art. 9 of PSD3, with para. 1, art. 3 of ECB decision 2025/222 on safeguarding accounts (Eurosystem central banks shall not offer or provide safeguarding accounts to NB-PSPs or to crypto-asset service providers).

PUBLIC

Question	MS reply
	To this end, we would like to seek a clarification from the ECB: in particular, it would be helpful to know whether the ECB will consider confirming the content of its decision on this issue or if it is evaluating reviewing it in light of the Presidency's proposal in the PSD3/PSR negotiations. IE (MS reply): We agree that such funds in settlement accounts with designated payment systems can be considered safeguarded until the end of the business day following the day when they are received and would note that this approach is essential to enable non-bank PSPs to participate effectively in SFD payment systems. We consider that the clarification in Recital 31a that commingling of funds in the settlement account is permissible where safeguarding is by way of an insurance policy/other comparable guarantees should also be reflected in Article 9(1a). HR (MS reply): In general, we are not against the proposal, however, we believe that it needs to be aligned with ECB policy. We have a question related to this proposal - in the case where part of the safeguarded funds is protected in settlement accounts and the other part is

PUBLIC

Question	MS reply
	covered by an insurance policy or some other comparable guarantee from an insurance company or a credit institution, does the "no commingling" requirement apply to all safeguarded funds or just to the part that is held in settlement accounts? In our view, "no commingling" requirement should not apply to the part of the funds which is covered by an insurance policy or some other comparable guarantee. FR (MS reply): It is in our collective interest for payment institutions to be able to directly access to designated payment systems following the changes brought by the IPR. However, we still have concerns at this stage: We support the fact that payment institutions should be required to ensure that all commissions/fees are separated from customers' funds « without undue delay », with reference to EBA RTS to define the implementing procedures. However, these funds would be safeguarded with entities that do not have the same prudential requirements than credit institutions with CRR requirements (as a reminder, the SFD doesn't lay down any prudential requirement): (i) Where a notified payment system (other than a systematically important payment system/SIPS) is operated by a non-bank PSP, this proposal would

PUBLIC

Question	MS reply
	allow non-bank PSP to provide safeguarding accounts even though the non-bank PSP prudential requirement are less stringent than the requirements applicable to credit institutions. (ii) Where a notified payment systems (other than SIPS) is operated by a corporation, without banking or non-bank PSP licence, the proposal will allow a company to provide safeguarding accounts, even though this corporation is not required to comply with prudential requirement such as those under PSD2 or CRR. This should be tackled to avoid serious financial stability issues that could stem from such proposal. The previous approach mentioned in LT non-paper was preferable. FI (MS reply): FI: We agree with the principle, that the funds held in settlement accounts would be considered as safeguarded. However, the key issue here is that national insolvency law can protect customer funds from third-party creditors only if those funds are segregated from own funds. The recital and the EBA-mandate provide the opportunity to commingle funds, leading to uncertainty whether the MSs should protect those commingled funds as well. Thus, we would propose to explicitly state that the obligation of MSs

PUBLIC

Question	MS reply
	to insulate customer funds from third party creditors would apply only to segregated funds. EL (MS reply): **EL:** We are still of the view that this issue is complex and requires further analysis rather than simply assume that settlement accounts in payment systems should be considered as safeguarding accounts. Settlement accounts at payment systems, should only hold funds for settlement and prefunding, while balances on such accounts cannot be considered as safeguarding accounts of users' funds.
Discussion Note: Treatment of payment transactions with EMTs in PSD3/PSR **(WK 4264/2025 INIT)**	
Q1. Do MS agree with the proposed changes in the first subparagraph of Recital 16 PSD3 and in the first subparagraph of Recital 29 PSR?	DK (MS reply): Denmark agrees with the proposed change. DE (MS reply): We agree. CZ

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): Yes. CY (MS reply): We have no comments. BE (MS reply): BE: We are not convinced that defining in PSR/PSD3 that EMTs are e-money regardless of whether they meet the definition of e-money is a good way forward. A token either meets e-money's definition or it does not. The solution is aligning the e-money definitions between MiCAR and PSD3, not considering all EMTs as e-money. Furthermore, the proposed way forward is only a half solution. When a case presents itself (issuer of a particular token) to an NCA, we will still need to make an assessment of whether it is an EMT or not. That is done by determining if it is e-money in the first place. AT (MS reply): **AT:** We agree. ES

PUBLIC

Question	MS reply
	(MS reply): We have reservations about the following amendments in **bold.** "*Regulation (EU) 2023/1114 lays down that electronic money tokens**, as defined in that Regulation,** shall be deemed to be electronic money. **This is regardless of whether the electronic money tokens meet the definition of electronic money in this Directive and Regulation xx [PSR]**. Accordingly, references to electronic money in this Directive should be understood to include electronic money tokens, unless otherwise stated **in this Directive**, and electronic money tokens should be included, as electronic money, in the definition of funds*". "*Regulation (EU) 2023/1114 lays down that electronic money tokens**, as defined in that Regulation,** shall be deemed to be electronic money. **This is regardless of whether the electronic money tokens meet the definition of electronic money in Directive xx [PSD3] and this Regulation**. Accordingly, references to electronic money in this Directive should be understood to include electronic money tokens, unless otherwise **stated in this Regulation**, and electronic money

Question	MS reply
	tokens should be included, as electronic money, in the definition of funds". In our view, EMT fall within the definition of funds as a necessary consequence of their consideration as electronic money as per article 48(2) of MiCAR. Therefore, we would prefer reinserting the eliminated reference according to which EMT should be included in the definition as funds, as electronic money. That is, for both Recitals, the end of the last sentence contained in the PCY proposal should read: "(…) and electronic money tokens should be included, as electronic money, in the definition of funds. […]". We do agree with the amendments on page 3 of the PCY proposal to the definition of funds in several Recitals and Articles in PSD3 and PSR, to clarify that electronic money includes electronic money tokens. SK (MS reply): We can support the proposed changes. SI (MS reply): /

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	PT (MS reply): PT agrees. NL (MS reply): The addition of "as defined in that Regulation" seems to be redundant, as it is already clear that the definition of that regulation is being followed by stating "lays down that". LV (MS reply): We support the proposal. LU (MS reply): Q1-Q10: under further scrutiny. IT (MS reply): IT. We do not agree with the amendments to Recitals 16 PSD3 and 29 PSR that would insert the following: "*This is regardless of whether the electronic money tokens meet the definition of electronic money in this Directive and Regulation xx [PSR]*". It should be removed as such a statement in the

Question	MS reply
	Recital would create uncertainty as to the legal qualification of EMTs, which would jeopardize the reading of PSD3/PSR provisions and complicate the interplay with MiCAR. IE (MS reply): We agree to the clarification that EMTs are regarded as e-money, unless specifically scoped out by PSD3, regardless of whether they meet the PSD3 definition. HR (MS reply): We agree with the proposed changes, if they do not pose a legal problem due to the inconsistencies between the definition of electronic money in PSD3 and electronic money tokens in MiCA. FR (MS reply): We don't oppose to such changes brought to Recital 16 PSD3 and Recital 29 PSR. It is indeed in line with Article 48 (3) MiCAR as exposed in the Presidency note. EL (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	EL: Acknowledging in a recital that EMTs are e-money that may not meet the base e-money definition is problematic and not legally sound – we would be against of including it in the recital or considering it as acceptable. The issue can only be addressed by level 1 text amendment. So far MS have been hesitant to change the core e-money definition to avoid creating market turbulence/interpretative challenges for existing business models. **Having this in regard, there may be merit in exploring a solution where the base e-money definition becomes a more general one and is further broken down to have two variants (a) "traditional e-money" (replicating the current EMD2 definition) and (b) "cryptoasset-based e-money" i.e. EMTs**. Existing market solutions would fit the first variant – without any changes to their regulatory treatment. This approach enables PSD3/PSR to potentially setup different rules (or a subset of current e-money related rules) for EMTs. Thus "traditional e-money" may share some common (base e-money) features with EMTs but can also differ from it (which is exactly the case we have at the moment). This can also take the form of a common set of rules for all (generic) e-money and specific rules for each separate kind of e-money.
Q2. Taking into account the above, do MS consider that more clarifications regarding the definition of funds in PSD3 and PSR are needed?	DK (MS reply): Denmark agrees with the proposed change.

PUBLIC

Question	MS reply
	However, the change does not account for the fact that providers of payment services merely with EMTs (and other funds) will be required to obtain a CASP-license, when transfer services under MiCA contains payment services. This should be seen in context of our position on Q3. DE (MS reply): We welcome the changes to Recital 16 PSD 3 and Recital 29 PSR. Further, we do think that it is necessary to change the wording of 'e-money, including EMTs' to 'e-money and EMTs' in the whole text, in order to reflect that EMTs do not have to meet the requirements of the e-money definition. CZ (MS reply): No. Partially, the issue is solved by excluding limited network from MiCA, e. g. recital 26 MiCA. CY (MS reply): We have no comments. AT

PUBLIC

Question	MS reply
	(MS reply): - SI (MS reply): No. PT (MS reply): No. NL (MS reply): No. LV (MS reply): This needs to be carefully reviewed in the light of the recent Commission opinion of the interpretation of the e-money funds are considered e-money only if the e-money issuer has direct contractual relationship with the e-money holder, including the merchants that would accept the e-money. This new interpretation of the old definition results in the situation that the EMTs definition, apart from the technical differences, also differs in the

PUBLIC

Question	MS reply
	application of EMT. EMT could be uploaded to VISA card, e-money when uploaded on VISA card will be considered scriptural money from now on. IT (MS reply): IT. No. IE (MS reply): We consider there to be sufficient clarification. HR (MS reply): There is no need for more clarifications regarding the definition of funds. FR (MS reply): We haven't identified any further clarification that would be needed regarding the definition of funds in PSD3. EL (MS reply): **EL:** Having regard to our comments in Q1, there are also two options:

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	Option 1: Funds encompass all e-money (traditional and EMT). Therefore, EMT transfers are still considered payment transactions, following the existing approach where exemptions are introduced for particular types of EMT transfers. In addition, under this option, the EBA could be mandated to develop technical standards in relation to the differences in fundamental characteristics between EMTs and traditional e-money, and how such differences should be resolved in practice, for example regarding unique identifiers and VoP, contractual relationships between the PSP and the PSU, safeguarding requirements and revocability of transactions. **Option 2**: A fundamental change is introduced in the base "funds" definition to cover only "traditional e-money" and not EMTs. The reasoning would be that EMTs have more in common with ARTs in MiCAR (as stablecoins) rather than traditional e-money and all stablecoins should have broadly a similar regulatory treatment. This changes all the approach considered so far, as no EMT transfer will be automatically a payment transaction (i.e. this effectively invalidates the MiCAR/PSD3 interplay discussion). In this case, the applicable rules for EMTs would be those of MiCAR and no additional rules should be considered within PSD3/PSR specifically for EMTs. This is effectively a reverse approach to what the council has been exploring so far.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
Q3. Do MS agree with the proposed changes in subparagraphs (2) to (5) of Recital 16 PSD3 and in the second subparagraph of Recital 29 PSR? If not, please explain why.	DK (MS reply): Denmark agrees on the position that custody and placing not in it-self should constitute payment services, and with the exemptions for specific payment transactions. Denmark also agrees that transfer services under MiCA – in itself and in combination with custody services – can be interpreted as containing payment services, if the underlying assets are EMTs. In that regard, it should be underlined that guidance is necessary to understand how to classify specific payment services in the context of a DLT-infrastructure. For example, when is the services offered acquiring compared to execution of payment transactions. And could the combination of transfer and custody constitute money remittance. Denmark is uncertain whether the requirement of double licenses for providers of payment services merely with EMTs (funds) is in line with the intention of MiCA being a supplementary to existing

PUBLIC

Question	MS reply
	regulation. It implies that such PSPs will be subject to requirements under both the PSP-framework and MiCA, for example capital requirements. We are not certain whether a solution is achievable by amending the PSP-framework. For example, by specifying that EMTs in the context of payment services should not be considered crypto-assets. From a perspective of technology neutrality this would also raise a need to consider how to substitute requirements under the PSD-framework with requirement under MiCA. DE (MS reply): We generally support the direction of travel. In regard to the service of custody and administration it should be clarified in Recital 16 PSD 3 that such service qualifies as a payment service, "where a crypto-asset service provider offers this service and also provides transfer services for crypto-assets on behalf of clients with electronic money tokens, or other payment services, then the respective services would qualify as payment services, unless such transfers are covered by a specific exclusion from the scope of this Directive and Regulation xx [PSR]."

PUBLIC

Question	MS reply
	Further, regarding the service of "placing of crypto-assets" a clarifying sentence should be added, regarding such constellations in which this payment service could qualify as a payment service. CZ (MS reply): Yes. We appreciate the clarifications made by the presidency. In general, we consider the "execution of orders" as crypto-asset service that should not automatically require additional licence for payment services. Therefore we support additional exemption as proposed by the presidency under question No. 5. CY (MS reply): We have no comments. BE (MS reply): BE: fully supportive of the PCY proposal. AT (MS reply): **AT:** We agree. ES (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We have no objections to the objective of the proposal aimed at avoiding a potential overlap between CASP services under MiCA and payment services under PSD3/PSR, and in line with one MS suggestion to clarify that the service of custody and administration of EMTs as defined in MiCA is not a payment service per se, but that the additional service of enabling transfers to and from custodial wallets would be a payment service, taking into account the European Securities and Markets Authority (ESMA) Q&A 2071/2024. However, the specific drafting proposed by the presidency in our view does not provide the required **clarity for the case where custody and administration services of EMTs are provided together with payment services** (transfer of EMTs or others). The proposed drafting states: where such custody and administration of EMTs is provided together with transfer services of EMTs or other payment services "then the respective services would qualify as payment services". As per this wording, we believe it is not clear in this scenario if the custody and administration of EMTs itself entails the provision of payment services and, if so, what type of payment services. It must be taken into account, in this sense, as pointed out in the PCY, that unlike PSD2, the

Question	MS reply
	payment services listed in the Annex to PSD3 no longer refer to "the operations required for operating a payment account". In addition, we deem important to ensure that business models consisting of a CASP using tokenised e-money to only operate within a DLT for settlement purpuses are not subject to double licence regime, both under MICA and PSR In our view the referred business model should only require licence under MICAR, since the referred use of EMTs would not be associated to the execution of any payment service Following this, we suggest to include the referred use case under the exclusions of PSR in Article 2(2) and to also modify Recital 29 PSR accordingly. SK (MS reply): We agree. SI (MS reply): Yes. PT (MS reply): PT agrees.

PUBLIC

PUBLIC

Question	MS reply
	NL (MS reply): We agree with the suggested approach but recommend referencing recital 90 MiCAR, which states that providing custody and administration of crypto-assets on behalf of clients, the placing of crypto-assets, and transfer services for crypto-assets on behalf of clients might overlap with payment services. LV (MS reply): We support changes. Already in the February WP materials we expressed our support for amendments to the MICA-related recitals and articles. IT (MS reply): IT. Yes, we do. Regarding the "exchanging of EMTs for funds or crypto-assets", we should clarify whether, when the CASP does NOT act in its own name and instead acts as an intermediary between the parties, we have or not an exchange service under MiCAR, as it would appear more similar to the operation of a trading platform, considering that the definition of exchange services requires CASPs to use proprietary capital. This clarification is preliminary

PUBLIC

Question	MS reply
	to any assessment as to the potential qualification of exchange services as payment services IE (MS reply): We can agree with the proposed drafting. HR (MS reply): As a general comment on all proposals related to the scope of application of PSD3/PSR to services with EMTs, we would support any proposal whereby the transfer services with EMTs for investment or trading activities would be excluded from the scope of PSD3/PSR, leaving in scope only transfer services where EMTs are used to pay for goods or services or for *peer-to-peer* transactions. FR (MS reply): We agree with such edits. EL (MS reply): **EL:** We agree with most of the changes. We do not agree with "*However, where a crypto-asset service provider offers this service and also provides transfer services for crypto-assets on behalf of clients with electronic money*

PUBLIC

Question	MS reply
	tokens, or other payment services, then the ***respective services*** *would qualify as payment services."* In this case the payment service status is given by the "EMT transfer service" not because of custody – we do not see a need to entangle the two. If CASP provides only EMT custody, then it is not a payment service. If a CASP provides EMT custody and EMT transfer service for those EMTs then it may be offering a payment service (subject to the exemptions) similar (but not equivalent to) a credit transfer irrespective of the custody service – the services don't need to be perceived as a bundle.
Q4. Do MS agree with the proposed exclusions from the scope of PSD3/PSR regarding EMTs in Article 2 points (a1), (l1), (h1) and Recitals 29a and 29b PSR? If not, please explain why.	DK (MS reply): Denmark agrees with the proposed changes. DE (MS reply): We generally support the direction of travel. In particular, we support the proposed amendment of the exclusion in Article 2(2) (h1). With regard to Recital 29b PSR, however, we think that the proposed amendments could contradict the wording of Article 2(2) (a1) given that such Article considers payment transaction "without any" intermediary involved. CZ

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	(MS reply): Yes. We do agree. CY (MS reply): We have no comments. BE (MS reply): BE: We concur with PCY approach, however we do think that the wording in recital 29 PSR on 'investment or trading purposes/activities' should be removed. This will be impossible to determine/assess by NCAs as it seeks to determine purpose of transactions. AT (MS reply): **AT:** We agree. ES (MS reply): Yes, we agree with the referred exclusions to minimise the burden. We believe the referred exclusions don´t undermine consumer protection:

PUBLIC

PUBLIC

Question	MS reply
	Indeed, in relation to payment of any settlement amounts or income gained in the context of an investment in EMT, in our view any such amounts should be considered as part of the settlement or investment activities and, therefore, should be excluded under PSD3/PSR. We propose introducing express reference to such payments with EMT, as was included in the December Hungarian Presidency Proposal, in order to avoid any possible doubts on whether such settlement transaction would or not be subject to PSD3/PSR in line with the amendments proposed to Recital 16 PSD3 and Recital 29a PSR. Additionally, we propose eliminating the word “including” from Recital 29a PSR. The use of the word “including”, generates doubts on whether in the case where the CASP is acting in its own name, such activity could also entail providing payment services and such doubt should be avoided: “This concerns in particular the exchange by crypto asset service providers of electronic money tokens for funds or crypto assets, regardless of whether, including where the crypto asset service providers are intermediating between buyers and sellers, or acting in their own name as sellers or buyers of electronic money tokens.” SK

PUBLIC

Question	MS reply
	(MS reply): We agree. SI (MS reply): / PT (MS reply): PT agrees. NL (MS reply): We are not in favour of the exclusion of (h1) since this type of action leans close to being a payment and should be included in the scope. It could also lead to a risk of forum shopping. For example, CASPs may provide the business case for merchants to exchange their EMTs to scriptural money. LV (MS reply): We support the proposal. IT (MS reply): IT. Article 2, Points (a1), (l1): we agree.

Question	MS reply
	Article 2, Point (h1): we agree with the 'extended' version to complement the exclusion, see Q5 ('*as well as payment transactions where ...*'). Recital 29a: for the sake of completeness, the words '*regardless of whether* […] *or acting in their own name as sellers or buyers of electronic money tokens*' could be kept. IE (MS reply): We agree with the proposed exclusions. HR (MS reply): We agree with the proposed exclusions. FR (MS reply): We agree with the proposed modifications of Article 2 (2) (a1), (h1), (l1) PSR. We would also like to see a modification in Article 2 (2) (h) PSR : (h) payment transactions related to securities asset servicing ***and crypto-assets services*** defined in Article 3 (16) of Regulation 2023/1114, including dividends, income, or other distributions, or redemption or sale, carried out by persons as referred to in point (g) or by ***crypto assets services providers***, investment firms, credit institutions, collective investment undertakings or

Question	MS reply
	asset management companies providing investment services and any other entities allowed to have the custody of financial instruments; On the Recital (29b) PSR, MiCAR doesn't define « self-hosted addresses » or « custodial wallets ». FI (MS reply): FI: In order to align recital 29a with the related Articles as well as to clarify the scope of the exemption we would have couple of drafting suggestions to recital 29, as follows: "Such an exclusion should **cover payment transactions in electronic money tokens facilitated**~~exchanges of electronic money tokens~~ as part of the provision of the service of exchange of crypto assets for funds, exchange of crypto assets for other crypto assets, operation of a trading platform for crypto assets, reception and transmission of orders for crypto assets on behalf of clients or execution of orders for crypto assets on behalf of clients, as defined in Regulation (EU) 2023/1114. **Such an exclusion does not cover payment transactions in other funds facilitated as part of provision of the aforementioned crypto-asset services. Furthermore,**~~However,~~ such an exclusion should not include

PUBLIC

Question	MS reply
	payment transactions in electronic money tokens facilitated as part of transfer services where, **for example,** electronic money tokens are used to pay for goods or services, for peer to peer payment transactions or payment transactions between payment accounts of the same person." Also, as a minor drafting remark on recital 29 b, it could refer to self-hosted address throughout the text (instead of referring to self-hosted wallet at the very end). EL (MS reply): **EL:** We agree
Q5. Do MS consider that additional exclusions are needed in Article 2 PSR, for example to complement the exclusion in (h1) to cover 'payments transactions carried out by a crypto-asset service provider where electronic money tokens are exchanged for funds or crypto-assets, as well as payment transactions where electronic money tokens are transferred between a custodial wallet or self-hosted address of a person and another custodial wallet of the same person that is used solely for the exchange of electronic money tokens for funds or crypto-assets', while clarifying in the recitals that this exclusion would not include transfer services where EMTs are used to pay for goods or services, for	DK (MS reply): Denmark agrees with the proposed changes. DE (MS reply): For now, we do not see need for further changes; however, we believe it would be prudent to align with EBA's no-action letter once t becomes available. CZ (MS reply):

PUBLIC

Question	MS reply
peer-to-peer payment transactions or for other payment transactions between payment accounts of the same person?	Yes, CZ can support the additional exemption as proposed. CY (MS reply): We have no comments. BE (MS reply): BE: no comment AT (MS reply): **AT:** We could be open to the exclusion in (h1) as proposed by the PCY. ES (MS reply): See comment above. We believe it is best to clearly and expressly include reference to all exclusions in Article 2 PSR, not only in the Recitals. SK (MS reply): We are open to consider further exclusions clarifying the setup. SI (MS reply): No.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	PT (MS reply): PT is flexible on introducing the suggested complement to the exclusion foreseen in (h1), as well as the respective needed amendments to the Recitals. With regards to additional exclusions, we do not identify at this stage a need to introduce further exclusions in Article 2 PSR. NL (MS reply): As also mentioned under Q4, we question exclusion of (h1), including its complementation. The transfer of EMTs between a custodial and non-custodial wallet should be in scope, if the CASPs can exert some influence over the payment transaction. This benefits consumer protection by incentivizing CASPs to use higher-quality DLTs for transactions. Additionally, we suggest including a disclaimer for users stating that when they transfer EMTs to a self-hosted wallet, the PSU assumes full responsibility once the EMT transaction from a custodial wallet to a self-hosted wallet is completed. PSUs should understand that they are responsible for managing their private key when using self-hosted wallets and cannot depend on a PSP or CASP for assistance. LV (MS reply):

PUBLIC

Question	MS reply
	We are very much in favor of this solution. Additionally, we would appreciate clarification on the last part – we would rather think that the custodial wallets, wallets holding stablecoins, EMTs would not be defined as payment accounts and not mentioned as such neither in the article nor in the recital. We are also in favor if the exclusion is expanded to the crypto payments to third parties as well. IT (MS reply): IT. We agree with the 'extended' version of (h1) to complement the exclusion ('*as well as payment transactions where …*'). However, compliance with this condition may be difficult to verify. We also agree with clarifying in the recitals that this exclusion would not include transfer services where EMTs are used to pay for goods or services, for peer-to-peer payment transactions or for other payment transactions between payment accounts of the same person. IE (MS reply): We support including an exclusion for transfers between custodial wallets/self-hosted addresses of the same person.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	HR (MS reply): See our answer to Q3. FR (MS reply): We don't agree with such proposals. FI (MS reply): FI: No, we do not see a need for further exclusions. EL (MS reply): **EL:** We agree with the additional exemption. Nevertheless, the fact that peer-to-peer EMT transfers are provided as a service by most CASPs would most probably effectively cancel out any benefit from the exemptions themselves, in terms of dual-authorization requirements.
Q6. Do MS agree with the proposed changes in Article 3(3a) PSD3?	DK (MS reply): Denmark agrees with the proposed changes. DE (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We appreciate the efforts of the POL PCY to further streamline the authorisation process of CASPs under PSD 3. However, in our view, we should be more ambitious in this regard. In particular, there are two dimensions to the question of authorisation processes that need to be addressed: 1. We need to ensure that the regular authorisation process for CASPs to obtain a PSD3-licence is as simple as possible. The POL PCY proposal for a Art. 3(3a) is a good starting point in this regard, however, we could imagine to simplify the process further e.g. by clearly spelling out the information to be handed in by CASPs or by setting a particular time frame for the completion of the authorisation process. 2. We need to carefully reflect on the necessity of dual licence regimes for CASPs and Payment Institutions providing payment services with EMTs. In particular, Art. 60 MICAR defines an array of notification options for different types of financial entities to perform certain crypto asset services. For payment institutions, however, there is no such option yet. We should consider adding a notification procedure to Art. 60 MiCAR for payment institutions. We have understood from the MiCAR-negotiations that such notification procedure was not applied in anticipation of the PSD 2 review.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	We have prepared a non paper with ideas how to further streamline the authorisation procedures and cut bureaucratic burden. CZ (MS reply): Yes. CY (MS reply): We do not object the proposed changes in Article 3(3a) PSD3. BE (MS reply): BE: We concur, but would urge to co-opt the wording in the No-action Letter drafted by the EBA in this regard. AT (MS reply): **AT:** We agree. Moreover, we could be open for a more ambitious streamlining as mentioned by the German delegation in the CWP on 4 April 2025. ES (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We do not have objections to the proposed changes which aim at streamlining the authorisation process where both PSD3 and MiCA would be required. SK (MS reply): We can agree. SI (MS reply): Yes PT (MS reply): PT welcomes the included amendment on information exchange between competent authorities and the account for the forthcoming EBA *"No-Action Letter on the interplay between PSD2 and MICAR in respect of CASPs transacting EMTs"*. NL (MS reply): Yes. LV (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We support the proposal. IT (MS reply): IT. We agree with the specific amendments to Article 3(3a) PSD3. We reserve to provide further comments on the more general issues on the interplay between PSD3-PSR/MiCAR as regards authorization/notification regimes. IE (MS reply): We can support an exchange of information provision to cater for separate PSD and MiCAR regulators in a MS, if deemed necessary by MSs in that situation. We question whether more prescriptive language might be necessary in addition to "where appropriate". HR (MS reply): We may agree with the proposed changes. We may also agree that PSD3 text could be further improved taking into account the content of the forthcoming EBA no-action letter, as long as such improvements serve the purpose of minimising the burden for CASPs and NCAs due to the application of two regimes to the same activity. In that connection, we believe that in some cases PSD licence for CASPs may not be needed.

PUBLIC

Question	MS reply
	Given that there is a possibility in Article 60(4) MiCA that EMIs can provide specific crypto-asset services by way of notification to the competent authority, without seeking an authorisation as a CASP, we propose the introduction of a similar notification regime in PSD3 for CASPs providing the transfer of EMTs, without seeking an authorisation as a PI. Such an approach would level the playing field for entities providing the same activities under MiCA and PSD3. FR (MS reply): We would prefer to avoid a dual authorisation for CASPs providing payment services with EMT. In our view, three situations should be distinguished: (i) A CASP provides payment services with EMT: such CASP shouldn't be subject to a dual authorisation as a payment institution. However, such limitation to dual authorisation would only be valid for payment services with EMTs. (ii) A CASP provides payment services with funds other than EMTs: the CASP shouldn't be entitled to provide payment services with funds other than EMT without being properly authorised as a payment institution.

PUBLIC

Question	MS reply
	(iii) A payment institution willing to provide payment services with EMTs would also be entitled to provide payment services with EMT, since EMT are to be considered as funds. EL (MS reply): **EL:** We support the changes, but also agree that the text needs further refinement.
Q7. Do MS agree with the proposed changes in Recital 6 PSD3?	DK (MS reply): Denmark agrees with the proposed changes. DE (MS reply): We are evaluating whether the current adjustments for electronic money institutions issuing EMTs are sufficient, or if further amendments are necessary – particularly with respect to electronic money institutions that also offer crypto-asset services. CZ (MS reply): Yes. CY

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): We have no comments. BE (MS reply): BE: no comment AT (MS reply): - ES (MS reply): We do not have objections to the proposed changes to reference EMI issuing EMTs as PI issuing EMTs. SK (MS reply): We can support. SI (MS reply): / PT (MS reply):

PUBLIC

Question	MS reply
	PT agrees. NL (MS reply): Yes. LV (MS reply): We support the proposal. IT (MS reply): IT. Yes, we do. IE (MS reply): We agree with the proposed changes. HR (MS reply): We agree with the proposed changes. FR (MS reply): We agree that issuers of EMTs will therefore be payment institutions providing e-money services under PSD3 after the merger of the e-money institutions and payment institutions regimes.

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	EL (MS reply): **EL:** We agree.
Q8. Do MS agree with the changes proposed in Article 9(1) PSD3?	DK (MS reply): Denmark agrees with the proposed changes. DE (MS reply): We generally support the direction of travel. However, in the drafting of Article 9(1) PSD 3 the special regime for issuers of significant e-money tokens needs to be taken into account. Hence, the Article should be adjusted as follows: "with the methods set out in Article 54 and 58 of Regulation (EU)." CZ (MS reply): Yes. CY (MS reply): We have no comments. BE (MS reply):

PUBLIC

Question	MS reply
	BE: no comment AT (MS reply): **AT:** We agree. ES (MS reply): We understand that the proposed modification in red aims to clarify that payment institutions issuing EMT must comply with the safeguarding methods of Article 54 of MiCA, to safeguard the funds received in exchange for the issuance of EMT. "*Member States shall require a payment institution which provides payment services as referred to in Annex I, points (1) to (5), or point (8), to safeguard all funds other than electronic money tokens it has received from payment service users or through another payment service provider for the execution of payment transactions, or where applicable the funds received in exchange for electronic money that has been issued, in one or several of the following ways: […]"* *[…] By way of derogation from subparagraph 1, and without prejudice to paragraph 4, where a payment institution issues*

Question	MS reply
	electronic money tokens, it shall ~~comply with~~ safeguard the funds received in exchange for the electronic money tokens in accordance with the methods set out in Article 54 of Regulation (EU)". We agree with the objective of the amendment, to clarify which are the applicable requirements. However, we have concerns that, through this proposed modification, the safeguarding methods of Article 9.1 of PSD3 will continue to apply to that payment institution issuing EMTs. This results from Article 54 of MiCA, which refers to the safeguarding obligations of Article 7 of EMD2, which ultimately leads to the application of Article 9 of PSD3 to the payment institution issuing EMT. To avoid this circular outcome, the reference that Article 54 of MiCA makes to Article 7 of EMD2 should be modified. SK (MS reply): We agree with the changes. SI (MS reply): / PT

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): PT agrees. NL (MS reply): Yes. LV (MS reply): We support the proposal. IT (MS reply): IT. Yes, we do. IE (MS reply): We agree with the proposed changes. HR (MS reply): We agree with the proposal to introduce clarification that payment institutions issuing EMTs should comply with the methods from Article 54 MiCA to safeguard the funds received in exchange for those EMTs. However, we would like to draw attention that Article 54 MiCA, beside regulating the methods for investment of funds received in exchange of

PUBLIC

Question	MS reply
	EMTs, also stipulates that those funds should be safeguarded in accordance with Article 7(1) of EMD2 which further refers to the application of PSD safeguarding requirements. In this sense, when introducing derogations for EMTs in Article 9 PSD3, it is necessary to take care that some of the requirements intended in Article 54 MiCA are not left out for EMTs, such as "no commingling" and insulation requirements. FR (MS reply): We agree that issuers of EMTs should only apply MiCAR safeguarding requirements. EL (MS reply): **EL:** We agree.
Q9. Are MS of the view that the provisions on the VoP service in Article 50 PSR should also apply to payment transactions with EMTs, except for payment transactions with EMTs between a selfhosted address and a custodial wallet? If so, do MS have any proposals on how this could be designed? And if MS are of the view that the provisions on the VoP service in Article 50 PSR should not apply at all to payment transactions with EMTs, please explain why.	DE (MS reply): We think that the obligation to provide the VoP service should not apply to EMT transactions. We do not think that it is easy to design such service. Even if self-hosted addresses are totally excluded from the obligation, one has to take into account the international nature of most blockchains. We further think that the onus should be on the supporters of the application of VoP to EMT transactions to sketch out how such a system could work. CZ

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	(MS reply): No, we are not in favour of extending the scope of VoP. It is still unclear how this system will work in practice and we consider its further expansion to EMTs to be premature at this stage. CY (MS reply): We have no comments. BE (MS reply): BE: Ideally, VoP should apply to payment transactions with EMTs. This for level playing field reasons. However, industry input is needed in order to correctly define an adequate unique identifier that can be leveraged to that end. AT (MS reply): **AT**: We could be open to this proposal. However, as one MS has mentioned in the CWP on 4 April 2025, the relevant identifier would have to be identified first. As the Commission has mentioned, self-custodial transactions should be excluded. ES (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We consider that the provisions on verification of payee are key for consumer protection and hence we would be in favour of extending this requirement to transfers with EMTs. Indeed, and according to Article 2(1)(f) of the SEPA Regulation, the SEPA Regulation does not apply to 'payment transactions transferring electronic money, unless such transactions result in a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN'. Despite transfers with EMTs not being under the scope of SEPA regulation, we consider that this provision can be analogically applied to EMT, and that hence the VoP provisions under Article 50 of PSR should also apply to credit transfers with EMTs (even if, as already mentioned, they do not fall within the scope of the SEPA Regulation. This is in line with the view of the majority of MSs that considered that VoP provisions should extend also to other credit transfers that are not covered by the SEPA Regulation, Nevertheless, and as highlighted in the DN, there are implementation issues, and question marks as when there are no 2 PSPs on both sides, in which case, this can technically not apply. But, we are aligned with the way of travel as to impose as a requirement VoP to transfer with EMTs where technically possible. SK

Question	MS reply
	(MS reply): No strong preference, might be costly, while bringing only limited benefits. Payment transactions with EMTs are not widespread yet, leaving the area relatively less regulated in comparison to the other types of payments might be justified with the aim to support the industry. SI (MS reply): It should be analysed if the proposed exception is in line with Transfer of Funds Regulation (TFR) Specifically, do transfers including self-hosted wallets (e.g. self-hosted to hosted, hosted to self-hosted), where CASPs are involved, require information about the payer and the payee? If yes, how does this impact suggested exception. PT (MS reply): PT is against expanding VoP requirements to payment transactions with EMTs and would like to raise 2 apparent concerns on the contemplated option. Firstly, and as recognised by the PRES PL, an analysis is still being conducted on extending said requirements to credit transfers directed at

PUBLIC

Question	MS reply
	accounts not identified by IBAN. Since EMT transactions can most likely be carried between such accounts, it might be premature to reflect on this issue now without having confirmed viability in this regard. Then, even if this is indeed the case, one must question whether imposing VoP requirements to transactions with EMTs is justifiable considering: i) the small size and emerging business model of the entities that provide such services, as well as ii) the current low usage of such services by the EU population at large, when compared with traditional payment instruments. Implementing such requirements may impose considerable investments and undue burdens to the entities providing these services, given the high costs associated with the operationalisation of VoP. This effect shall be especially evident for smaller players trying to enter the market with new and innovative services, which will be strongly hampered by these demands and may even deter them from carrying their intended activity. Moreover, in our view, the current initial stage of EMT transactions' uptake in our market may imply a reduced urgency and valued added in obliging the offering of a VoP service. NL (MS reply): We think that VoP should not be applied to all payment transactions with EMTs. We see the potential benefits for consumer protection, but we are

PUBLIC

PUBLIC

Question	MS reply
	also aware of how it would require a lot of work for the CASP. For this to be effective, EMT issuers and CASPs should maintain a database containing public keys associated with specific names. Although constructing such a database is feasible, there are associated costs that need consideration. We wonder whether these costs outweigh the rewards. We also want to highlight that a transaction between wallets is different than a traditional payment transaction, where IBAN/name checks are not always applicable. Moreover, we want to bring attention to the Travel Rule under TFR which determines the data that the originating CASP must communicate before or simultaneously with the transfer. It is up to CASPs to implement risk-based procedures to determine whether to execute a transfer. Creating a VoP seems to be contradictory to the Travel Rule. LV (MS reply): We do not support VoP service for transactions with EMTs. Probably, up to the point of access to the account in the VoP system, but no further. That is, at least what is outside the blockchain should be verified, but then there

Question	MS reply
	are private keys anyway, which are relatively long. If the first step were possible, third-party fraud could be reduced. IT (MS reply): IT.We are not opposed to extending the VoP service to EMTs , provided it is technically feasible. We acknowledge that applying the VoP to transactions involving a self-hosted address would likely not be possible. More in general, regarding the application of specific PSR provisions to EMTs (particularly when distributed ledger technologies are involved), please see our response to Q10. IE (MS reply): It makes sense to extend VoP requirements to EMT transactions if this is technically feasible. The goal of VoP is to reduce fraudulent transactions, from this point of view fraudsters could take advantage of any payment method which does not require VoP including EMT payments. However, further analysis is needed including industry input and a proper assessment of its feasibility including costs. HR (MS reply):

PUBLIC

PUBLIC

Question	MS reply
	In accordance with Regulation 260/2012, that Regulation does not apply to payment transactions transferring electronic money unless such transactions result in a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN. Therefore, we are of the view that the provisions on the VoP service should not apply to payment transactions with EMTs unless such transactions result in credit transfers to which those provisions apply. FR (MS reply): We consider that VoP services should not apply at all to payment transactions with EMTs. It is clearly a topic to be further thought and not to be imposed without proper assessment of its feasibility or in terms of costs. By definition a DLT environment doesn't rely on schemes like for traditional payment ecosystem. Thus require VoP services for payment transactions with EMTs would pose significant difficulties in terms of feasibility. EL (MS reply): **EL**: We agree with the statement included in the note that "that EMT transfers that do not result in a 'credit transfer or direct debit to and from a payment account identified by BBAN or IBAN' are not subject to the above mentioned VoP requirements in the SEPA Regulation." Therefore, there is

Question	MS reply
	no legal requirement to introduce VoP requirements for EMT transfers. If certain equivalent measures are deemed necessary, alternative means should be explored considering DLT specificities.
Q10. Do MS have any specific proposals for other amendments that they believe may be needed in PSD3/PSR to take into account the specificities of EMTs, or of payment transactions with EMTs, or of payment transactions with EMTs between a self-hosted address and a custodial wallet?	DE (MS reply): We can only reiterate that we need a full assessment, to what extent the requirements of PSR are feasible for EMT services. If the EBA letter provides such assessment, we should wait for its results before deciding on the application of particular requirements. CZ (MS reply): We propose that CASPs would still need a PSD authorisation for payment services, but we suggest streamlining the procedures (no double filing of documents; faster authorisation procedures etc). CY (MS reply): We have no comments. BE (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	BE: Discussion should be held or at least clarified in the legislative proposal in further detail on a few topics not discussed by the PCY in its note, i.e. transparency requirements, initial capital/own funds requirements, Open Banking provisions (discussions to be had), SCA requirements (should apply in full), etc. Cf also the EBA no-action letter on topics further suggested to discuss by EU co-legislators. AT (MS reply): - ES (MS reply): We do not have specific proposals on the referred. SI (MS reply): / PT (MS reply): PT does not wish to identify any further amendments at this moment. NL (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We wonder what the Presidency's view is on open banking and whether it should or should not apply to CASPs. The EBA has mentioned, although not yet definitive, that open banking should not apply. We also recommend stating that the open banking provisions do not apply to CASP or EMT-issuers. The implementation costs for EMT issuers and CASPs could be high without clear benefits from applying open banking provisions to EMTs. However, it should be included in the review clause to analyse to what extent the open banking provisions can add value to EMTs. The open banking provisions appear to have been designed without EMTs in mind and aim to challenge the incumbents, but the added value of specifying this to EMTs is unclear. Especially keeping in mind that CASPs do fall under the scope of FIDA. LV (MS reply): No comments. IT (MS reply): IT. Considering that the PSR negotiations are at an advanced stage and it would practically impossible to map all the provisions in PSD3/PSR in light of the specificities of EMTs and of payment transactions with EMTs,

Question	MS reply
	we suggest that the PSR should include a mandate for the EBA to develop draft regulatory technical standards (RTS) on how to apply the provisions of PSD3/PSR (in particular, of Titles II and III of PSR) to payment services in EMTs, especially when they are conducted on a DLT, i.e. on a network outside the control of the PSP/CASP. The decentralized and sometimes unpredictable nature of DLT may create difficulties for applying certain rules, including those on: unique identifier (including the VoP); execution time and value date; blocking of a payment transaction/payment instrument in case of suspicion of fraud; rectification of unauthorised or incorrectly executed payment transactions; etc. Regarding the D+1 maximum execution time, we should clarify whether any higher fee (to achieve D+1 execution) is to be borne by the PSP/CASP alone or, if provided for in the framework contract, may be passed on to the PSU. We should also clarify which is the liability regime for the "delay", particularly in cases of on-chain transactions where the maximum execution time cannot be achieved due to causes not attributable to CASPs but to the DLT. The rules on pre-contractual and contractual information should be amended accordingly to reflect these clarifications. IE (MS reply): No but we would like to emphasise our openness to the streamlining of authorisation procedures where dual authorisation is required.

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	HR (MS reply): We have no other proposals. FR (MS reply): The exclusion of open banking requirements regarding EMTs should also be envisaged in the PSR. We think it raises important questions of technical feasibility given the particularities of transfer of EMT, whether these transfers are done on-chain or off-chain.
Presidency Discussion Note: Discussion on the regime of distributors vs agents **(WK 4335/2025 INIT)**	
Q1. Do Member States agree with the proposed approach regarding the regime of distributors and agents, and the proposed drafting suggestions?	DK (MS reply): In general, we have often found it difficult to assert what is an agent, what is a distributor and what is "something else" (an "independent sales organisation" e.g.). At times, this leaves us without supervisory powers towards parties that play a central role in the provision of payment services – which is what left us preferring a broad definition of agents.

PUBLIC

Question	MS reply
	However, we find that coming up with a workable definition is Tricky. As we understand it, some business models which play an important part in financial inclusion relies on distributors to buy/sell e-money to PSU's. We are not convinced that the proposals of the PCY would allow these business models to continue. This should only occur if there is some inherent risk in it. We can live with the definition but would prefer an analysis of how this affects current business models. We do find this wording misleading, however, as it gives the impression that distributors can provide payment services (in which case they would be agents): To expand the reach of their services, payment institutions may need to use entities providing payment services on their behalf, including agents and distributors. Finally, we remain unconvinced by the definition of repurchase of e-money which is not redemption of e-money. This seems to some extent to be a definition aimed at allowing distributors to redeem e-money by calling it something else. DE (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We generally agree with the proposal of the PCY to retain the concept of a distributor in PSD 3. At this point, we would like to point out once again that the distributor activity described includes a subset of an agent activity (payment service), meaning that there may be overlaps and therefore also differentiation problems. However, in our understanding, the activities of an agent go beyond those of a distributor, as the agent's activity itself qualifies as a payment service, for the exercise of which he does not require his own authorisation only because he uses the authorisation of a licensed institution. Merging the two concepts might thus lead to unintentional interactions with other provisions of PSD3/PSR and MiCAR. What is more, the implications of distributing e-money tokens within the scope of MiCAR are not sufficiently clarified. In accordance with recital 92 MiCAR distributors should be exempt from the requirement to seek authorisation as a crypto-asset service provider for the activity of the placing of crypto-assets. The distribution of e-money tokens on the basis of Art. 2 (36) PSD 3 could potentially qualify as a ‘placing of crypto-assets’ or ‘exchange of crypto-assets for funds‘. However, we would also like to point out that due to comparable (considerable) levels of AML/CTF risks associated with the activities of

PUBLIC

Question	MS reply
	both agents and distributors, it is desirable to treat both agents and distributors equally and as obliged entities **regarding AML/CTF obligations** (e.g. measures to prevent AML/CTF, appointment of a central contact point (Art. 31(4) PSD3 for the case of agents and pursuant to Art. 20(3) i.c.w. Art. 31(4) for distributors)). We see merits in introducing the concept of repurchases. However, we need more time to analyse the text and its consequences to a full extent. CZ (MS reply): If registration is not going to be required, we do not understand, why the distributors are back in the text - there was widespread agreement that the distributors would no longer be in the text. This appears to lack added value. Could you please clarify what the distributor's responsibilities or obligations would be? CY (MS reply): We agree with the Presidency's suggestion to reintroduce the concept of distributors in PSD3/PSR and to avoid merging distributors into the concept of agents. However, the suggested wording of "or repurchases the electronic money from a holder, based on a contractual relationship

Question	MS reply
	with the payment institution issuing the electronic money, where this does not amount to a redemption of the electronic money" can create other complications. More specifically, the reference to the 'repurchase of e-money from a holder' can lead to misinterpretations i.e. who is the 'holder' of e-money? Does it apply to a merchant as well as a consumer? Which cases would not amount to 'redemption' of e-money? The 'redemption' of e-money should not only be linked to the request of the holder (legal or natural person) to transfer any remaining balances from the user's e-wallet to the user's bank account. The mere payment (e.g. utility bill) from a user's wallet can also lead to 'redemption' of e-money. BE (MS reply): BE: We strongly disagree with this approach, which, for reasons purely of ease, intends to reintroduce the concept of 'distribution' and render it even more convoluted a concept than it was before. Already today under EMD/PSD2 it is difficult to draw distinctions between the activities of a distributor and those of an agent, distribution as such not being a defined concept in EMD/PSD2. The PCY proposal to further distinguish between cases where redemption must occur through 'agents' but 'repurchasing' of e-money from its holder may be performed by a distributor makes it

PUBLIC

Question	MS reply
	inoperable in practice by the market and impossible to supervise by NCAs. It will be impossible to distinguish between cases where the e-money is redeemed/exchanged for funds and ceases to exist/is extinguished, as opposed to the case where the distributor purchases the e-money from an e-money holder, without the e-money being redeemed/extinguished. In reality, market participants will be able to craft their contracts in any manner that suits them to do the regulatory shopping they wish in relation to these requirements. AT (MS reply): **AT:** The proposal by the PCY could be a step in the right direction. However, we think that "redemption of e-money" might still be a useful activity that distributors should be able to perform without qualifying as a payment service. The term "distributor" should be clarified and only cover the head of a system of distributors. ES (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	We agree with the overall intention of the proposal of keeping the role of distributors separate from the role of agents in order to avoid unnecessary burden to NCAs and PIs in this regard. However, according to the wording of Article 20.1, it seems that agents could not distribute electronic money. *"Member States shall allow payment institutions that provide electronic money services to distribute ~~and redeem~~ electronic money through distributors."* It would be necessary to assess the reason for this limitation, when the reserved activity is the issuance and provision of payment services, not the distribution. We suggest considering the possibility that agents can also distribute, as is the case in PSD2, and that distributors can only distribute and redeem. The mention that distribution was not a service of an agent was to ensure that distributors were not considered agents, but if a separate regime for distributors is to be established, we do not see the reason for not allowing agents to distribute. SK (MS reply):

PUBLIC

PUBLIC

Question	MS reply
	We can show flexibility on the issue. SI (MS reply): Yes. SE (MS reply): We prefer the current proposal from the previous one. However, we think it would be appropriate if agents and distributors were to be subject to the same requirements. PT (MS reply): PT agrees. NL (MS reply): We would like to advocate for retaining the term 'distributor in PSR/PSD3, as a distributor could represent a different type of entities than an agent across jurisdictions, which is the case in the Netherlands. An agent acts on behalf of a payment institution or an electronic money institution (EMI) in offering payment services as defined in the current PSD2. In contrast, a distributor is currently considered a more passive entity that can distribute

PUBLIC

Question	MS reply
	or redeem electronic money on behalf of an EMI but is not permitted to issue electronic money on behalf of the underlying EMI (i.e., it is prohibited from performing the core activity of an EMI). In this regard, it is particularly important that (a) clarity is provided on which entities under PSR/PSD3 may or may not issue electronic money on behalf of the underlying license holder, and – even more importantly – (b) that PSR/PSD3 provides a clear definition of both agents and distributors. This definition is absent in the current PSD2, resulting in divergent supervisory practices and interpretations across various member states, which is undesirable. Particularly from a notification perspective, it is essential that member states operate uniformly with respect to agents and distributors. To ensure this and establish a level playing field, clear definitions and precise demarcations are necessary. LV (MS reply): It is not clear why return to the inclusion of distributors could support as long as clear separation of functions. LU (MS reply):

PUBLIC

Question	MS reply
	Q1-Q2: under further scrutiny. LT (MS reply): We would favor a single category of intermediaries, i.e. agents for both payment services and e-money services, and without distinguishing distributors for e-money. For agents which only sell or distribute e-money, exclusions regarding certain requirements could be foreseen, e.g. lighter AML requirements. The proposed setup makes the whole model very complex and hard to understand in which cases what type if intermediary can be used. However, if the concept of distributors is re-introduced, firstly, it is important to have a clear understanding of difference between e-money and other funds in the account. We have raised a number of times the need to clearly distinguish e-money and other funds, and have proposed a recital for that. It would be useful also for this case. (see below) Other remarks on the proposed text: The clarity regarding the possible models of distribution and redemption in case of online models is needed. Is e-money distribution possible online, when no payment services are provided by the distributor? Redemption should not be called as a payment service, but rather a functionality or requirement for the provision of e-money services. (in rec 45a) Regarding the purchase of e-money by a distributor: from the perspective of a PSU – he exchanges his e-money for scriptural money or cash, so it seems that his e-money are redeemed; but the recital states that it is not redemption. Moreover, it would be the expectation of PSUs to be able performing both transactions – buy and sell – of e-money at the same place, and at par value. Having one category of intermediaries (agents) would help to address these issues.

Question	MS reply
	Proposed recital in the PSD3 on e-money. *(5a) In light of the European Court of Justice (ECJ) ruling, the classification of products qualifying as electronic money within the EU payments market has become more restricted. Currently, only a limited range of instruments, such as prepaid cards not linked to payment accounts, closed-loop payment systems, and electronic money tokens under the Markets in Crypto-Assets Regulation (MiCA), fall within this definition.* *Furthermore, it is recognized that payment institutions that do not engage in the issuance of electronic money are nevertheless permitted to open payment accounts for their customers, in which funds may be held for an indefinite duration. Given this distinction, a specific category of accounts—electronic money accounts—can be identified. An electronic money account constitutes a specialized form of payment account designed exclusively for the storage of electronic money, lacking the full functionality typically associated with standard payment accounts.* *The regulatory framework governing initial capital requirement and the calculation of own funds differs between electronic money issuers and other payment service providers. Consequently, distinguishing electronic money accounts serves to ensure the appropriate application of initial capital requirements and methodologies for own funds calculation in accordance with the applicable regulatory provisions.* IT (MS reply): IT: Having in mind the previous discussions on the regime of distributors and agents, and in consideration of the current negotiation stage, we are not in a position to support the proposal put forward by the Presidency on the distribution regime. In particular, we notice that such a proposal limits the activities performed by distributors to: i) the distribution of e-money and ii) its re-purchase, with the latter being something distinct from the redemption of e-money, which

Question	MS reply
	would be an activity reserved to agents instead; however, we are not sure we understood in what the repurchase substantiates and therefore its difference from redemption (i.e. why the distributor would repurchase e-money from clients for goals other than redeeming it?). More generally, we believe that such approach would be contrary to the simplification goals pursued by the entire recast of PSD2 and EMD2 into a single body of law, especially in light of the intrinsic similarities between the electronic money services (distribution/ redemption/issuance) compared to payment services; under an application-oriented point of view, we wonder also whether this approach would lead to some forms of operative fragmentation in the payment services processes. Therefore, in our view, distributors of e-money should be treated as agents: indeed, we notice that distribution and redemption of e-money involve the same risks (ML/TF included) as other payment services such as cash placement/withdrawal and therefore the rules on distribution/agency network should be the same with regard to such activities. IE (MS reply): We are supportive of the reintroduction of the separate definitions of agents and distributors. We understand that this means that the EC's drafting in

PUBLIC

Question	MS reply
	respect of distributors across Articles will be reintroduced, including the register requirement under Article 17. HR (MS reply): We strongly support the proposal to reintroduce the concept of distributor. In our opinion, distributors should continue to be treated as they are treated today because we do not see a need to change the model that has been working well for years. Therefore, it is important to recognize that distribution and redemption of electronic money are key activities of distributors. In that connection, we would not support the proposal that redemption is an activity reserved to agents. We would not oppose the possible clarifications in the text of PSD3 that PIs using distributors remain ultimately liable for any acts of distributors acting on their behalf. FR (MS reply): France is strongly against the reintroduction of the notion of distributor and is in favour of merging the status of agents and distributors of e-money. It should be added that in terms of liability, a payment institution using distributors or agents remains ultimately liable. Maintaining such dual status will inevitably lead to regulatory and level-playing field issues as we are

PUBLIC

PUBLIC

Question	MS reply
	merging at the same time the status of payment institutions and e-money institutions. EL (MS reply): **EL:** We do not have knowledge of any such business cases in Greece where a distributor purchases e-money from an e-money holder—without the e-money being redeemed or extinguished—based on a contractual arrangement with the PI or EMI issuer. It appears that this provision, especially when combined with the use of an e-wallet, could potentially conflict with the "cash-in-shop" regime, which is an exempted payment service. Moreover, the purchase of e-money in this context could raise concerns related to anti-money laundering (AML) risks. In general, we are of the view that entities operating as distributors should be treated as agents, which is also consistent with the current legal framework in Greece.
Q2. Member States are kindly invited to put forward their further proposals for the definition of an agent, which still remains an open key issue for Member States.	DK (MS reply): Please see Q1. We do not have a better definition. DE (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	We would oppose any change to the definition of agent as compared to PSD 2 / the COM proposal for PSD 3. From our point of view there is no need to change this well-established definition. In particular, the activity of an agent should continue to qualify as a payment service itself. The agent is not merely participating in the provision of payment services. On the basis of this understanding, it can be clearly determined which activities, namely the provision of a payment service, qualify the partner of a PSP as an agent. Differentiation problems can thus be avoided and the question of de minimis contributions would not even arise. This is also relevant in terms of AML/CTF obligation of the agent (and possibly distributors; see answer to Q1), since AML/CTF obligations pursuant to Regulation (EU) 2024/1624 are linked to the provision of e.g. payment services. CZ (MS reply): We can support the deletion of the distributor or even with the PSD2 approach. We also support BE's proposal to simplify the registration of agents. PI would be responsible for registering its agents. CY

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	(MS reply): Based on the response provided for question 1, we could consider keeping the two concepts (agents and distributors) as in the current legal framework with minor changes on the definition of the distributor. The revised definitions would largely depend on the approach (i.e. refer to Q1). BE (MS reply): BE: BE strongly urges the PCY to maintain the removal of the antiquated notion of 'distributor' from the text of PSD3/PSR. We continue to be highly supportive of the previous compromise text the PCY introduced. AT (MS reply): - ES (MS reply): No further comments. SI (MS reply): /

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	SE (MS reply): We prefer to keep the current definition as is. It is difficult to foresee the consequences of making amendments to the definition at this late stage of the negotiations. As we have said before, the definition is closely linked to the definition of a payment service. The agent definition itself mainly targets whether it is the PSP itself that provides the service or if it is provided via an agent. Any amendments to the agent definition therefore risks blurring the definition of a payment service, and thus the scope of the entire regulation. This needs to be carefully considered. PT (MS reply): PT would not oppose adopting Article 2(28) as originally proposed by the COM. NL (MS reply): - LV (MS reply): We support. LT

PUBLIC

Question	MS reply
	(MS reply): The latest definition of an agent does not give enough clarity regarding its roles and activities. Therefore, we invite to revert to the definition proposed in 15/11/2024 meeting. This definition includes some criteria, which define the essence of an agent, namely. Also, it is important to have the reference to the "name of PI", as it has to clear for PSU, which entity is ultimately responsible for the services. (28) 'agent' means a natural or legal person who under the full and unconditional responsibility of a payment service provider on whose behalf and in the name of it acts, participates to the provision of payment services, including the execution of payment orders or the collection and transfer of payment orders and of the associated payment service users' consent to a payment service provider, or distributes or redeems electronic money. IT (MS reply): IT. As said before under Q1, since distribution and redemption of e-money involve the same risks (ML/TF included) as other payment services such as cash placement/withdrawal, we deem that the definition of agent should be wide enough in order to include the following activities (please note that the list hereafter assumes that the definitions of payment services and e-money services are kept distinct): placement/conclusion of framework contracts regarding payment services and e-money services; presentation and offer of payment services; distribution, top-up, and redemption/withdrawal of e-money; provision of services in support to the allocation of payment services

PUBLIC

Question	MS reply
	and e-money services (white-label models and Banking-as-a-Service models). Here a possible drafting suggestion: "*Agent means a natural or legal person who acts in the name and on behalf of a payment service provider in providing payment services and electronic money services and who: presents and offers payment services and electronic money services, concludes framework contracts regarding payment and electronic money services, distributes or redeems electronic money, provides services in support to the provision of payment services and e-money services*." Starting from this proposal, we would like also to take this opportunity to recall our main view on the other intertwined issue (especially under the AML point of view) of the large network: at this regard, as also stated during some previous WPs, we believe that all the relevant stakeholders (i.e. the PSPs, the AML Supervisory Authorities and FIUs) should have full knowledge of the PSPs extensive network through a unique repository kept at national level by NCAs, where to gather relevant information on all agents which are part of the network; such framework would ensure also a prompt knowledge of agents serving multiple mandates on behalf of more PSPs. As a consequence, we would not support any simplification of the registration

Question	MS reply
	process for large network of agents aimed at limiting obligations to the agents acting as heads of network and requiring PSPs to maintain a public register of agents. We also reiterate our strong perplexities regarding the SE proposal of the registration agents (pursuant to which such activity would be performed by the host authority) in light of possible, unintended consequences on the effectiveness of the prudential supervision of home authorities on the PSPs using agents in host MS. HR (MS reply): We strongly support not changing the definition of an agent. We have concerns that changing this definition could have unintended consequences on the business models that exist in the market and could bring confusion on the market. FR (MS reply): We consider that two main separate criteria can be used to determine whether a PSP's partner qualifies as an 'agent': - (i) whether it enters into possession of the funds on behalf of the PSP's customers (collection of funds on behalf of third parties) or

PUBLIC

PUBLIC

Question	MS reply
	- (ii) whether it is directly involved in the PSP's provision of payment services. The second item of this proposal would encompass several business models such as (i) tobacconists collecting funds and opening payment accounts on behalf of a payment institution (that would still be required to be registered) or (ii) marketplaces collecting the prices of transactions on an account opened in its name in the books of a PSP. It would be more precise than the current definition that is too wide and interpreted with too much divergences by Member States.
Any other business and Presidency closing remarks	
Q1. Could Member States accept adding a reference to Articles 3(5) and 36(4a) PSD3 stating that the entity's own funds or initial capital shall not be excluded from what a comparable guarantee is, or would MS prefer to leave the clarification of what constitutes a comparable guarantee to national discretion?	DE (MS reply): We do not agree with the proposal. Initial capital or an entity's own funds are funds which an entity has to hold in order to cover its own funds requirements or in other words the risks that arise from its business activities (which exclude any civil law claims by clients) at any given time. If a portion of this capital is used as a comparable guarantee, it can no longer be considered readily available to cover such risks since these funds do always need to be kept "on the side" for possible civil law claims by clients CZ

Question	MS reply
	(MS reply): We support the removal of the EBA mandate and leaving the clarification of what constitutes a comparable guarantee to national discretion. At the same time we appreciate the addition of a reference to Articles 3(5) and 36(4a) PSD3 stating that the entity's own funds or capital shall not be excluded from what is a comparable guarantee. In case the EBA mandate is removed the statement could be moved to sentence describing MSs discretion (MSs may provide that *the entity's own funds or capital constitute a comparable guarantee*). CY (MS reply): We prefer to leave the clarification of what constitutes a comparable guarantee to national discretion. AT (MS reply): **AT**: We could be open to both solutions. ES (MS reply):

PUBLIC

Question	MS reply
	As mentioned in previous comments, we do not agree to considering initial capital as comparable guarantee for the purposes of PII, given it provides much lesser consumer protection. SK (MS reply): We are open to the addition. SI (MS reply): We could accept first option together with RTS. SE (MS reply): We would prefer to leave the clarification of what constitutes a comparable guarantee to national discretion. PT (MS reply): **This is one very important topic for PT.** We strongly support the adoption of one of these options to facilitate the emergence of alternatives to the possession of a Professional Indemnity Insurance (PII) for the purposes of authorisation for payment institutions (Article 3(4) PSD3) and registration for Account Information Service

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

Question	MS reply
	Providers - AISPs (Article 36(4) PSD3). Over reliance on the PII requirement is, in our view, undesirable and unbalanced, given that certain MS face a considerable lack of offering of products that would allow interested entities seeking to provide these services to obtain the demanded PII. Experience from the implementation of PSD2 also highlights that the EBA mandate drafted at the time failed to provide clear characteristics of what constitutes a comparable guarantee, an omissive precision that has prevented pursuance of this concept by interested parties and NCA. Therefore, it is our understanding that appropriate alternatives to the PII need to be detailed in L1 text. Despite the EBA RTS currently depicted in Articles 3(5)(d) and 36(4a)(d), foreseeing a conceivable usage of own funds or initial capital under certain conditions to deduct the minimum monetary amount of the PII, there is the chance this mandate might end up imposing severe restrictions in this regard, outcome which we have to avoid. From the 2 presented options, PT would prefer maintaining full harmonisation across MS, leaving in place the EBA RTS but adding a reference to Articles 3(5) and 36(4a) PSD3 stating that the entity's own funds or initial capital shall not be excluded from what a comparable guarantee is. It is worth noting this option is aligned with the FIDA

PUBLIC

PUBLIC

Question	MS reply
	compromise text, as the same exact reference is previewed in its Article 12(4), on the authorisation of FISPs. With this setting in mind, please consider the following adjustments: *"Article 3 PSD3* *5. The EBA shall develop draft regulatory technical standards specifying:* *(...)* *(c) what is a comparable guarantee, as referred to in paragraph 4, which should be interchangeable with a professional indemnity insurance;* *(d) the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee as referred in paragraph 4* ~~***and the conditions under which initial capital or own funds may be taken into account for the purpose of reducing the minimum monetary amount of the professional indemnity insurance or other comparable guarantee***~~*.* ***For the purposes of point (c), a payment institution's own funds or initial capital beyond the level required pursuant to this Directive shall not be excluded from what a comparable guarantee is.*** ~~***For the purposes of point d), where an undertaking that applies for authorisation to provide payment services as referred to in Annex I, point (6) holds additional initial capital beyond the level required pursuant to this Directive or own funds, the respective funds may be deducted from***~~

PUBLIC

Question	MS reply
	~~***the minimum monetary amount of the professional indemnity insurance or comparable guarantee as referred in paragraph 4, subject to the conditions to be set in the regulatory technical standards referred to above.***~~*"* *"Article 36 PSD3* *4a. The EBA shall develop draft regulatory technical standards specifying:* *(…)* *(c) what is a comparable guarantee, as referred to in paragraph 4, which should be interchangeable with a professional indemnity insurance;* *(d) the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee as referred to in paragraph 4* ~~***and the conditions under which initial capital or own funds may be taken into account for the purpose of reducing the minimum monetary amount of the professional indemnity insurance or other comparable guarantee***~~*.* ***For the purposes of point (c), an account information service provider's own funds or initial capital shall not be excluded from what a comparable guarantee is.*** ~~***For the purposes of point d), an undertaking that applies for registration as an account information service provider holds initial capital or own funds, the respective funds may be deducted from the minimum monetary***~~

PUBLIC

Question	MS reply
	~~*amount of the professional indemnity insurance or comparable guarantee as referred to in paragraph 4, subject to the conditions to be set in the regulatory technical standards referred to above.*~~*"* Nevertheless, we would alternatively urge leaving to national discretion what constitutes a comparable guarantee, removing that part from the EBA RTS, and allowing each MS to accommodate that definition to their respective market reality. If this is indeed the chosen path, please consider the following suggestions: *"Article 3 PSD3* *5. The EBA shall develop draft regulatory technical standards specifying:* *(...)* ~~*(c) what is a comparable guarantee, as referred to in paragraph 4, which should be interchangeable with a professional indemnity insurance;*~~ *(c~~d~~) the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance* ~~*or other comparable guarantee as referred in paragraph 4 and the conditions under which initial capital or own funds may be taken into account for the purpose of reducing the minimum monetary amount of the professional indemnity insurance or other comparable guarantee*~~. ~~*For the purposes of point d), where an undertaking that applies for authorisation to provide payment services as referred to in Annex I, point*~~

PUBLIC

Question	MS reply
	~~*(6) holds additional initial capital beyond the level required pursuant to this Directive or own funds, the respective funds may be deducted from the minimum monetary amount of the professional indemnity insurance or comparable guarantee as referred in paragraph 4, subject to the conditions to be set in the regulatory technical standards referred to above.*~~ ***6. For the purposes of paragraph 4, Member States may determine what constitutes a comparable guarantee and its minimum monetary amount. A payment institution's own funds or initial capital beyond the level required pursuant to this Directive may be considered for this purpose."*** *"Article 36 PSD3* *4a. The EBA shall develop draft regulatory technical standards specifying:* *(…)* ~~*(c) what is a comparable guarantee, as referred to in paragraph 4, which should be interchangeable with a professional indemnity insurance;*~~ *(c~~d~~) the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance* ~~*or other comparable guarantee as referred to in paragraph 4 and the conditions under which initial capital or own funds may be taken into account for the purpose of reducing the minimum monetary amount of the professional indemnity insurance or other comparable guarantee*~~.

PUBLIC

Question	MS reply
	~~*For the purposes of point d), an undertaking that applies for registration as an account information service provider holds initial capital or own funds, the respective funds may be deducted from the minimum monetary amount of the professional indemnity insurance or comparable guarantee as referred to in paragraph 4, subject to the conditions to be set in the regulatory technical standards referred to above.*~~ ***4b. For the purposes of paragraph 4, Member States may determine what constitutes a comparable guarantee and its minimum monetary amount. An account information service provider's own funds or initial capital may be considered for this purpose."*** LV (MS reply): We support adding references. LU (MS reply): We have a preference for an addition in the legal text instead of the introduction of a national option. IT (MS reply):

Question	MS reply
	IT. We would not support the proposal of leaving to national discretion what constitutes a comparable guarantee since, in our view, it may pose risks of regulatory arbitrage. If the PCY HU proposal of recognize initial capital or own funds as comparable guarantee directly in the text of PSD3 should not be supported by MSs, we deem that the second best option is to define what constitutes comparable guarantee in L2, giving a mandate to EBA to draft RTS addressing this issue. IE (MS reply): Our preference would be to add appropriate references. HR (MS reply): We accept adding a reference to Articles 3(5) and 36(4a) PSD3 stating that the entity's own funds or initial capital shall not be excluded from what a comparable guarantee is. In our previous comments we pointed out that, in order to find an appropriate solution to the problem of PII availability, we would support any viable alternative to PII for the first year of operation of PISP/AISP. and we also supported the proposal for the RTS specifying the conditions under which additional initial capital or own funds may be deducted from the minimum

PUBLIC

PUBLIC

Question	MS reply
	monetary amount of the PII or another comparable guarantee. Considering that a solution in that sense is provided in the latest proposal by the Presidency in Discussion Note on interplay with the FIDA Regulation (WK 3395/25), in our comments we remained consistent with our previously expressed positions and supported the proposal, but we also added a proposal to amend that solution in order to allow that capital may completely replace the PII. In case that this proposed solution is not accepted, we would be open to other solutions in a common approach because the point is that an appropriate alternative to PII must be provided. FR (MS reply): We don't oppose to introduce a reference to Articles 3(5) and 36(4a) PSD3 stating that the entity's own funds or initial capital shall not be excluded from what a comparable guarantee is.
Q2. Would Member States agree with increasing the transposition deadline of PSD3 (Article 49) and the implementation of a due date of PSR (Article 112) from 18 to 24 months?	DE (MS reply): We support lengthening both periods. CZ (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We strongly support increasing the transposition deadline to 24 months. However, we strongly disagree with the obligation to implement Article 46 PSD3 (the Amendments to Directive 98/26/EC) within 6 months as required by Article 49. This requirement is legally impossible in view of the national legislative process. The Amendments to Directive 98/26/EC (Article 46 PSD3) should by implemented at the same time as PSR and PSD3. Until PSD3 is implemented the institution under SFD will cover PI and **EMI!** The proposed change of the definition in 6 months will cause significant harm. We therefore urge that the transposition deadline for Article 46 should also be 24 months. CY (MS reply): We agree with increasing the transposition deadline of PSD3 (Article 49) and the implementation of a due date of PSR (Article 112) from 18 to 24 months. BE (MS reply): BE: We see no need in extending the deadline. AT (MS reply):

PUBLIC

Question	MS reply
	-
	ES (MS reply): We have no objections to the referred proposed extension
	SK (MS reply): We support longer transposition deadline.
	SI (MS reply): Yes, we strongly agree.
	SE (MS reply): Yes.
	PT (MS reply): PT strongly supports the increase of the transposition deadline of PSD3 to, at least, 24 months, given the significant dimension of this Directive and its complexity. Moreover, the PT specific regime for transpositions foresees in almost all cases a needed approval of the transposed legislation by the PT Parliament, which results in a very lengthy process. We believe, that at

PUBLIC

Question	MS reply
	least, 24 months could be a more reasonable timeframe to ensure correct and effective transposition drafting, as well as the full carrying of the national process to adopt it. Additionally, given the synergies between the PSR and PSD3, namely regarding cross references to each other in the text, and bearing in mind that both will demand adjustments to national legislation, PT believes a concurrent alignment of the implementation period of PSR to 24 months is needed to avoid additional undue burdens. NL (MS reply): Yes. A transposition deadline of 18 months is too short for a proposal of this size also keeping in mind the many procedural steps member states need to take. LV (MS reply): We support the proposal. LU (MS reply): OK. IT (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	IT. Yes IE (MS reply): Agree. HR (MS reply): We agree with increasing the transposition/implementation deadline to 24 months. FR (MS reply): We agree with increasing the transposition deadline and the implementation of a due date of PSR from 18 to 24 months. FI (MS reply): FI: Yes, we would strongly favour extending the deadlines and would be ready to consider even longer postponement (i.e. 24 + 6 months). Furthermore, the deadlines for level 2 regulation should be taken into account when determining the transposition deadlines and the date of start of application. EL (MS reply):

PUBLIC

Question	MS reply
	EL: no strong view.
France's Non Paper: Treatment of Digital Wallets (WK 4384/2025 INIT)	
Q1. Do Member States agree with the approach proposed in the FR non-paper?	DK (MS reply): We do see some interesting aspects in the non-paper from France and we can agree on many of the points regarding digital wallets if they do not offer payment services. However, we think that going down this road is to open pandora's box and we would prefer not to bring into the regulation providers who do not offer payment services. DE (MS reply): We agree, that re-evaluating the role of digital wallets has merit, given their growing significance in the market for digital payments. However, we do not support adding a separate notification regime for digital wallet providers, as proposed in the non-paper by FRA. Further regulation of wallet providers, who do not themselves provide payment services but at best contribute to them (which may make them the contact person for the supervision of the relevant payment service provider), appears alien to the PSD3/PSR system – **at least as long as the provision of wallets is not itself defined as a payment service**. If the

PUBLIC

Question	MS reply
	proposed notification system (Article 38a PSD3) initially only aims to obtain an **overview of the market and services** and thus to obtain a basis for decisions on possible further regulations, **this should be possible outside of a provision in the PSD3/PSR –** possibly via an EBA-query or in DORA as part of the monitoring of ICT services. We further would like to point out that even under PSD2 NCAs can address a TSP indirectly by taking measures addressed to a PSP that uses this TSP. In addition, the current PSR draft already foresees supervisory powers over TSPs in Art. 91(3)(ii). At the moment, the proposed notification regime in PSD3 goes far beyond the objective of initially obtaining an overview of the market. Rather, it leads to considerable administrative effort, which regularly requires a comprehensive review of the respective product and business model. As the proposal for Article 38a(1)(2) PSD3 reads "On the basis of this notification, the competent authority shall take a duly motivated decision on the basis of assessment criteria" it is not clear, what the possible outcomes of this decision should be (maybe to accept or reject the notification?); in addition, there is no hint to the actual "assessment criteria" whereupon the decision should be based, but just a proposed mandate for the EBA to include such criteria in a draft RTS. Should this proposal be adopted, the draft RTS should also mandate the EBA to

PUBLIC

Question	MS reply
	specify the assessment methodology in order to facilitate a common understanding amongst Member States. In our understanding, the proposed notification system essentially corresponds to that in Art. 39 PSD 3, the deletion of which we are in favour of or the adoption of which should be left to the discretion of the MS and their NCAs (see Annex below). **In this sense, we also reject the introduction of another notification procedure.** As far as the question of whether a payment service is provided is concerned, wallet providers may be required to first check their product on their own responsibility, if necessary with the help of legal advisors, to determine whether they are providing a payment service and thus have to apply for any necessary authorisation. As emphasised in the paper, EU-wallet-providers are currently subject to supervision by the ECB under PISA. We assume that the ECB is required to inform the NCAs if it has indications in individual cases that these providers are providing payment services so that the NCAs can take appropriate measures. If non-EU-actors operate domestically without the necessary authorisation, NCAs already have the option to take action. If non-EU operators provide payment services without PSD3/PSR-authorisation, it is generally almost

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	impossible to enforce supervisory measures. The same applies if a notification obligation is not complied with. Finally, we would be **open to fundamentally re-evaluating the role of digital wallets**. However, given that it is too late to address this within the current legislative process, **we propose shorting the review period stipulated in Article 43 PSD3**. Annex: We thank the PCY for their efforts to discuss our Non-Paper in the working party. We thank other MS for their feedback provided to the Non-Paper. We agree with the proposed deletion of Article 81(1)(3) PSR and Article 83a(4) PSR. Further, we agree with the deletion of Article 32(7) PSR and the proposed wording of Article 32(6) PSR. Based on the feedback provided by MS to our non-paper, **we do not agree with the proposal of the PCY to keep Articles 48(6) and (7) PSR in the text**. In fact, 22 MS responded to the questionnaire following up the Working Party on the 21st of February, containing questions on our non-paper on simplification. Of those 22 MS, 19 MS responded to our

PUBLIC

Question	MS reply
	proposal to delete Article 48 (6) and (7) PSR. Of those 19 MS, 12 MS support the deletion of Article 48(6) and (7) PSR and 2 MS do not object the deletion of Article 48(6) and (7) PSR. Only 3 MS are against a deletion, 1 MS provided a suggestion to streamline the reporting obligation and 1 MS applied a scrutiny reservation. **According to those numbers, there is a clear majority of MS in favour of deleting the reporting obligation of Articles 48(6) and (7). Hence, we do not see any ground for keeping the reporting obligation in text and continue to ask for its deletion.** **Fallback option:** Should the deletion of article 48 (6) and (7) PSR not be possible, we would like to make the following proposal: 1. In our view, then the primary objective of article 48 (6) PSR should be brought to the fore. This objective, as we understand it, is to provide the Commission with an assessment of „[…] size and operation of the markets for account information services and payment initiation services in the Union […]“ (please see the penultimate sentence in article 48 (6) PSR). In our view, the reporting obligation for this objective should lie with the AISPs and PISPs, who could report on their actual use of the interfaces just as well or even better, and not

PUBLIC

Question	MS reply
	with the ASPSPs. This would not only better serve the overarching objective, but would also reduce the effort required for notification processing, as there are simply significantly fewer AISPs and PISPs than ASPSPs. Therefore, we would like to propose the following amendment: „6. ~~Account servicing payment service providers~~ **Account information service providers and payment initiation service providers** shall provide competent authorities with data on access ~~by account information service providers and payment initiation service providers~~ to payment accounts ~~which they service~~. ~~Competent authorities may also, where appropriate, require account information service providers and payment initiation service providers to provide any relevant data on their operations.~~ […]“ The notified EBA RTS in article 48 (7) PSR can regulate the details of this notification. 2. If the above proposal is not accepted, the proposal of ITA in its written comments to the working party on the 21st of February should be considered, as this would require ASPSPs to provide information

PUBLIC

Question	MS reply
	that they already publish quarterly in their availability and performance statistics. However, it should be noted that ITA's proposal not only targets the statistics under Article 35 (5) PSR (please see points (i) and (iii) of the Italian proposal), but also the response times under Article 36 (1) (c) PSR. These response times are not currently included as a requirement in the statistics to be published, subject to the yet to be developed EBA RTS pursuant to Article 38 (5) (a) PSR, and would therefore still need to be converted into a reportable format by the ASPSPs. This would result in increased efforts for the industry. In our view, it would be sufficient to shorten ITA's proposal in Article 48 (6) PSR as follows: „Such data set should include the quarterly statistics on the availability, unplanned unavailability and performance of the dedicated interface pursuant to Article 35 (5) respectively the EBA regulatory technical standard according to Article 38 (5) (a)." In principle, this addition would ensure that, when compiling the EBA RTS pursuant to Article 38 (5) (a) PSR, account is taken of the fact that the quarterly statistics should form the basis for the data provision pursuant to Article 48 (6) PSR. In this case, a separate EBA RTS for

PUBLIC

Question	MS reply
	reporting as provided for in Article 48 (7) PSR would no longer be necessary. In our opinion, individual additions to the data by the competent authority (as also proposed by ITA in Article 48 (6) PSR) do not appear to be expedient due to the reason that individual information would conflict with harmonised data collection and analysis.] **Regarding Article 39 PSD 3,** we do see a split in the feedback provided by MS. In fact, 20 MS responded to the proposal to delete Article 39 PSD 3. Of those 20 MS, 11 MS argued against a deletion of Article 39 PSD3, while 7 MS favour a deletion and 1 MS does not object a deletion – 1 MS applied scrutiny reservation. Those MS who do not support the deletion of Art. 39 PSD 3 predominantly argue with the reliance of their NCAs on information about domestic market activities collected by this notification duty. In other MS, like Germany, however, NCAs do not need the notification obligation to generate evidence, but collect evidence e.g. by conducting market studies and targeted investigations on service providers. In this regard, it becomes clear that the notification duty of Art. 39 PSD 3 is merely a particular supervisory instrument in order to collect

Question	MS reply
	information from the market than a certain standard applied to market participants. Accordingly, there is no need for a harmonized, EU-wide application of the notification duty of Art. 39 PSD 3 from a level playing field point of view. Rather, the **choice whether to utilize on such supervisory tool should be left to the discretion of MS and their NCAs**, with a view to their markets and their other information generating instruments at hand. Leaving the choice to MS and their NCAs would be in line with the general approach of PSR / PSD 3 to merely prescribe that NCAs have all supervisory and investigatory powers necessary for the exercise of their functions, while the choice about the use of individual supervisory instruments is left to the discretion of MS and their NCAs. **To be concrete, we propose to change the text of Art. 39 PSD 3 in order to leave the decision to require service providers in the scope of Art. 39 PSD 3 to notify to competent authorities to the discretion of MS. We have provided concrete drafting in our written comments on the consolidated tables.** CZ (MS reply):

PUBLIC

PUBLIC

Question	MS reply
	We are sceptical here. We do not see a need to amend the text on this point. CY (MS reply): We have no comments. BG (MS reply): We do not agree with the approach proposed in the FR non-paper as it would create a quasi-authorisation regime, that could lead to market fragmentation. Our understanding is that under the proposed framework wallet providers would be required to get authorisation in every member state where they would like to provide services as there is no envisaged procedure for recognition of authorisation in another member state. We believe that this would be disproportionate administrative burden, as the regime for authorisation of payment service providers, that actually **hold** client funds, allows for the exercise of the right of establishment or the freedom to provide services. Moreover, payment service providers are already responsible for the actions of digital wallet providers as they are considered technical service providers. Consequently, we believe that the initial proposal of the European Commission, in which such entities are categorised as technical service

PUBLIC

Question	MS reply
	providers, over which national competent authorities have specific supervisory powers, is balanced. BE (MS reply): BE: In general we support the proposal, with 2 caveats and 1 important broader reflection: - The notification duty to each NCA does risk being very intensive e.g. Apple or Google Pay will have 27 different notifications, which creates a lot of red tape in times were we aim to have less red tape. - Why if there is notification, there also has to be a "decision" by the NCA. This could be seen as a disguised "authorisation" More fundamentally, although we agree with the aim of the FR non-paper, we also believe the remarks made by the Commission during the working party on the geopolitical sensitivities of such proposal are valid and we might want to take more time to prepare the ground. In this regard, taking this up during the review seems a more sensible way going forward. AT (MS reply): **AT**: We want to highlight the fact that according to the PCY's non paper on EMTs, the service of custody under MiCA shall not in itself constitute a

Question	MS reply
	payment service. Custody shall only be a payment service if it is provided together with transfer services under MiCA for EMTs. We should aim for consistency regarding EMTs under MiCA and other funds under PSD/R. ES (MS reply): We do not have objections to the inclusion of a duty of notification from digital wallet providers in order to help NCAs monitoring compliance. Moreover, we also agree with requiring these providers to report annually on services offered and statistical data on payments and fraud. SK (MS reply): We are flexible FR non-paper. SI (MS reply): / SE (MS reply): First of all, we would like to thank the French delegation for raising this issue. We agree that the integrity and security of digital wallets is essential.

PUBLIC

Question	MS reply
	We sympathise with the notion of collecting more information on digital wallets, to be able to properly assess these services. If this can be achieved in some appropriate format, the focus should perhaps be on cyber and IT security more generally and not just on fraud. We are however hesitant towards giving competent authorities supervisory duties towards these wallets, especially as they may be difficult to enforce. If we are worried about the security of the digital wallets, an alternative could be to explore whether the liability provisions in article 87 could be extended to cover IT and cyber security issues more generally. PT (MS reply): PT welcomes the FR effort on raising awareness on the topic of digital wallets. However, its release at a late stage in the negotiations prevents us from indulging in a deserving detailed discussion and carrying an impact assessment sustained with more evidence, both of relevant importance given the magnitude of the changes proposed. After our preliminary analysis, we underscore certain aspects that are not entirely clear for us: i) Whether the oversight framework for electronic payment instruments, schemes and arrangements (PISA), that encompasses the control of players

PUBLIC

Question	MS reply
	thar provide digital wallet services has, since its publication in 2021, proven not to be adequate or is failing to consider the risks relating with this activity. ii) If the levels of fraud cases related with payment cards tokenisation are significant at present, and if this is indeed a problem widely recognised across the Union. iii) If additional monitoring of the offering of digital wallet services, and of the resilience of the entities that perform these activities, justify the added burdensome for NCA, EBA and the entities themselves. In the spirit of approaching new regulatory requisites with an evidence-based mindset, PT believes further data and clarification on these topics are needed in to sustain the value added of the suggested provisions. Based on current information, and again considering the timeline related with the conduction of these negotiations in the Council, we would refrain at this stage from going beyond the notification requirement suggested in Article 38a(1), not agreeing with the periodic reporting of statistical data and the granting of another EBA mandate. Ideally, we would suggest leaving this subject to be entirely addressed within the package's review clause. NL (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We appreciate the awareness being raised regarding the increasing use of digital wallets for payments and their position within the regulatory framework. However, we believe that more time is needed to thoroughly assess all the implications of the current proposal. Therefore, we suggest exploring the feasibility of advancing the review clause for digital wallets to an earlier date, rather than waiting five years after the entry into force of PSD3. LV (MS reply): In our view, it is bureaucratically redundant to require PSD3 to inform that an ICS exists and to report statistics accordingly. If fraud risks are indeed seen with DW, then the articles on fraud should also include DW that they also bear a certain amount of responsibility if SCA is not in order, in addition then there should also be a link to DORA issues or similar. But information and statistics for statistics sake seems redundant. LU (MS reply): We do not agree with this approach. There is no evidence for justifying the introduction of such a “light regime of authorization” for digital wallet providers. The mere fact of an increasing market share of such digital

PUBLIC

Question	MS reply
	wallet providers as mentioned by FR during the meeting cannot be considered as a substantiated argument. Given the role of digital wallets in the payment eco-system, we consider that the current regime of technical service providers under PSD/PSR, together with DORA, are fit-for-purpose as to managing any potential risks stemming from their activities. Hence we believe that the review clause, which includes a mandate for COM to assess the issue in a comprehensive manner, is the right approach at the current juncture. LT (MS reply): We would be cautious regarding distinguishing wallets separately. It would make difficult to define the scope and set the proper requirements. IT (MS reply): IT. We do share the concerns expressed by our French colleagues and believe that the introduction of specific supervisory measures for digital wallet providers is appropriate. In particular, the provisions proposed in the FR non-paper go in the direction of including in the next future these providers in the regulatory perimeter, while clarifying certain obligations towards the ECB and, consequently, the NCAs. However, the complexity of the subject matter, also considering that the main providers are often part of global groups, seems to require further analysis that may not be compatible with the

Question	MS reply
	already advanced state of the negotiations. Therefore, we wonder whether there is time to address this issue in adequate manner or, conversely, whether it would not be preferable to postpone it until the next review of the regulatory framework. IE (MS reply): This approach seems reasonable in the context of the growing usage of digital wallets, albeit some of the finer detail might need further development and clarification e.g., which CA(s) does the notification go to and what decision is the CA making? HR (MS reply): We are open to this proposal, but it requires more substantial discussions. Preliminarily, we may agree with the introduction of the notification obligation for providers of digital wallet, but we oppose the proposal to introduce an obligation of the competent authority to take a duly motivated decision as well as the proposed EBA mandate. FR (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	We consider very important to pay some attention to the treatment of digital wallets because they are more and more broadly used by PSU, either at point of sale or for e-commerce. The current regulatory status with PSR that (i) creates an outsourcing requirement (Article 87 PSR) and (ii) liability for failure to provide SCA elements to the PSP (Article 58 PSR) is insufficient. If the Council disagreed with our proposal, it is key to ensure that very quickly the Commission would quickly bring to the table proposal for digital wallets providers, given the pace of adoption of these digital wallets. It would go through a shortened review clause in Article 43 PSD3. FI (MS reply): FI: We are ready to consider this proposal. However, there would be a need to clarify what exactly is the requirement, is it notification only, or some form of a registration or licencing procedure, the proposed formulation is a mixture of these. If the latter, the criteria for granting or refusing registration/license should be elaborated. EL (MS reply): EL: In our view, pass-through digital wallets (such as Google Pay and Apple Pay) have significantly dominated the retail payments market by operating under a model that closely resembles the Payment Initiation Services offered

PUBLIC

Question	MS reply
	by regulated PISPs. While authorized PISPs must be licensed as Payment Institutions to initiate payment orders from ASPSPs via Open Banking channels, pass-through digital wallets effectively achieve the same outcome. They do so by executing payments using a tokenized version of the PSU's card, ultimately utilizing another PSP's payment instrument to complete the transaction. In Greece, the Bank of Greece has taken steps in relation to SCA requirements concerning pass-through digital wallets, focusing on the following aspects: • Ensuring valid SCA during card provisioning (during the registration of a card in a digital wallet). Requiring compensation to PSUs who fall victim to fraud through pass-through wallets where stolen cards were registered without proper SCA (often accepted with inadequate methods such as SMS-OTP alone). • Ensuring that appropriate outsourcing arrangements are in place between card issuers and digital wallet providers. On the latter point, it has become evident that although issuers have contractual agreements with wallet providers, these agreements are typically based on a standardized format dictated by the wallet providers themselves. Such contracts do not classify the service as an outsourcing arrangement for SCA purposes. Issuers have stated that they are unable to negotiate revisions

PUBLIC

Question	MS reply
	to these agreements, at least not without coordinated regulatory intervention targeting the wallet providers. • For the reasons outlined above, we align with the French position that providers of pass-through digital wallets currently bear limited liability relative to the actual risks involved. We support the introduction of clear and binding obligations for these providers, particularly in the areas of ICT risk management, cybersecurity, and fraud prevention. Should these arrangements be regulated under DORA, it must be ensured that their services are classified as critical in order to enable the appropriate level of oversight.
End	DK (MS reply): ***End*** DE (MS reply): ***End*** CZ (MS reply): ***End*** CY

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): ***End*** BG (MS reply): ***End*** BE (MS reply): ***End*** AT (MS reply): ***End*** ES (MS reply): ***End*** SK (MS reply): ***End*** SI (MS reply): ***End*** SE

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	(MS reply): ***End*** PT (MS reply): ***End*** NL (MS reply): ***End*** LV (MS reply): ***End*** LU (MS reply): ***End*** LT (MS reply): **End** IT (MS reply): ***End*** IE (MS reply):

Presidency questionnaire following the WP meeting on 4 April 2025

From: DK, DE, CZ, CY, BG, BE, AT, ES, SK, SI, SE, PT, NL, LV, LU, LT, IT, IE, HR, FR, FI, EL **Updated: 22/04/2025 09:55**

PUBLIC

Question	MS reply
	End HR (MS reply): ***End*** FR (MS reply): ***End*** FI (MS reply): ***End*** EL (MS reply): ***End***