Council of the European Union
General Secretariat

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

Brussels, 07 March 2025

WK 3128/2025 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 comments PSR/PSD to the Presidency Questionnaire Ddl 28/02/2025, following WP 21/02/2025. Replies from 22 MS + ECB

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
Presidency Discussion Note **Discussion on fraud-related issues in PSR** **(authorisation, liability, burden of proof,** **gross negligence, cooperation with ECSPs) WK 2161/25**	
Q1. Which option of the two proposed above would Member States support?	AT (MS reply): We favor option 1. BE (MS reply): BE: While Belgium expressed preference for option 2 in the past, we understand that the majority of Member States who expressed their preference in the last Working Party are leaning towards option 1. If option 1 would indeed be chosen, we have some additional remarks. Firstly, special attention must be given to a clear definition of 'initiated'. There should also be some amendments on the liability regime. Also there should be clearly stated in PSR that authentication is not (in itself) sufficient to prove the consent. It is also important that the PSU can contest having authorised the payment transaction despite the fact that the procedure for giving consent as described in the contract has been completed. In this sense, PSR should clearly state that when assessing the authorisation, all the factual circumstances of the transaction should be taken into account. This could be integrated in Article 55. In this respect, we believe that the cooperation of all the

Question	MS reply
	involved parties, included the PSU and ECSPs, is important in order to provide the PSP with all the relevant information needed to understand the context in which the transaction took place. In particular, where the burden of proof falls on the PSP, there should be a clear duty of collaboration of the PSU to provide the necessary information and documents to the PSP. If option 1 is chosen, we also advocate strengthening the liability regime to provide a solution for PSUs that have been victims of social engineering fraud. In particular, we plead for an extension of the scope of the Article 59 to other types of impersonation frauds (see comment on Q5). In that case caps could be introduced for APP fraud (see comment Q3). Since par. 3 and 4 of Article 49 is deleted, we question whether the situation where a payment is initiated through or via a payee should not be elaborated more in a recital? Lastly, we strongly agree with the replacement of the word "permission" with "consent". BG (MS reply): We prefer option 1 as an approach to addressing the authorisation of payment transactions. CY (MS reply): We are supportive of Option 1 relating to the European Commission's version of Article 49(1).

Question	MS reply
	CZ (MS reply): For the sake of compromise, we support Option 1 as a way forward**. We are strongly against Option 2.** While we are still opposed to Article 59, Option 2 would in fact be much stricter than Article 59 as in the proposed Option 2 there is no correction for gross negligence. The new correction about notifying the payer is not sufficient. Article 59 is still hardly acceptable for the Czech Republic, but taken into account only the approach to authorisation, we could support Option 1. Even if Recital 69g explains that this provision would only cover cases where the payee is not the intended beneficiary, this new wording of Option 2 could lead to millions of payment transactions being challenged. It is also not clear why PSPs should be held liable for these transactions. How could PSP know that PSUs are being manipulated? The IBAN check is not sufficient in this case. DE (MS reply): **GER strongly supports option 1.** Option 1 contains a legally clear definition of authorisation that strikes a fair balance between the interests of PSPs and the protection of customers. Under the authorisation concept proposed in Option 1 (and especially with the amendment proposed in Art. 49(2)) a significant amount of fraud cases are already considered as unauthorised transactions. We consider a duality of such clear concept of authorisation and specific liability regimes as a balanced and future-proof approach. We also support the proposed wording of Art. 49(2) (Option 1). In fact, we would even go further than the proposed wording as the current wording only deems such

Question	MS reply
	transactions as unauthorised where the transaction is carried out by a third party after the personal security credentials have been fraudulently obtained, which would not include simple theft. We would suggest to deem any transaction as unauthorised where a third party carried out a transaction without the PSU's consent. Drafting proposal: ***Art. 49*** ***Authorisation*** 2. 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. Finally, we would like to express **Germany's strong opposition against option 2**. - Adding subjective elements to the concept of authorisation would present a significant shift in principle which we cannot agree to. It would lead to an excessive liability of the PSP leading to increased consumer prices and increased moral hazard as mentioned in the Presidency Note. The current proposal for option 2 would, for instance, include so called love scams where a fraudster uses a fake online identity to gain the PSU's trust and makes the PSU transfer money to a fake person pretending to be in love. These cases are completely outside the sphere of responsibility of PSPs and we do not see any justification to make them liable.

Question	MS reply
	- Besides, the current wording seems unworkable as there is no definition on what social engineering is. This could – again - potentially cover any form of deception, immensely expanding the PSPs liability without them having any chance of influencing these fraud mechanisms. DK (MS reply): We support option 2. However, we do not support the deletion of the reference to amount and payee in article 49(1) which was not reflected as an option. Though we do believe that the wording should be "with regards to" and not "including as regards". However, as a majority of MS indicated support for option 1 in the meeting, we believe the best way forward is to secure adequate consumer protection in the other articles (especially article 59). Much of the discussion has been focused on ensuring adequate safeguards for the PSPs in case we decided to include subjective elements in the definition of authorised/unautorised (e.g. spending limits, cooling off, different tools such as transaction monitoring, data sharing, blocking and postponing transactions and a burden of proof on the PSU). However, since it has now been decided not to include these elements, focus should also turn to protecting the PSU as well as reasonable liability rules (e.g. by ensuring art. 59 not only covers bank employee impersonation fraud but social engineering fraud in general). At least it should also cover impersonation fraud where the fraudster claims to be from an

Question	MS reply
	authority (e.g. the police) – not only the bank. There should also not be caps on liability if we end up with something similar to the Commission's version of article 59. If social engineering fraud is included in article 59, we could discuss national caps. EL (MS reply): EL:. We prefer option 2. If Option 2 is chosen, a clearer framework for defining gross negligence and overall liability would be essential. The key shortcoming of PSD2 is the lack of provisions for proactive fraud prevention. ES (MS reply): Option 2: a payment transaction initiated by a payer shall not be deemed as authorised where the payer was manipulated through social engineering into initiating the payment transaction. We are also open to go beyond bank impersonation fraud and cover other types of financial impersonation fraud (such as public administrations impersonation when a payment is immediately asked for). However, this must be accompanied by safeguards, including compliance of preventive measures by the PSU and sound gross

Question	MS reply
	negligence regime in articles (not only recitals) with some clear examples, as well as a robust regime for telcos. In any case, commercial fraud should not be covered. HR (MS reply): We support option 1. HU (MS reply): As we said at the CWP meeting, we strongly support Option 1 proposed by the Presidency. We understand that a shift is important in the context of consumer protection, but we need a solution that will stand up in court, that won't cause any moral hazard and is legally sound and will be interpreted in the same way. We think that changing the term 'permission' to 'consent' could be risky, as it's open to different interpretations and does not give the payer any safeguards. We understand the Presidency's reasoning, but we need to think through all the different scenarios that might come up. Inserting the term 'consent' means that there will be no single regulation, but we will need to build up the logic from different directions. This is not a problem in itself, but we must assess the cases carefully, to avoid duplications, to not leave anything out and to be able to justify the distinctions.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	IE (MS reply): Option 1 IT (MS reply): **IT.** We think Option 2 goes in the right direction. As a second-best alternative, we can agree to Option 1. The following observations concerns mainly Option 1, but are also relevant for Option 2. First of all, in our understanding, under both Options, a transaction is unauthorized when the payment order inserted by the PSU is altered by a third party without the PSU's knowledge and consent (i.e. the PSP's liability would cover cases such as man-in-the-middle/browser attacks). It may be useful to include a clarification to this effect in a Recital. Our main concerns with Option 1 are as follows: - From our national perspective, it narrows the definition of "unauthorized transactions" by excluding, at the very least, those cases where the PSU is unaware that its actions lead to the execution of a payment transaction (see again Scenario 4 described in the DE non paper of November 2023). We are uncertain whether all such cases would fall under the new Art. 59. For instance, if the PSU is not a consumer; if the third party does not impersonate a PSP; if the third party impersonates a PSP different from the consumer's PSP (what if the consumer has accounts with multiple PSPs?) or if the impersonation occurs through means not covered by Art. 59. We are not sure that such distinctions should determine whether a "fraudulent authorized" transaction is deemed worthy of protection. - The relationship between Art. 49 e Art. 59 remains unclear. In many cases the third party obtains the credentials from the PSU by impersonating the PSP, making both articles applicable. This could result in a transaction being classified as both "unauthorised" and "fraudulent authorised" at the same time. Furthermore, as currently drafted, Art. 59 imposes greater obligations on the PSU (reporting the fraud to the police; providing supporting evidence).

Question	MS reply
	We should clarify the relationship between the two articles. If Art. 59 is just a subset of Art. 49, its current wording could reduce the PSU's level of protection. If, on the other hand, Art. 59 applies only where Art. 49 does not, the aforementioned concern would be relevant. - At the same time, Art. 59 could potentially be used to extend the PSP's liability to certain cases of "external" fraud / APP fraud, a result we do not support. For example, fake investment scams. We should therefore clarify, for example in a Recital, that if the PSU carries out a payment transaction but is mistaken – be it fraudulently or not – about the underlying circumstances of the payment, the payment transaction would be authorised. We think we should clarify the relationship between Art. 49 and the "IBAN check": - Under Option 1, where Art. 49 applies, the IBAN check should not be relevant, as the transaction was initiated by the third party; - Under Option 2, in our view, the PCY proposal helps clarify the meaning of "intended payee" in the first subparagraph and prevents it from being interpreted too broadly, thereby encompassing most cases of so-called APP frauds, since in many such frauds the PSU is generally misled by a third party about the match between the payee and the unique identifier (es. romance scam; emergency scam; invoice fraud; fake investment fraud; etc.). In light of this, and in accordance with the principle that only the unique identifier is relevant for identifying the payee, the discrepancy between the payee entered by the payer and the unique identifier should not, by itself, be a reason to consider the payment unauthorized. We suggest revising the proposal's wording to explicitly state this principle. We believe the status of authorized payments should not depend on the PSU's reaction to the IBAN check—especially since the IBAN check does not apply to certain credit transfers (e.g., one-leg transactions). The above mentioned rule would also avoid making the authorized/unauthorized distinction contingent on the outcome of a complex process where multiple factors could go wrong. We propose therefore the following wording: "***Without prejudice to Article 50 and article 56 of this Regulation and to Article 5c of Regulation (EU) 2024/886 of the European Parliament and of the Council [IPR], a payment transaction shall not be deemed as unauthorised due to a discrepancy between the name of the payee entered***

Question	MS reply
	by the payer and the payee associated with the unique identifier provided by the payer". Finally (only for Option 2), we would not use the term "social engineering", as its meaning can be ambiguous. LT (MS reply): We strongly believe that a clear delineation between authorised and unauthorised, authenticated and authorised payment transactions must be introduced in PSR. Not all MSs have relevant case-law to interpret these concepts by ruling out merely formal approach, even more so – PSPs tend to follow such formal approach without litigation. Therefore, making no amendments in the definition of authorisation could bring the risk of leaving a big part of PSUs without the right to reimbursement, hence, unprotected. We would be in favor of wider protection, meaning that PSUs could be potentially protected against authorised push payments as described in option 2, however, this wider protection should be granted only under certain circumstances and conditions. Treating APP in an equal manner to unauthorised payment transactions as mentioned in option 1 would potentially create moral hazard and disproportional liability of PSPs. Therefore, we support option 1. LV (MS reply): We support Option 2 it sets more secure requirements for the payer We support deletion of paragraph 1 of Article 49 and inclusion of 2 paragraph for a option 2. We support Recital 69g,

Question	MS reply
	Regarding Article 59 we support inclusion of cooperation between PSP and electronic communication services providers. NL (MS reply): We support option 1. As indicated before we think that it is important that there is no discussion on the certainty of payments which might occur when subjective elements are included in the definition. A strong reimbursement framework within art. 59 is a more effective way to address fraud and protect consumers. PT (MS reply): PT supports going forward with **Option 1**, as it embodies our priority of not including notions of PSU's intent or other subjective indicators when assessing authorisation. The distinction between an authorised vs unauthorised transaction in those circumstances would be extremely complex for PSP to address and a proper evaluation in this regard should rather be done by the courts. We also cherish the specific finetune foreseen in Article 49(2) to highlight that a transaction initiated by a fraudster, even if subsequently authenticated by the PSU, cannot be considered authorised, as per EBA's rationale presented in its Opinion (EBA-Op/2024/01, paragraph 31(a)(ii))). On a final note, we would not oppose replacing "permission" with "consent" on Article 49(1), despite the latter appearing to be more subjective than the former.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	RO (MS reply): We support Option 2, with the following amendments We have some concerns that the complementary condition for considering authorized a payment transaction, i.e. that the payer was not manipulated through social engineering into initiating the payment transaction in favour of a third party which was not the intended beneficiary of the payment, was included into the recital 69g and not in level one text. We also have some concerns on the fact that the clarifications for the situation of unauthorized payment transactions provided under recital 69g includes only the impersonating fraud. So, we appreciate necessary that an authorized payment transaction to include the principle that the payer has given its consent for the execution of the payment transaction, including as regards the amount of the payment transaction and the payee. We appreciate necessary to maintain "including as regards the amount of the payment transaction and the payee", Art. 49 (1) A payment transaction or a series of payment transactions shall be authorised only if the payer has given its consent for the execution of the payment transaction, including as regards the amount of the payment transaction and the payee. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the account servicing payment service provider, after the execution of the payment transaction. SE (MS reply): We support option 2. This is a civil law issue. It is genuinely difficult to decide exactly which fraud victims should be compensated. Therefore, we do not think the

Question	MS reply
	PSR should make these assessments beforehand, based on the fraud method used. Instead, the PSR should provide a reasonable framework for making these assessments, much as option 2 suggests. We think that it is a misconception that this would lead to full liability for PSPs. Option 2 would simply mean that the PSP has a non-zero liability in cases of social manipulation fraud, the rest is decided by the assessment of gross negligence and other circumstances. SI (MS reply): We support **option 1.** SK (MS reply): We have strong preference for Option 1.
Q2. Do Member States agree with the proposed approach and drafting suggestions to Article 51(2), 83(1a), 83a(1a) PSR? If not, please provide an alternative wording.	AT (MS reply): We do not support the proposed amendment to Art. 51 para 2, as this could cause excessive derisking by PSPs who may block a payment instrument even if there are only slight suspicions of fraud in order to avoid any kind of liability. This kind of derisking could seriously hamper the efficient flow of payments instead of improving it.

Question	MS reply
	In general, however, the obligation to block a payment instrument in the case of a suspicious transaction should apply in any way and not only if agreed upon in the framework contract. BE (MS reply): BE: We support the drafting suggestions on Article 51(2) and Article 83(1a). As we mention previously, the PSP is in a better position to prevent fraud and should have robust fraud prevention mechanisms in place. We however share the comment of the Commission that having such mechanisms in itself is not sufficient. The mechanisms should be efficient in fraud prevention and the PSP should carry the burden of proof of this. If the PSP does not comply with its obligations on fraud prevention, it is a logic consequence for the PSP to bear the risks and the liability. However, regarding Article 83a(1a), we are not opposed to the proposal but we fear that a complete shift of liability on the PSP would be going too far given the current wording of the provision. Firstly, the causal link between the fraud data sharing and the occurrence of a fraud is quite remote. Secondly, the provision provides PSPs with a large room for manoeuvre regarding the data that could be shared and the cases where such data sharing could be allowed. Finally, we support the comment made by the Commission during the meeting regarding the validity of such shift of liability. Such liability could only be valid is data sharing arrangement is mandatory.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	BG (MS reply): We would like to see a more precise version of the Presidency's drafting proposals in Articles 51(2), 83(1a), 83a(1a) PSR. For example, it could be explicitly defined what is meant by "**reasonable grounds** for suspecting fraud". In addition, in the circumstances regulated by Articles 51(2), 83(1a), 83a(1a) PSR there do not seem to be clear examples of the payment service provider not applying due care. Finally, the drafting proposals suggest that the payer shall not bear any financial consequences. However, it is not clarified who in fact will bear the financial burden. In practice, this would create difficulties during dispute resolution processes, especially in cases of cross-border payment transactions. CY (MS reply): We agree with the proposed drafting suggestion to Articles 83(1a) and 51(2), and remain sceptical regarding the drafting suggestions for Article 83a (1a). CZ (MS reply): We support strengthening the link between monitoring mechanism and potential PSP´s liability. Article 51(2) – In principle, we agree. It might be useful to include a limitation not only regarding PSU acting fraudulently but also with gross negligence. This also applies to Article 83(1a). Article 83(1a) – In general, we agree, but it might be unclear what exactly the PSP should monitor. Regarding the definition of "execution of a payment transaction," the

Question	MS reply
	process of execution starts once the initiation of a payment transaction is completed. A more precise drafting of "prior execution of a payment transaction" would be welcomed. Article 83a(1a) – We are unsure about the second sentence. It is quite complicated to imagine how it will work in practice, as the obligation to share is between PSPs, and the payer does not play any role in the sharing. DE (MS reply): In the context of a balanced compromise, GER could in general agree to a specific liability regime for PSPs as proposed by the POL PCY in Article 83(1a) PSR. We are however critical of a PSP's liability when it comes to data sharing as suggested in Art. 83a(1a). We see difficulties as to the causality of any damage incurred due to a lack of data sharing. Regarding the proposed liability regimes in Art. 83(1a), we see the need to clarify and fine-tune these liability regimes, for instance: - We would suggest to include a provision relating to negligent behaviour of the PSU. Under the current wording, the PSP will bear all costs even if the PSU has acted grossly negligent. This might lead to unbalanced outcomes. We would therefore suggest a shared liability in such cases. In the end, it would be left to the national courts to decide on the exact proportion of liability attributed to each party. The

Question	MS reply
	shared liability provision should furthermore be accompanied by and explained in a recital. - We would furthermore include a clarification that the PSP's liability is fault-based, i.e. where the PSP is responsible (intent or negligence) for not carrying out the duties stipulated in Art. 83(1a). - The wording so far only stipulates that the PSU should not bear any financial consequences. It is not clear whether the PSU has a direct claim only against his/her PSP or also the payee's PSP. Those issues could be addressed in a new provision – similar to Art. 57 PSR – regulating the liability regime that dependents upon the PSP carrying out the duties in 83(1a), instead of adding a sentence to Art. 83(1a) PSR. Finally, in the context of a balanced compromise we could accept a similar specific liability framework for a PSPs duty to block the use of a payment instrument based on objectively justified reasons relating to the security of the payment instrument (Art. 51(2) PSR). However, we share the concerns of MS raised in the working party that such provision would pose significant risks of de-risking and hence, would finally be to the detriment of consumers. If such specific liability regime was introduced, the issues referred to in the context of the specific liability regime of Art. 83(1a) need to be addressed as well. DK

Question	MS reply
	(MS reply): Overall, we support the proposed changes. However, we believe the lists for both transaction monitoring and data sharing should either be non-exhaustive or alternatively be moved to level 2 to provide for more flexibility. Regarding the condition in article 83a it seems excessive. The assumption seems to be that information sharing will always be able to stop fraud. Furthermore, data-sharing is not easy and will involve difficult trade-offs (and will not always be an option, e.g. in a cross-border context). Hence, we would prefer not to add to article 83a - or at the least prefer that this condition be qualified so that it only has relevance if such data-sharing could have stopped the fraud. EL (MS reply): EL: We generally agree with the drafting suggestions. However, we are concerned about derisking by PSPs and the potential incentives to reject large volumes of transactions out of fear of repercussions. ES (MS reply):

Question	MS reply
	We strongly support amendments to Article 51 (2). Indeed, there is added value in putting the focus on prevention and linking liability to the lack of compliance with preventive measures, and in this case where such blocking does not take place despite reasonable grounds for suspecting fraud, the payer shall not bear any financial consequences, except where the payer has acted fraudulently. The same applies to article 83 a) which we also strongly support: Where such monitoring does not take place, the payer shall not bear any financial consequences, except where the payer has acted fraudulently. In relation to article 83a i (a) we consider a good way forward to convert into mandatory the exchange of information in fraud (we note the amendment from "may exchange" to "shall exchange" and to link it again with liability: where such exchange of information does not take place, the payer shall not bear any financial consequences, except where the payer has acted fraudulently. We can also add: "*where the PSP does not take any action when the exchange of data provides information to suspect fraud in a concrete transaction, the payer shall not bear any financial consequences, except where the payer has acted fraudulently"*. FI (MS reply):

Question	MS reply
	FI: We support the idea of incentivising PSPs to take action where there are grounds for suspecting fraud. We should ensure that PSPs are able to understand when such grounds take place. For this, recital 69d is a good starting point. HR (MS reply): We do not support the proposed shift of liability in cases where payer's PSP fails to fulfil its obligation for data sharing. We agree with the proposals for the shift of liability in cases where PSP fails to fulfil its obligations regarding blocking a transaction or transaction monitoring. HU (MS reply): Fraud prevention is essential, we support everything that strengthens it and oppose everything that weakens it. However, we cannot accept burdens that are not causally linked. We consider these specific liability cases to be acceptable for the sake of a compromise, but further clarification and specification is needed. Caution should be exercised when imposing liability, we do not believe that there is any justification for over-exemption of the client from liability and imposing liability based on a reason outside the interest and scope of the PSP. IE (MS reply): 51(2) – Agree, 83(1a) – Agree, 83a(1a) – Agree.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	IT (MS reply): **IT.** We understand the rationale behind the proposal, since the measures in Art. 51; Art. 83 and Art. 83a are very important to prevent fraud. In our understanding, the proposal would exclude, in certain cases, the relevance of the PSU's intent or gross negligence (and the rest of art. 60 PSR). We do not agree with the proposal, as currently presented. In general, the proposal to introduce stricter liability rule could incentivize PSPs to apply such security measures too broadly (so called de-risking). An excessive number of "false positives" could undermine the effectiveness of the TRM and data sharing, disrupting the regular flow of payment transactions. We also have the following observations: - Art. 51(2): the proposed rule applies when the PSP fails to block a payment instrument "*despite reasonable grounds for suspecting fraud*". We point out that assessing such suspicion is inherently case-dependent and probabilistic. The failure to apply such measure correctly could be a matter of dispute, as determining whether a specific payment is "suspect" is not always straightforward. Therefore, we do not believe that a blanket rule is justified. (Furthermore, the blocking is only possible "if" agreed in the framework contract). - Art. 83(1a): the proposed rule applies when the TM does not take place. In principle, we could agree if the proposal were limited to cases where the PSP *entirely* fails to conduct the TM. However, we are concerned that ADR bodies or Courts may easily extend the rule to cases where the TM was performed, but it is debatable whether it was performed correctly. In such a case, the concerns outlined above would apply. - Art. 83a(1a): the proposed rule applies when the PSP fails to exchange with other PSPs data relating to a PSU suspected of fraudulent behaviour. As this assessment is also case-dependent and probabilistic, the abovementioned concerns applies. Furthermore, in this scenario, the PSP "at fault" would be the payee's, yet the stricter liability rule would apply to the PSP of the payer.

Question	MS reply
	(Also, in our understanding, the participation in an "information sharing arrangement" is not mandatory for PSPs). Moreover, from a practical standpoint, these aspects are difficult to assess in the initial phase (after the PSU denies having authorised a transaction), since only the PSU and the PSP are involved. Even if the PSP has the burden of proving its compliance, the PSU has no means to evaluate the evidence and, in any case, the final decision on the reimbursement request, at this initial stage, is taken by the PSP. Any potential fault by PSPs to comply with the above mentioned provisions is more appropriately evaluated by an ADR body or a court, which, at that stage, would have the necessary means to conduct a more comprehensive assessment of all parties' actions and can reach a decision based on all the relevant circumstances of the specific case. Therefore, if the reimbursement request reaches such a stage, there is no need for a blanket rule. We think that a rule on "contributory negligence" could be useful in addressing the concerns underlying the proposal. Indeed, if the PSU was "grossly negligent" it would be improper to shift all the liability because, for example, the transaction monitoring was not properly performed or not enough data was exchanged. If both parties are "at fault" a shared liability would the most flexible and equitable solution. To this end, a preliminary proposal could be to amend the final subparagraph to **Article 60(1)** as follows. The PSP's failure to fulfil its obligation should be relevant only when the PSU has been grossly negligent (if the PSU was not grossly negligent, then, in accordance with the general rule of Art. 49, the PSP should fully refund the unauthorized transaction). "*1. […] Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, national competent authorities* ***or dispute resolution bodies*** ~~***or payment service providers***~~ *may reduce the liability referred to in this paragraph, 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* ***and, where applicable, the payment service provider's failure to fulfil its obligations under this Regulation, including transaction monitoring referred to in Article 83***". LT

Question	MS reply
	(MS reply): We agree with the proposed drafting suggestions for 51(2) and 83(1a). However, regarding 83a(1a) and its practically applicable additional value - it is not clear how a PSU could know and prove the fact that its PSP has failed to provide or has failed to use such information. Also, it is not clear whether this proposal refers to situations that involve only the payer-its PSPs or the payer and payees an/or other PSPs that failed to fulfil data sharing obligation. LV (MS reply): We support the drafting proposal. NL (MS reply): Article 51(2) We can agree to this and can support the shift in liability in case the PSP did not block transactions despite reasonable grounds for suspecting fraud. However, we must introduce certain safeguards to avoid that transactions are preventively blocked. Article 83(1a) We can agree to the addition of this sentence. We suggest the following wording: Where such monitoring did not take place, the payer shall not bear any financial consequences, except where the payer has acted fraudulently. We would also like to add a clarification that transaction monitoring should be conducted in real-time, to

Question	MS reply
	prevent adverse impacts of ex-ante monitoring of transactions on the efficiency of payments. Article 83a(1a) We agree to making the sharing of data mandatory. We can follow the reasoning that PSPs should be penalized in case they do not fulfil their obligation under this provision. However, we suspect that this would be within the sphere of the relevant national supervisory authority, who can examine the case further and if required, take measures against the PSP. A penalty in the form of reimbursing the PSU seems less logical, also because it seems impractical: how would a PSU know and prove that the PSP did not fulfil its obligations? We also want to refer to our previous comments regarding broadening the purposes for which data sharing is allowed. PT (MS reply): PT is not against the amendments introduced in Article 51(2), but we fear this approach may incentivise over usage of such options for protective reasons when a PSU proceeds with an idoneous, but unusual payment. We understand "for objectively justified reasons" may preview this concern. Concerning Article 83(1a), we are in favour of the respective draft.

Question	MS reply
	Finally, on Article 83a(1a), we do not to favour tying a liability shift provision for failing to carry the data sharing. In our view, in case of a fraudulent transaction, it would appear to be rather complex to ascertain the degree of information that should have been exchanged, and which PSP (payer or payee) should have better contributed to prevent this occurrence. Therefore, we recommend removing the sentence previewing the liability shift to PSP in case the exchange of information does not take place. RO (MS reply): We support the wording of articles 83(1a) and 83a (1a) of PSR, including the sentence added "*Where such exchange of information does not take place, the payer shall not bear any financial consequences, except where the payer has acted fraudulently" that* we think will have a positive outcome on payer security and afterwards on limiting its liability in case of fraudulent transactions. SE (MS reply): It is difficult to assess the consequences of the proposal to explicitly link these obligations to financial liability. We would suggest that such negligence on behalf of the PSP should be included in the gross negligence list in recital 82 instead, side by side with the other PSP obligations in point c.

Question	MS reply
	Furthermore, we support the change from "may" to "shall" in article 83a, but think it is important to clarify that the list of information to be shared is not exhaustive. We find the current wording inconclusive, saying that: "The catalogue of data that may be shared shall include:…" . We would therefore propose to add, "but not be limited to" in accordance with a previous proposal from the Danish delegation. SI (MS reply): We agree. SK (MS reply): We can agree with drafting suggestions.
Q3. Would Member States also prefer to introduce a cap with regard to the PSP's liability? If so, would Member States agree to set it nationally?	AT (MS reply): A cap set at a reasonable level that does not affect low value payments could contribute to a balanced liability framework. If introduced, it should probably be set nationally to cater for price and income level differences between the MS. BE (MS reply): BE: If option 1 is chosen and there is a broad scope of fraudulent authorised payments in Article 59 PSR (so not only bank employee impersonation fraud), we are not

Question	MS reply
	opposed to having a cap on the PSP's liability since a right balance should be struck and gross negligence is still in play. For the time being, our preference would be to set such a cap at national level.. But if option 1 is chosen and the scope of frauds being subject of such refund would be limited to bank employee impersonation fraud, we are not in favour of having caps since this would be a regression compared to the Commission's proposal. If option 2 is chosen, APP fraud would be considered as an unauthorised payment and Article 59 PSR would no longer be needed (safe from the cooperation duty with ECSP's). In this case caps are not acceptable concerning unauthorised payments. BG (MS reply): We disagree with the Presidency's proposal to introduce a cap to the payment service provider's liability. CY (MS reply): We do not oppose the introduction of a cap, at a level to be agreed among the member states and which should be made known to consumers. CZ (MS reply): We are flexible. It depends on the final agreement and other elements of the liability issue as potential caps are not standalone measures.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	DE (MS reply): - DK (MS reply): If we decide to go with option 1 in article 49, we do not support the introduction of caps (if article 59 is expanded significantly we could be open to discuss national caps, but with the Commission's proposal and the currently suggested wording, we do not support caps). EL (MS reply): EL: We do not support a cap on the PSP' s liability but If we go to caps, we may consider allowing member states to apply different levels of caps based on domestic criteria. ES (MS reply): ES is flexible on caps. If we were to introduce caps there needs to be some granularity depending on the type of fraud, and we have preference for a percentage of the total amount lost, rather than a maximum amount to be reimbursed.

Question	MS reply
	FI (MS reply): FI: We remain sceptical towards caps. But if a cap would be introduced, it should be set nationally. HR (MS reply): We do not support introducing caps. HU (MS reply): Regarding Art. 59(1), we propose the introduction of a cap, with the Member States' specificities and differences taken into account, so we support the development of a national cap option. IE (MS reply): In regard to the potential use of caps on reimbursement, they would need to be carefully calibrated in order to ensure they are not detrimental to PSUs. IT (MS reply): **IT.** We do not agree to introduce a cap on the PSP's liability, if the liability of the PSP is not extended beyond "unauthorised transaction" (with the caveats outlined above). A hard cap could be considered more appropriate, for example, in the context of the UK liability regime

Question	MS reply
	for APP fraud, where it might well be seen as a counterbalance for the (virtually unlimited) scope of the PSP's liability. LT (MS reply): Setting a liability cap could be left to MSs discretion, however, liability cap could be deemed mandatory in case of bank employee impersonation fraud - to avoid disproportional burden of liability on PSPs part. LV (MS reply): In general, we could support the inclusion of a cap, but in EU level. NL (MS reply): We are not in favour of setting a cap, either at EU-level or at national level. If the conditions for reimbursement have been met, the PSU should receive full reimbursement. PT (MS reply): PT does not support introducing caps in the legal text, since, in our view, such limits could be deterrent to the implementation, and further expansion, of mitigation measures by the PSPs. As these need to be future proof and account for new emerging fraud modus operandi, continuous adaptation will be needed and imposing a static cap may hamper those efforts. Moreover, we highlight the emergence of negative

Question	MS reply
	externalities could also be verifiable on PSU, given the probable less caution on their part when conducting payments with value bellow the adopted cap. If caps are to be implemented, PT would prefer it to be set at national level. RO (MS reply): We do not support to introduce a cap with regard to the PSP's liability. We appreciate that in order to introduce a cap with regard to the PSP's liability an extended analysis must be performed in order to ensure a correct implementation. In addition, we think that a formula, or percentage, if considered necessary should be detailed based on fraud type and should be decided upon and applied to all MS in order to ensure uniformity. SE (MS reply): No. We would consider a cap as a safeguard if we were to introduce very consumer friendly renumeration rules. If a compromise is to be based on option 1 in article 49 however, this would be a very unbalanced approach. SI (MS reply): If we agree to Option 1, we believe that the caps are unnecessary and that, combined with Option 1, the PSR could become "consumer-unfriendly". However, if Option 2 is supported, we could support the introduction of caps. SK

Question	MS reply
	(MS reply): No, we do not support capping the PSP´s liability. PSP is liable under specific circumstances, under which it is in its hands to avoid or minimize damages. If PSP fails to do so, there is no reason to cap its liability. On the other hand we supportive towards claim excess, which set liability for payments under certain level on the PSUs as it can motivate their prudence.
Q4. Do Member States agree with the proposed approach and drafting suggestions to Recital 69d and Article 69(2a) PSR? If not, please provide an alternative wording.	AT (MS reply): Yes, we agree. BE (MS reply): BE: We agree with the Presidency's proposal. Freezing funds can be seen as a double security measure with regard to the execution of a payment transaction for which there are reasonable grounds for suspecting fraud. Nevertheless, we believe that the payer's PSP and the payee's PSP should communicate with each other immediately where one of them has reasonable grounds for suspecting a fraud. In this case, all the PSPs involved in the payment transaction should collaborate to prevent funds being available to the fraudster. BG (MS reply):

Question	MS reply
	We believe that it could be explicitly defined what is meant by "**reasonable grounds** for suspecting fraud". CY (MS reply): We do not oppose the proposed approach. CZ (MS reply): In general, we can agree, but the ability to block funds based on the results of the transaction monitoring mechanism should be available to the payer's PSP as well, not just the payee's PSP [Article 69(2a)]. Recital 69d – very useful. DE (MS reply): Regarding Rec. 69d: support Regarding Art. 69(2a): GER could generally support Art. 69(2a). DK (MS reply): We are very happy to see the presidency's proposal and support this option. However, we would prefer to delete the reference to the transaction monitoring mechanism since

Question	MS reply
	there could be other indications of fraud which the PSP should also be allowed to act on. EL (MS reply): EL: We agree with the proposed drafting suggestions in recital 69d about the transaction monitoring mechanism and the fact that a payment order is unusual should not automatically constitute grounds for suspecting that the payment transaction is fraudulent, nor should it by itself constitute reasonable grounds to suspect fraud. Regarding the suggested changes in article 69.2a in order to give possible ways for the Payee's PSP to support in combatting fraud, we generally agree, however we propose the following drafting suggestion in orange for article 69 (2a) which are aligned with the Presidency' s suggestion for article 65(1a) in the fraud note of the meeting of 28 January. 2a. If the **transaction monitoring mechanisms**, referred to in Article 83, indicate reasonable grounds to suspect a fraudulent payment transaction **from either the payer's payment service provider or the payee's payment service provider**, ***then the payer's PSP may have the right to block or delay the execution as per article 65(1a)*** or the **payee's** payment service provider may postpone making the funds available to the payee. The payee's payment service provider shall without undue delay as necessary ascertain whether the transaction is in fact fraudulent and either make the funds available to the payee or, if the transaction is deemed fraudulent, return the funds to the payer's payment service provider. ES (MS reply):

Question	MS reply
	We agree to recital 69 d) we consider that indeed, the fact that a payment order is unusual should not automatically constitute grounds for suspecting that the payment transaction is fraudulent, nor should it by itself constitute reasonable grounds to suspect fraud and that where the payment service provider has duly justified and it has reasonable grounds to suspect fraud, a refusal in good faith to execute or postpone a payment transaction should not involve the payment service provider in liability of any kind. We also agree to article 69 (2a) since indeed there was a lack of regulation on the payee PSPs side " If the transaction monitoring mechanisms, referred to in Article 83, indicate reasonable grounds to suspect a fraudulent payment transaction from either the payer's payment service provider or the payee's payment service provider, then the payee's payment service provider may postpone making the funds available to the payee. Finally, in order to consider the network network of digital payments, we could also include any payment service provider in the payment chain: "*the payer's service provider or any other payment service provider in the payment chain might refuse to execute the payment transaction*." FI (MS reply): FI: Mainly yes. Regarding Article 69(2a), we support the proposal. However, the provision could be improved by deleting the reference to TMM and the payer's PSP

Question	MS reply
	or only mentioning TMM as an example. The information could be obtained from other sources, and we should not limit the sources from which the indication for reasonable grounds to suspect a fraudulent payment transaction should come in this provision. Also, we are wondering if the last sentence of recital 69d should also mention blocking of a payment instrument to reflect the changes suggested in Article 51(2). HR (MS reply): We strongly support the new proposal to add a tool for the payee's PSP to freeze funds in case of a suspected fraudulent transaction. However, we propose to consider the part of Article 69(2a) in relation to the returning the funds to the payer's PSP because that provision is vague in terms of further steps to be taken by the payee's PSP. Sufficient time should be provided to verify the transaction. Funds should not be returned to the payer's PSP before a court or FIU decision is obtained. We support recital 69d. HU (MS reply): We support the measures to strengthen fraud prevention and can therefore agree with the proposal, however, we also propose to clarify and specify the content of Article

Question	MS reply
	69(2a) and the related Recital in order to clearly impose liability on the PSP on the basis of this provision. IE (MS reply): The drafting appears reasonable and we support the intentions here but it needs to be balanced to stop non-execution of transactions by PSPs being the default position. There is (generally) an asymmetrical power relationship between PSP and PSU – so non-execution should also come with actions for the PSP toward the PSU (speedy execution of 'false positives' without significant PSU input or similar). We agree that PSPs should be facilitated in taking a risk-based approach to processing payment transactions where they suspect fraud. This could be achieved by allowing PSPs delay making an outbound payment transaction so that investigation can be carried out if there are reasonable evidence-based grounds to suspect fraud or dishonesty on the part of someone other than the payer. It is important that this does not adversely affect consumers by causing unnecessary delays to legitimate payments and that consumers continue to get fast and reliable payment services. This could also be achieved by allowing/obliging PSPs not to process a transaction that is suspected of being fraudulent; this could mirror or align with provisions in Article 71(1) AMLR (Anti-Money Laundering and Terrorist Financing Regulation). IT (MS reply): **IT.** We would like to know the Presidency's assessment of the proposals regarding Article 65(1a) that were presented at the previous WP and why they were not taken as a starting point.

Question	MS reply
	On R(69d): We agree that if the PSP has *correctly* exercised the powers granted to it by the PSR, it should not be held liable. However, if an ADR/Court, after assessing all the circumstances of the specific case, determines that the PSP has misused its power to refuse/postpone a transaction, resulting in a measurable harm to the PSU, the PSP's liability may be recognized. Accordingly, we understand that Recital (69d) excludes the PSP's liability only when a set of conditions is met ("good faith", "duly justified and reasonable grounds"), the existence of which may be subject to judicial review. In any case, the wording should be "*a refusal in good faith to execute or **the decision to** postpone a payment transaction*". LT (MS reply): We agree with the wording. LV (MS reply): We support the drafting proposal. NL (MS reply): We find the proposed approach generally agreeable; however, a discussion is necessary to address how we will minimize adverse effects on PSUs. If a significant portion of transactions are delayed, it could lead to inefficiencies in the payment

Question	MS reply
	system. What is for example the acceptable percentage of false positives in transaction monitoring, and how long can these funds be delayed without causing cash flow issues? Additionally, how would this be technically implemented, given that it differs from rejecting a payment, and how would the communication to the PSU be presented? A timeframe should be included within which a PSP must decide whether a transaction can indeed be classified as fraudulent. Regarding recital 69d, it is not completely clear to us what is meant with the last sentence and the wording 'should not involve the payment service provider in liability in any kind'. What liability is meant here? **The following provisions were not part of any questions, but we would still like to comment on them:** Recital 69g We believe that it would be necessary to provide some explanation as to what social engineering may entail. The text is also rather confusing, as it mentions social engineering twice. If we understand correctly, the aim is to distinguish between manipulation that does not directly concern the elements of the transaction (regular manipulation) from manipulation that is concerned with such elements (social engineering). This should be clarified. Recital 79

Question	MS reply
	This recital should be amended to reflect the changes made in the corresponding article. If we require both the name and mail address, this should be stated here as well. The additional sources added to the provision (website and application) should be added here as well. PT (MS reply): On Article 69(2a), PT considers that it is important to clarify in the draft that postponing cannot result in permanent blocking of the funds, which can embody risks for the regular functioning of payments and to the PSUs' confidence in the payment system. Therefore, we propose the Payee's PSP analysis in this regard should be carried within a maximum of two working days, taking inspiration from the current mandated execution period for payment transactions, as depicted in Article 83 PSD2. We also believe the payer's PSP should be informed of the suspension of the transaction. Please consider the following adjustments: *"2a. If the transaction monitoring mechanisms, referred to in Article 83, indicate reasonable grounds to suspect a fraudulent payment transaction from either the payer's payment service provider or the payee's payment service provider, then the payee's payment service provider may postpone making the funds available to the payee. The payee's payment service provider shall without undue delay as necessary, and within a maximum of two working days, ascertain whether the transaction is in*

Question	MS reply
	fact fraudulent and either make the funds available to the payee or, if the transaction is deemed fraudulent, return the funds to the payer's payment service provider. The payee's payment service provider shall notify the payer's payment service provider about the assessment being conducted." Moreover, PT disagrees with including the last sentence of the proposed Recital 69d (*"Where the payment service provider (...) in liability of any kind."*) since, in our view, expectations in this regard may be highly dependent on the cases presented and ultimately the courts' intake should be expected to be a decisive factor. RO (MS reply): We strongly support the drafting suggestions of recital 69d, since these are in line and very supportive for the efficient tool included under article 69 for blocking/postponing payment transaction. SE (MS reply): We agree with the proposal in recital 69(2a) but would suggest to **delete the reference to transaction monitoring**. The payee's PSP should be able to freeze incoming funds if there are reasonable grounds for suspecting fraud, regardless of source of information.

Question	MS reply
	We also agree with recital 69d and support the amendment that a PSP blocking a payment transaction should not risk facing liability. Our only remark would be that we find the words "of any kind" a bit excessive and could be left out. SI (MS reply): We agree. SK (MS reply): We agree with proposed approach, however some time limit on the postponement of making funds available should be set, to avoid situations where, based on the suspicion, funds are frozen for long periods of time.
Q5. Do Member States agree with the drafting suggestions to Article 59 PSR (for Option 1 or 2, depending on the chosen approach)? If not, please provide an alternative wording.	AT (MS reply): We still remain sceptical regarding the liability of PSPs for bank employee impersonation fraud. In particular, the amendment regarding the PSP's website or mobile application seems excessive, as the PSP cannot control any such kinds of fraud. On the other hand, the obligation for consumers to provide supporting evidence seems a step into the right direction to mitigate the PSP's burden of proof. BE (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	BE: In case option 2 would be chosen by the Presidency (see Q1), we would be in favour of deleting Article 59 PR, except as regard the duty of cooperation for ECSP's. However, in case option 1 would be chosen, the scope of frauds subject to a refund would be rather limited. In this respect, we suggest to extend the scope of the Article 59 PSR to other types of frauds based on social engineering and not limit it to bank employee impersonation fraud since there are a lot of different types of impersonation fraud which lead to significant financial losses and a lack of confidence in several entities like for example national institutions and public entities. BG (MS reply): We prefer the drafting proposals in Option 1. CY (MS reply): We agree with the drafting suggestions to Article 59 PSR under Option 1. CZ (MS reply): Despite we can imagine supporting Option 1, we do not support Article 59. The reasons were mentioned many times – moral hazard, shift of liability to PSPs which are not able to prevent fraudster from pretending to be their employees etc. In any case, our disagreement with Article 59 cannot be understood as support to Option 2.

Question	MS reply
	DE (MS reply): As argued before, we strongly support option 1. In the context of a balanced compromise, GER can in principle agree with the drafting of Art. 59 PSR as proposed by the POL PCY. In particular, we believe that the safeguards included in Art. 59(2b) regarding fraud and gross negligence on the part of the consumer strike a fair balance. We are however critical regarding the proposed changes to Art. 59(1) that the name and telephone number or e-mail address are required. In our view the Commission proposal does not impose a disproportional burden on PSPs. The PSP also has the possibility to react when the fraudster uses the bank name but another e-mail address or telephone number. We further support widening the scope to include fake websites and apps. DK (MS reply): We agree with the need to adapt the liability rules to reflect the outcome of the authorized/unauthorized discussion. If we go with option 1 in article 49, we see a need to significantly strengthen the protection offered in article 59. This could for instance be by including social engineering fraud in article 59 or at least expand to include impersonation of not only the bank but also public authorities as well.

Question	MS reply
	Regarding the suggested amendments to art. 59(1) in option 1 where it is suggested that two elements need to be included to consider it as bank employee impersonation fraud. We do not support these amendments as we would see it as a step back for consumer protection compared to the Commission's proposal. It would also be significantly more difficult for a PSU to prove this. We believe there should just be a reference to bank employee impersonation fraud more generally without requirements for the number of elements to be used. The notion of "without any delay" also seems too strict and should be changed to e.g. "without undue delay". It is also very important to add that it should be from when the fraud is actually discovered by the PSU. If the PSU has not been aware of the fraud taking place, they can of course not be expected to notify neither the police nor their PSP. Many PSUs and especially vulnerable persons might not notice the fraud right away but only later on. Furthermore, we believe the obligation to report it to the police could be on the PSP instead since this would be a significant step for vulnerable citizens. Lastly, we also believe that the PSP should be requesting the information from the PSU. The obligation should not be on the PSU to proactively provide this, since we cannot expect the PSUs to know this when notifying the PSP of the fraud, and we fear that

Question	MS reply
	many would be rejected by their PSP if this wording is included. It would be easy for the PSP to request the PSU to provide this information. It is also important that there are not unrealistic expectations as to what kind of evidence the PSU could be expected to have. Drafting suggestion: "…under the condition that the consumer has, without ~~any~~ **undue** delay, reported the fraud to the police and notified its payment service provider **when becoming aware of the fraud,** providing supporting evidence available to the consumer **upon the request of its payment service provider**." Shared liability We are also not sure where to place this, but we still support a potential shared liability between the sending and receiving PSP. The receiving PSP allowed a fraudster into their system and should therefore also share the liability for the fraud with the PSU's own PSP. This would incentivize the receiving PSP to act swiftly to postpone making transactions available, make use of the possibility to postpone making transactions available, and ensure proper KYC-procedures. Regarding the wording of article 59 para (5). We support that ECSPs should co-operate with PSPs in cases of fraud.

Question	MS reply
	However, we think this should be a more general obligation, not only in cases of bank impersonation fraud as the proposed wording suggests. Furthermore, we see no reason to limit this obligation to cases concerning consumers. We are supportive of the suggested obligation for ECSPs to cooperate with PSPs, as it provides a flexible framework for ECSPs. The flexibility allows them to both utilize the most effective methods available at any future point in time and to adapt solutions to differences in member state's legislative requirements. Differences in national legislation means that telcos have different tools and methods available for especially the prevention of fraud telcos, which should be taken into account. Suggestions to ensure more ambitious and effective cooperation efforts by telcos could be to include a preamble with examples of existing methods and cooperation between telcos and PSPs, and/or to require the Commission to provide guidelines for the compliance with the cooperation requirement. We are further supportive of the specification that measures should be in compliance with the ePrivacy directive. We would prefer to split up the definition of ECSPs into two separate definitions of telcos and digital platforms, respectively. Telcos and digital platforms have very different possibilities to act and have very different roles with regard to the kind of content they host, why they should be given different obligations.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	EL (MS reply): EL: We agree with the conditions in relation to the provision of supporting evidence. ES (MS reply): We agree with option 2. We believe the approach of converting article 59 into a cooperation related article between electronic communications services providers and Payment service providers's liability in terms of impersonation fraud fits very adequately in the context of the objective of involving all players in the fight against fraud. We bring here again our previous comments, and we update the approval of the amendment of our national law: *We would like to highlight the relevance of declaring the obligations of all actors in the payment chain under the PSR, so that they arise at the same time, with a specific mandate to Member States to develop such provisions under the specific sectorial regulation and amend if needed the national telecommunication regime. For instance, in Spain, national legislation is currently being amended in order to allow ECS the possibility to block calls and/ or SMS where fraudulent elements are identified.* See our comments below.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	FI (MS reply): FI: In case option 1 will be chosen as the way forward, the scope of Article 59 should be carefully evaluated. At this stage, we note that requiring multiple elements under the provision (i.e. *the name and~~or~~ e-mail address* etc.) could significantly narrow the provision's scope of application. Furthermore, it is unclear whether fake websites or mobile applications etc. would be covered by the provision, and if not, the scope would be extremely limited. Moreover, the wording "*without any delay*" under Article 59(1) is unnecessarily strict and should be amended to "**without undue delay**". This would also reflect recital 80 in COM proposal. Furthermore, it could be added that the PSU reported the fraud and notified its PSP "**when becoming aware of the fraud**" and that supporting evidence available to the PSU would be provided "**upon request of its payment service provider**". HR (MS reply): We agree with the drafting suggestions to Article 59 PSR, as proposed for option 1. HU (MS reply):

Question	MS reply
	Considering that we can only support the direction under Option 1 for Article 49, we can show openness to a modified Article 59 (option 1), but we indicate that we basically agree with the use of a closed logic system under PSD2. IE (MS reply): We can support option 1 or the Commissions text but we don't support the deletion of paragraph (5), we support the inclusion of paragraph (5) as amended in our non-paper. IT (MS reply): **IT.** If option 1 is to be followed, see our answer to Q1. If option 2 is to be followed, we agree with the deletion of Art. 59(1)-(4). In our understanding, under option 2 for Art. 49, the only transactions that would remain covered by art. 59 would be certain APP frauds, where the fraudster impersonated a PSP employee (e.g. to offer a fake investment). On the other hand, cases where the fraudster, by impersonating a PSP employee, convinces the PSU to hand over the personalized credentials or to perform an action that results in a payment without the PSU being aware of it (e.g. by faking security concerns), would fall under Art. 49, as the transaction would be considered unauthorized. We therefore agree to the deletion of Art. 59(1)-(4), as we believe PSPs should not be liable for APP frauds.

Question	MS reply
	In any case, we believe that the remaining paragraph (5) of art. 59 (on the duty of cooperation for ECSPs) should not be limited to cases of impersonation of a PSP employee. Such a duty would be useful in all fraud cases (not just in that specific scenario) and for all PSUs (not just consumers). LT (MS reply): We agree with the wording. LV (MS reply): We support Option 2 and Article 59 - Regarding Article 59 we support inclusion of cooperation between PSP and electronic communication services providers NL (MS reply): We basically could also accept the proposed new replacement text of the old article 59(1), but have some remarks with some minor amendments. The provision now states that the third party should use the e-mail address / number / website / mobile application of the PSP. This should read: reasonably suspected appear to use, as the third party (fraudster) will likely not use the actual number/website et cetera. Furthermore it is unclear whether the use of the name of a PSP/bank refers to the use within the body of the message or call or to – as it is technically possible - the

Question	MS reply
	message origin header or Calling Line Identification (CLI). We assume that the first is meant. We note that alphanumeric characters may be used also in message origin headers and in CLI. This makes the consideration by the PSU (e.g. when no fake name in the message/call body is used there might be a disproportional burden on PSPs) more complex and in the latter scenario there are possible reactive/preventive measures that could be taken by PSPs (in collaboration with ECSPs). While taking note of the proposal for new recital 81a and article 108, we see merits in some elements of our previously shared text proposals to Article 59(5). If the wording of Article 59(5) is kept in its current state, we fear that legal uncertainty for ECSPs may be a consequence until the foreseen relevant additional regulations will be introduced. To minimize this uncertainty, and to be able to balance actions between different types of ECSPs within the service chain, at least: - the collaboration obligation should be applied also to interactions between all involved ECSPs; - the required actions with regard to the ending of fraud occurrences should be specified more accurately. In the framework of the possible new Article 108, if maintained, in a second stage an additional regulatory framework for ECSPs for taking preventive measures should be considered. PT

Question	MS reply
	(MS reply): Considering the draft previewed for Option 1, PT welcomes the amendments introduced on Article 59(1), on pairing PSP's name usage with either the e-mail or phone number to guarantee a liability shift, given sole name impersonation might be difficult and an unbalanced expectations for PSP to effectively mitigate such cases. On the scope broadening to include manipulation of the PSP's website and app, despite not opposing it, PT would leave this expansion contingent on advancements to be adopted in PSR regarding ECSP involvement in combating fraud, as effective prevention measures from PSP also depend on the former entities' cooperation and effectiveness. The mentioned advancements need to go beyond the review clause in this regard proposed by the PRES PL. RO (MS reply): We support option 2. – This option is more complete because it adds essential information to art. 56(6) ref. to the USP refunds by the PSP and should be read in conjunction with Art. 56(6). SE (MS reply): If a compromise is to be based on option 1 in article 49, we see a need to significantly strengthen the consumer protection offered in article 59.

Question	MS reply
	First of all, we strongly oppose the proposed amendments to art. 59(1) in option 1 (changing "or" to "and"), suggesting that two specific elements need to be included in the fraud to be considered as bank employee impersonation fraud. The proposal would **weaken consumer protection** and significantly **change the scope of the article**. For example, it would exclude a common modus operandi in bank impersonation fraud in Sweden, where the customer's identification process with the bank is hijacked by the fraudster. The identification process is provided by a standardised identification application (BankID), owned by the large Swedish banks. They are therefore collectively responsible for the security of the application. Secondly, in principle, we support widening the scope of bank impersonation fraud to cover the use of fake apps and websites, but we think that a reference to bank employee impersonation fraud more generally should suffice, without specifying different elements of fraud – for example as follows: "*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…"*

Question	MS reply
	Furthermore, we think that article 59 should cover social engineering fraud more generally, or at least be extended to include impersonation fraud of public authorities as well. We also agree with the Danish delegation that the notion of "without any delay" is too strict and that this time frame in any case should be counted from when the fraud is actually discovered by the PSU. Furthermore, it may be difficult for the PSU to assess exactly what information the PSP needs. Therefore, we suggest that the article is updated as follows: "…under the condition that the consumer has, without ~~any~~ **undue** delay, reported the fraud to the police and notified its payment service provider **when becoming aware of the fraud**, providing supporting evidence available to the consumer **upon the request of its payment service provider**." This would be in line with the provision in article 55(3). SI (MS reply): We agree. SK (MS reply): We agree. However, we have some concerns on the wording "name and e-mail address or name and telephone number". We agree that PSP´s name itself should not

Question	MS reply
	be enough to categorise fraud as a bank employee impersonation fraud, however current wording would allow PSP to avoid liability in cases where e-mail address is used in combination with part or incorrect version of the name of the PSP, or cases when fraudster uses telephone number of a PSP to mislead the consumer while not mentioning name of the PSP explicitly or in full. Also, it is not clear to us if abbreviation of PSP´s name would count as a name of the PSP for the purpose of this article.
Q6. Do Member States agree with the proposed approach and drafting suggestions to Articles 55(3), 56(6) (for Option 2 only), 60(1) PSR? If not, please provide an alternative wording.	AT (MS reply): Yes. BE (MS reply): BE: On Article 55 (3), we agree with the drafting suggestion. However, as mentioned in our comment under Q1, we believe that PSR should clearly state that when assessing the authorisation, the PSP should take into account all the circumstances under which the PSU authorised a transaction. *Drafting suggestion:* *Article 55* *1.[…]* *2.[…]*

Question	MS reply
	3. For the purpose referred to in paragraph 1, the circumstances under which the payment service user authorised a transaction should be taken into due consideration by the payment service provider. The payment service user shall 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. Regarding Article 56 (6), in case option 2 would be chosen , we would agree with the drafting suggestion. But we understand that this will not be implemented in case of option 1 to be chosen. Regarding article 60 (1), we agree with the drafting suggestion. However, we still have a concern regarding this provision. In our practice, we notice some uncertainty regarding the interplay between the second subparagraph and the third subparagraph of paragraph 1. The second subparagraph states that the payer shall not bear the financial losses relating to an unauthorised payment transaction where the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently. In this subparagraph, there is no mention of gross negligence. The third subparagraph states that the payer shall bear all of the losses if these losses were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 52 with intent or gross negligence. In our understanding, the third subparagraph only applies to the first subparagraph of this provision and has any impact on the second subparagraph. In this

Question	MS reply
	sense, gross negligence cannot be taken into account where the loss, theft or misappropriation of the payment instrument was not detectable. An opposite interpretation would render the second subparagraph meaningless. It should not be possible to consider that the PSU acted with gross negligence by not immediately notifying PSP of any incident if the PSU could not detect the incident. Can the Commission confirm this interpretation? Depending on the answers to this question, we should consider to clarify Article 60 (1) PSR. *Drafting suggestion:* *Article 60* *1. By way of derogation from Article 56, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.* *The first subparagraph shall not apply where any of the following occurred:* *(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or* *(b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.* *By way of derogation from first subparagraph, tThe payer shall bear all of the losses relating to any unauthorised payment transactions if those losses were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in*

Question	MS reply
	Article 52 with intent or gross negligence. In such cases, the maximum amount referred to in the first subparagraph shall not apply. *[…]* BG (MS reply): We agree with the proposed approach and with the drafting suggestions of the Presidency. CY (MS reply): We have no comments. CZ (MS reply): Article 55(3) – we agree. Article 56(6) – we do not agree with Option 2 at all. Article 60(1) - we support adding ADR bodies and courts. However, we do not support competent authorities and PSPs included in the original proposal. NCAs are mostly not allowed to settle private disputes, therefore they are not entitled to reduce liability. If the PSPs will be allowed do so, PSU will be that forced to take an action at court/ADR body. DE (MS reply): Regarding Art. 55(3): GER generally supports Art. 55(3). We would however suggest to include that the PSU should provide the information “without undue delay”.

Question	MS reply
	Regarding Art. 60 (1): In our view, it is systematically wrong to designate ADR entities in Article 60(1) of the PSR. ADR entities are required to reach decisions that are based on the prevailing legal framework. ADR solutions are based on the factual situation as it has arisen in the procedure, should be aligned with the applicable law and in particular respect mandatory consumer protection laws. It is therefore misleading if, in the context of liability rules, as it is now expressly provided that ADR entities may accept a limitation of liability under certain conditions. If the applicable substantive law provides for such a possibility of limitation, the ADR entity should base its solution on it anyway. The same applies for national competent authorities. It is suggested that the MS be granted the authority to establish exceptions in such circumstances, with the matter to be subject to general regulation. DK (MS reply): We support all the changes, including the addition of dispute resolution bodies in article 60(1). We assume the amendments to article 56(6) will not be included here if we go with option 2. However, since the same wording is included in article 59(1) under option 1, we have commented on this wording there instead. EL (MS reply):

Question	MS reply
	El: we agree with the drafting suggestion in 55(3) and 56(6). We would like to indicate that in the proposed Art. 60 (1) PSR if the power to reduce liability would be given to PSPs it carries outs risks. It is the MS that should have the discretion to reduce liability, not competent authorities or PSPs ES (MS reply): We agree to Article 55 (3) that foresees the payment service user shall 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 available to him regarding the events leading to the disputed payment transaction. We also agree to Article 56 (6), indeed conditioning the right of full refund to the PSU to the evidence of reporting to the police seems proportionate. It is of the utmost importance for the police to be able to cooperate in preventing fraud, and investigate and chase fraud, to have all information related to fraud, coming from the victim. Finally, we agree to article 60 (1) which includes dispute resolution bodies: "*Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, national competent authorities, dispute resolution bodies or payment service providers may reduce the liability referred to in this paragraph, taking into*

Question	MS reply
	account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated" FI (MS reply): FI: Yes. HR (MS reply): We agree with the proposals for Article 55(3) and Article 60(1) PSR. We do not support option 2 so accordingly we do not support the proposal for Article 56(6). HU (MS reply): We agree. IE (MS reply): We agree that consumers should be obliged to report the fraud to the police as soon as the consumer becomes aware that he/she has been subject to fraud and the PSP should be allowed to request proof of such a report contingent on there being a legitimate basis under GDPR to request same. We welcome the insertion of 'dispute resolution bodies' as consumers should be encouraged to resolve disputes by way of ADR in the first instance.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	IT (MS reply): **IT.** On art. 55(3): We have no objections. We agree that the information the PSU can be expected to provide in compliance with the duty of cooperation depends on the circumstances of the case. We reiterate the need to consider introducing **clearer procedural rules** for PSPs when assessing PSUs' refund request. This would help avoid a protracted period of uncertainty between the parties, particularly given the additional complexity introduced by the proposed duty of cooperation, which entails a more structured interaction between the parties. See, as a possible starting point, our preliminary drafting proposal of art. 56 PSR in the "HU PCY drafting suggestions on art. 49-84" following the WP of last 26 November. On art. 56(6): We do not agree with such a hard-and-fast rule. We believe that the PSU's duty of cooperation is sufficient to address the concerns underlying the proposal. We do not consider it appropriate to introduce a specific rule for "social engineering": firstly, it is not an independent case of PSP liability and therefore should not be treated differently; secondly, as mentioned, the concept of social engineering is very vague. On Art. 60(1): we agree with the addition. But we are unsure about the reference to the PSP. The rationale behind the rules clearly suggests that the decision to reduce liability should be made by an independent third party.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	LT (MS reply): We agree with the proposed drafting suggestions (except 56(6) which is for option 2 only). We believe PSUs should have the obligation to always cooperate with PSPs in cases when they deny the fact of authorisation, however, it should not be an indispensable condition for the right to reimbursement in case where the provision of additional documents or information on the part of PSU would have influence on PSPS decision or in those cases where or up to the extend that a PSU cannot objectively provide certain information requested by its PSP. LV (MS reply): Article 55 (3) – We support the drafting proposal Article 56 (6) We strongly support the drafting proposal Article 60 (1) – We support the drafting proposal; it allows MS to choose the competent authority. NL (MS reply): We can agree with the drafting suggestions to articles 55(3) and 60(1). PT (MS reply): PT agrees with the revised Article 55(3) and does not see constraints in the mention to dispute resolution bodies incorporated in Article 60(1). RO

Question	MS reply
	(MS reply): We support the drafting suggestions to Articles 55(3), 56(6) (for Option 2 only), 60(1) PSR. However, we would like to add the following remark on Art. 55 (3): "However, the payment service provider should only initiate reasonable and proportionate requests, without overburdening the payment service user. It is the payment service provider's responsibility to ensure that the request has reached the payment service user. Finally, the refusal of the payment service user to respond to reasonable and proportionate information requests will be considered gross negligence on their side." SE (MS reply): We agree with the drafting in article 55(3) and welcome the inclusion of dispute resolution bodies in article 60(1). SI (MS reply): We agree. SK (MS reply): Regarding Article 55(3) we would be cautious using phrase "reasonably be expected to have" as it might differ considerably between countries and across demographic groups. It should not led to the misuse of the concept by the PSP to avoid liability. We agree with proposed drafting of 60(1).

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
Q7. Do Member States agree with the proposed approach and drafting suggestions to Article 55(2) PSR? If not, please provide an alternative wording.	AT (MS reply): Yes. BE (MS reply): BE: We strongly disagree with the inclusion of the word "necessarily" in this sentence. In our understanding, the mere fact that the payment transaction has been authenticated is not sufficient in itself. It could be one element of proof but it can never be the only element. The addition of the word "necessarily" could imply that it could still be possible for the PSP to assess the authorisation only on the authentication process and on any other circumstances. This wording could be dangerous as our initial objective was to prevent banks from automatically considering a transaction as authorised as soon as it has been authenticated. Such situation is currently strongly opposed by the Belgian Financial Ombudsman and consumer protection associations. BG (MS reply): We agree with the proposed approach and with the drafting suggestions of the Presidency. CY (MS reply):

Question	MS reply
	We see merit in the proposed approach, however we remain sceptical regarding the proposed drafting suggestion to Article 55(2). CZ (MS reply): We agree. DE (MS reply): As you know GER has in the past argued for a retention of the current PSD2 wording of Art. 55(1) which differentiates between authentication and authorisation. However, in the context of a balanced compromise, GER could agree to the proposed change of wording in Art. 55(1) that the PSP should prove that the transaction was authorised. Furthermore, we could also agree to the additions made in Art. 55(2) on authentication and SCA. However, it is of utmost importance for GER to keep the current wording of Art. 55(2) that authentication is **not necessarily** sufficient to prove authorisation. This will give leeway to courts to assess each individual case at hand and allow courts to handle situations where the PSU simply remains silent as to why he/she disputes the authorisation of a transaction. We therefore strongly support the POL PCY's proposal in Art. 55(2), in particular to reintroduce the word "necessarily". We believe that the reintroduction of the word "necessarily" as well as the introduction of duties to

Question	MS reply
	cooperate are a good compromise to mitigate the potential hardships stemming from the burden of proof rule. DK (MS reply): We agree. EL (MS reply): EL: We support the old wording of this paragraph, to clarify that the "authenticated by the payer" - which means application of SCA- should not automatically be considered as authorized transactions.The drafting suggestions under 55(2), where the exempted of SCA transactions are also included in this clarification, should be better explained in the article. We propose the following wording: "*2. Where a payment service user denies having authorised an executed payment transaction, ~~the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate~~, the fact that the payment transaction was authenticated, ~~including where applicable~~, via strong customer authentication, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided shall in itself not necessarily be sufficient to prove either 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. The payment service provider, including, where appropriate, the payment initiation service*

Question	MS reply
	provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user ***2a**. When a payment service user denies having executed a payment transaction, where an exemption of strong customer authentication is applied, and this transaction is accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided shall be subject to the provisions of article 60.2 and 60.3 respectively, except if the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52.* ES (MS reply): We prefer not to leave this open since we consider that this should be regulated as much as possible in level I text. As mentioned in previous comments, gross negligence is a key element for liability distribution, and this should be solved at level I and not leave it to national level. The proposal to introduce "**not necessarily**" allows for too much flexibility in this respect, therefore we are not supportive of the referred proposal. HR (MS reply): We agree with the proposed drafting suggestions to Article 55(2).

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	HU (MS reply): We agree. IE (MS reply): Article 55(2) – Agree. IT (MS reply): **IT.** On art. 55(2): We agree. LT (MS reply): We agree with the wording. LV (MS reply): We support the drafting proposal. PT (MS reply): PT welcomes the drafting of Article 55(2), as it foresees that the inclusion of SCA as an authentication method. RO (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	We strongly support the drafting suggestions of Article 55(2) and we find it important to incentives PSP for establishing efficient preventive tools in order to identify potential fraudulent transactions. SE (MS reply): We largely agree but think that the word "unnecessary" should be deleted. SI (MS reply): We agree. SK (MS reply): We agree.
Q8. Do Member States agree with the proposed approach and drafting suggestions to Recital 82 PSR? If not, please provide an alternative wording.	AT (MS reply): We are open to such an approach. However, it must be sufficiently clear that the distinction between gross or simple negligence is always up to the national courts evaluating the special circumstances of the individual case. BE (MS reply): BE: we can agree with the drafting suggestion made by the Presidency regarding the list of non-exhaustive and non-binding circumstances. However, regarding the

Question	MS reply
	examples, we are strongly opposed against adding examples that could imply situations that are in any case qualified as grossly negligent. The mention of such examples could imply that in practice such situation cannot longer be discussed on a case-by-case basis. This is the case with the example related to PSP's warnings. In this regard, we share the concerns expressed by the Commission during the meeting that some examples are linked to obligations that are already addressed in the provisions of PSR. It is the case for the example related to the notification of the loss of the payment instrument to the PSP, which is an obligation for the PSU under Article 52. The consequences of failure to comply with this obligation are already specified in articles related to the PSU's liability. Moreover, some examples are related to circumstances that still need a case-by-case assessment. This example, and the following example (on the elements dynamically linked and displayed during SCA) are in any case included in the list of circumstances that may be taken into account. This allows an evaluation on a case-by-case basis. We therefore suggest to delete these 3 examples cited above to avoid any inconsistency with the provision of PSR and to allow an evaluation on a case-by-case basis. BG (MS reply):

Question	MS reply
	We agree with the direction of travel undertaken by the Presidency in Recital 82 PSR. However, we would prefer to have a non-binding and a non-exhaustive list of circumstances only. CY (MS reply): We remain sceptical regarding the proposed drafting suggestions to Recital 82. CZ (MS reply): In general, we agree. But the legislative technique is quite uncommon, will the lawyer-linguists agree with the list in a recital? In any case, we would not support any definition or list in the binding operative text. DE (MS reply): GER could generally support the new drafting of Rec. 82 since the list is merely non-exhaustive and the discretion of the courts to assess each individual case at hand is highlighted. We do have some minor comments, however: - we would suggest to further specify the warning the PSP needs to issue. We would suggest to specify that "the warning should only be sufficiently clear, specific and concrete if it is on a case-by-case basis and individualized to the specific type of fraud. The payment service user should receive the warning in a timely and simple

Question	MS reply
	manner before the fraud occurs. In contrast, general warnings, which refer to complex fraud patterns or several cases of fraud, should not be adequate." - we would further clarify that to enable spying when entering access data at ATMs should not be sufficient by itself to justify gross negligence and that inexperience and unskillfulness of the payment service user may exclude gross negligence in individual cases. - in order to achieve a uniform wording, we would suggest to replace the word "bespoke" with "case-specific" in Rec. 82(g) - the sentence starting with "the specificity […]" should receive its own bullet point (h) DK (MS reply): We are of the firm belief that gross negligence should be a question for courts. However, we can agree to the proposed examples (although it is unclear to us what is meant by "sharing account credentials …without the right of disposal"). We also note that there seems to be suggested something reminding of a list in the main body of the text. There should probably only be one actual list to ensure clarity. We also agree with the Commission's concerns regarding the use of examples though we do not have specific comments for the drafting at this point.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	EL (MS reply): EL: We see merit in introducing a comprehensive and open-ended list of criteria or predefined case lists to provide guidance for all stakeholders, particularly national courts and dispute resolution mechanisms. We have been among the few Member States supporting a mandate for the EBA to develop Guidelines (GLs) for this purpose. The proposed changes in recital 82 is though a good start towards this direction. ES (MS reply): We welcome the approach taken by the presidency of providing both a list of examples and criteria to consider at national level when there is gross negligence. We believe this is a good compromise. We consider this matter of key importance and hence we have a strong preference for it to be at level I text, and not at EBA level. Also, we have some doubts on the non-binding nature of the criteria by national courts. We support having gross negligence in Level 1 text, in articles, and with a short open list of examples, including: 1) notifying the PSP that the consumer has been victim of a fraud in due time (before 48 hours, for example), 2) file a report at the police, 3) not having being victim of the same kind of fraud in a period of time (2/6 months), 4) not having considered and attended the specific warning of the PSP on the specific transaction that was identified as fraudulent. FI

Question	MS reply
	(MS reply): FI: In the spirit of compromise, we can agree on non-exhaustive and indicative criteria on the circumstances to be possibly taken into account when assessing gross negligence. However, a more cautious approach should be had with the examples as these would automatically constitute cases involving gross negligence. HR (MS reply): We agree with the proposed approach and with the introduction of an open-ended list of circumstances to be taken into account when assessing the gross negligence as proposed. HU (MS reply): We agree in principle with PRES's ambition to define only the circumstances to be taken into account in Recital 82 in a non-taxative way instead of defining the cases of gross negligence. The definition of specific cases/examples could also be useful, in our view, but it needs to be properly elaborated, which the Regulation does not do in substance. We also see a possible EBA mandate as justified. IE (MS reply): Given that national law and the assessment of negligence under national law may vary from country to country, we see benefit in introducing a comprehensive and open-ended list of guidelines in the recitals which should be closely aligned to the EBA Opinion on new types of

Question	MS reply
	payment fraud and possible mitigants. Such an approach would facilitate and promote uniform application across Member States. IT (MS reply): **IT.** On R82: We have no objections. LT (MS reply): In general, we agree with the proposal to introduce a comprehensive but non-exhaustive list of criteria to assess the possibility of gross negligence on PSU part, but some drafting amendments are needed. With reference to what some MSs have stated regarding 'gross negligence' being a civil law concept developed and interpreted by courts, it should also be taken into account that payment services is a highly specific area of regulation. It is not by chance probably that when it comes to payment services, 'gross negligence', before it is interpreted by courts, is and is on the main part done by PSPs which then become the initial and main interpreter of the content of this concept, especially since only a minority of disputes in this are reach the courts. A list of criteria would not only serve as a toolbox for PSPs, then ADR bodies, then, finally, courts, but also would serve as a sort of control mechanism against automatism on PSPs part while making decisions that deny reimbursement of losses. Lastly, the list of criteria is and should be only in-exhaustive, meaning other circumstances on an individual basis could be evaluated as well, and also PSPs would have the prerogative and responsibility to evaluate what criteria should be taken into account in an individual case in

Question	MS reply
	order to make a well-grounded decision that denies reimbursement. Regarding the recitals: on the one hand, providing examples brings more clarity, however, on the other hand, it should be noted as well that the existence of one or more of these circumstances noted in the example should not automatically end in the conclusion that the PSU in question was grossly negligent - more flexibility should be left to let individual circumstances of the case determine the outcome of the evaluation. This extra caution regarding examples is also necessary in order to avoid turning 'gross negligence' as a condition for making an exception from reimbursement rules into a requirement to behave attentively as a condition for reimbursement of unauthorised payment transactions. Therefore, if examples are provided, they should raise doubts about their suitability to illustrate 'gross negligence' under certain circumstances. LV (MS reply): We agree with the proposed approach and drafting suggestion. NL (MS reply): The recital now becomes somewhat confusing, as examples are listed both in the text (such as keeping credentials beside the payment instrument in an open format) and subsequently in a list at the end of the recital. We suggest to only use the list at the end, as we understand that the examples may not always constitute gross negligence

Question	MS reply
	(but are relevant factors to be taken into account). As for the factors themselves, we can agree to the following factors (our suggestions are in track changes): 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 purpose, one or more of the ~~following~~ below circumstances may be taken into account. The existence of one or

Question	MS reply
	more of these circumstances does not automatically lead to the conclusion that the payment service user has been grossly negligent. The payment service provider should motivate its decision based on the circumstances of the case.~~:~~ - (a) keeping the credentials used to authorise a payment transaction ~~beside~~ next to the payment instrument in a format that is open and easily detectable by third parties; - (b) sharing account credentials with ~~the~~ a third person ~~without~~ who does not have the right of disposal, i.e. is not eligible to use the payment instrument; - (c) 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;~~ Note: this can be deleted, as it was already mentioned in the list.~~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.~~ Note: this can be deleted, as it was already mentioned in the list. ~~(a) payment service user's behaviour or communication with third parties, where relevant;~~ (d~~a~~b) innovativeness, complexity of the fraud, and means or strategies used by third parties to illegally ~~take over~~obtain the payment service user's personalised security

Question	MS reply
	credentials o~~f~~r payment instruments owned by the payment service user. The innovativeness and complexity of the fraud may follow from the circumstance that the fraudster used a new type of modus operandi or complex technologies that are not commonly used by the general public or require technical skills; ~~(c) innovativeness, complexity of fraud;~~ (~~b~~d) whether the payment service user has previously fallen victim of the same type of fraud; (~~e~~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; (f~~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;~~ (g~~eg~~) 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; (f~~h~~h) ~~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

Question	MS reply
	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;~~ (~~g~~ij) whether the payment service provider~~s~~ offered clear, concrete and ~~case-specific~~ bespoke warnings ~~against currently used frauds methods that were brought directly~~ to the ~~attention of~~ ~~payer~~payment service user, 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 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~~provider, and whether those interventions offered a clear assessment of the probability that an intended payment was fraudulent. 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.

Question	MS reply
	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 *and modus operandi* 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 been victim of the same fraudulent modus operandi**.** PT (MS reply): Despite agreeing with the reintroduction of Recital 82, PT believes introducing 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. With this setting in mind, we reiterate our previous suggestion in this regard 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. RO (MS reply):

Question	MS reply
	We support the drafting suggestion to Recital 82. Additionally, we believe that letter (d) should be deleted as well since it is written in a way that allows PSPs to shift responsibility back on the PSU, based on gross negligence, whenever the PSU is manipulated into displaying their security credentials or whenever they are manipulated into installing malware/remote access tools that can expose security credentials. SE (MS reply): Firstly, we find the inclusion of both examples and circumstances rather confusing. As the two lists largely overlap, we suggest to **delete the examples** and stick with the more nuanced and generally held list of circumstances. The example stating that a PSU should report the loss of a payment instrument **immediately** after the loss is discovered is especially problematic. The concluding remarks, on PSU's that fall victim of bank employee impersonation multiple times, should also be deleted as this is already covered by point (b). Secondly, we propose to give some nuance to point (b), by adding the underlined: "whether the payment service user has previously fallen victim of the same type of fraud**, and under what circumstances**:" This is to take into account that criminals sell lists of fraud victims' personal details, to use their vulnerability and desperation to defraud them again. Previous victims of fraud are therefore much more likely to be exposed again.

Question	MS reply
	Thirdly, we would suggest to add further obligations of the PSP, apart from the obligations in point (c), including those in 51, 83(1a) and 83a, as all relevant obligations of the PSP should be taken into account, not just the information requirements in article 84. SI (MS reply): At the beginning, we were not in favor of including examples in the recitals, as, in our opinion, it is not necessary, considering that this is a matter of civil law, which is not harmonized at the EU level, and gross negligence is a legal standard defined by the courts. In the interest of reaching a compromise, we are willing to support it. However, when drafting Recital 82, we should be very careful about both the content and the wording. Regarding point (e) in Recital 82 "he 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": it suggests that, when assessing gross negligence, certain known characteristics of the PSU—such as the user's age, level of education, or profession—could be taken into account as factors. In Slovenian jurisprudence, the question of gross negligence is assessed not only based on the expected conduct of a normally diligent user but also that of a less diligent user. The standard applies to a

Question	MS reply
	"user" in general, not a "70-year-old user" or a "highly educated user." It is the concept of a “less diligent user” that matters. We should keep this in mind and avoid subcategorizing gross negligence based on PSU characteristics, especially not in the regulation. Therefore, we propose the deletion of point (e) of Recital 82. SK (MS reply): We can support introduction of an open-ended list of guidelines in the Recital.
Q9. Do Member States agree with the proposed drafting suggestions to Article 56(1) of the PSR? If not, please provide an alternative wording.	AT (MS reply): We do not see the need for any such amendment. BE (MS reply): BE: preliminary, we are in favour of considering measures aimed at protecting PSUs from inappropriate practices by PSPs. However, we need more explanation regarding the concrete proposal in order to have a strong position. We would welcome any further clarification in this respect and have a scrutiny reservation on this question. BG (MS reply): We believe that the phrasing of the Presidency’s drafting proposal in Article 56 PSR creates ambiguities with regard to the payment service provider’s ability to initiate claims from the

Question	MS reply
	same payment transaction against the payer. Consequently, we believe that the drafting proposal of the Presidency's should be removed. CY (MS reply): We do not support the proposed drafting suggestions to Article 56(1). CZ (MS reply): **We strongly disagree and cannot support this drafting.** The proposal essentially leads to the fact that 100% of PSUs who make a claim for compensation for an unauthorized payment transaction under Article 56(1) PSR will be compensated by the PSP. This also applies to cases where the PSU acted with gross negligence. The PSP then has the only option, which is to file a lawsuit with the court and recover the amount of the unauthorized transaction in court proceedings. We therefore consider this proposal to be completely contrary to the effort to maintain objective elements in the authorization of a payment transaction. PSUs will not be motivated in any way to be cautious when authorizing a payment transaction. The reason is precisely the fact that in 100% of cases, the PSU will be compensated by the provider after reporting an unauthorized payment transaction under Article 56 PSR. The result will be an enormous increase in litigation before courts. Under the current legal situation, the PSU has the right to initiate an out-of-court settlement (ADR procedure) of the dispute. However, this does not apply to the PSP.

Question	MS reply
	PSPs are supervised entities and cannot violate the requirements of Article 56 in completely obvious cases. DE (MS reply): While GER does agree with the approach presented in the discussion note that the PSP should not be entitled to set off any claims against the PSU stemming from the same payment transaction, the current wording of Art. 56(1) does not align with the text of the presidency note on page 5 and cannot be supported. The current wording reads that the PSP is not entitled to initiate claims against the PSU. This wording, however, will lead to the PSP not being able to initiate claims in court that the PSP might rightfully have. Such a provision would be in breach of Art. 47 of the Charta of Fundamental Rights of the European Union as it limits access to courts. The prohibition should merely include the setting-off of claims, not the right to

Question	MS reply
	initiate claims in court. The rationale behind the suggested prohibition to set off claims stemming from the same payment transaction is the following: If a PSU claims that a payment transaction has not been authorised and approaches his PSP in order to receive a refund, PSPs often claim that the PSU has acted negligently and that because of the PSU's negligence the fraudulent transaction was enabled in the first place. In the case of actual negligence on the part of the PSU, the PSP has indeed a counter-claim against the PSU under Art. 60. So, if the PSU claims that a transaction of (e.g.) 1.000 € has not been authorised, but has indeed acted negligently, the PSU has a claim for refund against his PSP amounting to 1.000 €, but the PSP, on the other side, also has a claim amounting to 1.000 € as a counter-claim under Art. 60. Under the current provisions of PSD2, the PSU can simply set off its claim against the claim of the PSU (= 1.000 € - 1.000 € = 0 €). While this is no problem when the PSU has indeed acted negligently and therefore the PSP's counterclaim of 1.000 € actually exists, it is a problem in cases where there has indeed been no negligence on the part of the PSU, but the PSP simply claims that the PSU has acted negligently and sets off its alleged counterclaim against the PSP's claim for refund nonetheless. This situation leads to the PSPs not refunding the PSUs and the PSUs being forced to assert their claims in court which is why the practice of setting-off of claims should be restricted in those cases. This, however, should not restrict the right of either the PSP or the PSU to initiate claims in court.

Question	MS reply
	Drafting suggestion: ***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. **The payment service provider shall not be entitled to set off any claims stemming from the same payment transaction against the payer under Article 60.** EL (MS reply): EL: Suggested amendment is not clear to us. HR (MS reply): We do not agree with the proposed drafting suggestions to Article 56(1). In our opinion, the proposal is too broad because it refers to "any claims" and might be in conflict with the civil law. HU (MS reply):

Question	MS reply
	We do not really see the meaning of this modification in Art. 56(1) and we would be thankful if the Presidency could elaborate on why they think it is important. IE (MS reply): We propose the following text - "Without prejudice to Article 54, in the case of an unauthorised payment transaction, after noting or being notified of the unauthorised 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, 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. The payment service provider shall not be entitled to initiate any claims stemming from the same payment transaction against the payer under Article 60". IT (MS reply): **IT.** On art. 56(1): We strongly disagree. Article 60 regulates certain cases where the PSU can be held liable for an unauthorized transaction (e.g., fraud or gross negligence). These are exceptions that the PSP can raise in defence against the PSU's reimbursement request (and, as a general rule, the PSP has no interest to raise such exceptions before the PSU's request). Therefore, the proposal is effectively equivalent to abolishing Article 60.

Question	MS reply
	It is true that there is a risk of abuse of Art. 60 by the PSP, particularly in the initial phase, when the PSP must decide on the PSU's reimbursement request. However, the risk of abuse stems not so much from the substantive rules of liability but from the fact that, at this initial stage, there is no independent third party involved. For this reason, it is crucial that independent, fast, and low-cost ADR schemes be available to the PSU. LT (MS reply): The drafting suggestion seems rather vague and it is not easy, even having the Pcy's explanation, to understand what the addition to article 56(1) actually refers to in article 60(1). The straight forward conclusion that could be drawn is that PSPs on their own could not refuse reimbursing PSUs if the payment transaction is deemed as unauthorised. We presume that probably the goal of the proposal is not to give an unlimited right to PSUs to get reimbursed for unauthorised payment transactions (that might cause unwanted outcomes - more fraudulent transactions could be deemed as authorised to avoid litigation), nor it should unreasonably burden PSPs' right to refuse reimbursement if fraud or gross negligence is detected. In order to avoid automatism on PSPs part, we believe, the goal should be to oblige PSPs to make well-grounded decisions in case reimbursement for fraudulent, especially unauthorised, payment transaction is rejected on the grounds of gross negligence on PSU's part. As an alternative, we propose this drafting suggestion: 'The decision of the PSP to refuse to compensate the PSU for losses resulting from a disputed payment transaction in the case of

Question	MS reply
	fraud – whether the PSP determines that such a payment transaction has been authorised or whether it refuses to compensate the PSP for losses resulting from a payment transaction that has not been authorised by the PSP after assessing the PSU's behaviour as grossly negligent – shall be evidence-based and well-reasoned, and be taken after having examined the totality of all the circumstances of the case in question." LV (MS reply): We do not see the need and added value for the proposed drafting suggestion. NL (MS reply): We can agree. PT (MS reply): PT would like so seek clarification on how this will interplay with the drafting of Article 60, on transactions below the 50€ limit. In result of this new prohibition, will PSP need to reimburse the PSU of such transactions even if fraud is suspected to have been committed by the payer. Please consider the following amendment: *"(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*

Question	MS reply
	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. The payment service provider shall not be entitled to initiate any claims stemming from the same payment transaction against the payer under Article 60 but is entitled to recollect the refunded proceeds from the payer if confirmed that fraud was committed by the payer." RO (MS reply): We support the drafting suggestions of Article 56(1). SE (MS reply): We see some merit in the principle, but find it difficult to interpret the current drafting. SI (MS reply): We agree.
Q10. Do Member States agree with the proposed drafting suggestions to Recital 81a and Article 108(1b) PSR? If not, please provide an alternative wording.	AT (MS reply): We still favor a more active role of ECSPs in fraud prevention. For example, experiences in different MS have shown that the obligation for ECSPs to block

Question	MS reply
	fraudulently used, suspicious phone numbers used for smishing has yielded very positive results, leading to a dramatic decrease in corresponding fraud rates. We think that similar approaches should be considered in the PSR framework. BE (MS reply): BE: we are not opposed to a review clause but we believe that further strict rules on the cooperation of ECSPs should be introduced in PSR. We may support suggestions for leveraging existing EU rules such as the DSA but we do not see such initiative as an obstacle for stricter rules on the collaboration between ECSPs and PSPS in PSR. In case of fraudulent payment transaction, we believe that the cooperation between all the parties involved is essential. In some types of fraud, it should be useful to have a communication between the PSP and the ECSPs in order to share all the relevant information on the context of the fraud, to block the fraudulent message that leads to the transaction and to investigate on the modus operandi of the fraudster. PSR should also provide for a possibility to set national sanctions. In this sense, we support the proposal made by the Irish delegation in its non-paper regarding the dedicated communication channel and the collaboration of the ECSPs under Article 59 PSR. Regarding the regime stated in Article 59, we believe that the scope is very limited. In our understanding, the collaboration of ECSPs could be useful in other types of impersonation frauds.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	BG (MS reply): We agree with the proposed drafting suggestions of the Presidency. CY (MS reply): We do not support the drafting suggestion for Recital 81a and we do not object to the proposal of Article 108(1b) regarding the introduction of the review clause. CZ (MS reply): Regarding Article 59(5) while we could support cooperation between ECSPs and PSP, we again call for explanation how the obligation to cooperate in Article 59(5) PSR differs from the obligations under the DSA. We see no reason why the same obligation should exist under the PSR. Also, any potential obligations must be technically feasible. Regarding the review clause and Recital 81a, we can agree with that. One issue that remains unresolved is the definition of ECSPs. We note that, to the best of our knowledge, Recital 80 of the PSR remains unchanged. This recital still states that ECSPs include all internet platforms, even the small ones: "through adequate prevention and robust technical safeguards developed with electronic communications services providers such as mobile network operators, internet platforms, etc." It is also unclear which communications services fall within the scope of the definition. In addition to electronic communications services, these could include, for example, associated services, emergency services and other smaller services, which often do not have the same financial, human and technical resources as their larger counterparts. On this basis, we call for clarification and narrowing of the definition and amendment of Recital 80.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	We propose this definition for purpose of PSR: *Article 3 (58) PSR: 'electronic communications service enabler means any of the following service providers:* *i) provider which provides the services falling under the scope of Article 2(4), point (b) of Directive (EU) 2018/1972 (European Electronic Communications Code).* *ii) ´very large online platform´ or ´very large online search engine´ within the meaning of Article 33(4) of Regulation (EU) 2022/2065 (Digital Services Act).* We also call for a division of responsibilities between ECSPs and online platforms. These two types of businesses are completely different, as are their roles in the fight against payment fraud. It does simply not make sense to have the same obligation for them. DE (MS reply): We have understood from the last working party that the PCY in joint work with the COM will test potential ways of how to leverage existing sectorial legislation on ECSP more in order to accentuate the role of ECSP and platforms in the prevention of

Question	MS reply
	payment fraud. We do think that the results of such work should be carefully discussed in the working party. Besides, GER is generally open to establish a review clause regarding the duties of ECSPs, which could also be combined with concrete rules for ECSPs in the PSR as proposed in the IE non-paper or currently worked on by PCY and COM. We would also be open to include other areas for review, for instance, the newly introduced specific liability regimes (IBAN name check, bank impersonation fraud). We only wonder whether the time frame of 2 years is too short, however. We think it might lead to a more effective review to lengthen the period. DK (MS reply): Regarding the obligation to collaborate between ECSPs and PSPs we can support the Presidency's proposed drafting suggestions to Recital 81a and Article 108(1b). We find that it is a sensible solution to introduce a review clause, which requires a report on the impact of the collaboration between ECSPs and PSPs and if appropriate present a legislative proposal on this basis. This approach ensures a proper impact assessment before introducing requirements on ECPS with potentially unintended and far-reaching consequences. The wording could

Question	MS reply
	be adjusted to indicate that it would be relevant for the Commission to look into the role of telcos and digital platforms both before, during, and after fraud has taken place. Nevertheless, we can also support introducing requirements for online platforms in the current negotiations. This could for instance be measures to ensure more efficient removal of fraudulent content from online platforms. It could prove efficient to allow PSPs to become trusted flaggers under the DSA, in order to make digital platforms prioritise notices from PSPs. EL (MS reply): EL: We agree with the introduction of a review clause for an impact assessment done by the Commission for the collaboration of the ECSP and the PSPs, however we regard this as not enough. We consider the inclusion of Electronic Communication Service Providers (ECSPs) at this point as crucial in the fight against fraud. It is preferable to establish a framework with targeted preventive measures also from the part of ECSPs for fraud types such as spoofing, SIM-swapping, or phishing sites - especially those presented as sponsored results in search engines. For the last point of search engines, we also agree with the IE non paper and the need to establish in PSR a link with the requirements of the DSA (art. 34), for the Very Large online search

Question	MS reply
	engines (VLOSE) to validate the authenticity of institutions that require an advertisement as well as perform risk assessment for the dissemination of illegal content through their services. ES (MS reply): We strongly recommend being more ambitious as regards the involvement of Telcos in the fight against fraud. We consider the review clause proposed by the presidency is not sufficient. Liability should stem from all actors at the same point in time, with the occasion of the entry into force of PSR. Although there already exists sectorial regulation for telcos, most of it is at the level of minimum harmonised Directives, and hence, not EU harmonised, and regarding the Digital services Act, although it is a directly applicable Regulation, it focusses on mitigation measures, and not on liability, the result being banks and telcos are not symmetrically involved in terms of prevention and liability. We propose to include them already now under the scope of PSR, both in terms of a strong and clear cooperation duty, as well as in terms of liability, and to include a review clause to assess the potential need to any amendments. Should the presidency consider not to go so far in level I text, a second option, would be, as already flagged in ES previous written comments, to declare the obligations of all actors in the payment chain under the PSR, so that they arise at the same time, with

Question	MS reply
	a specific mandate to Member States to develop such provisions under the specific sectorial regulation and amend if needed the national telecommunication regime. - For instance, in Spain, national legislation is currently being updated in order to allow ECS the possibility to block calls and/ or SMS where fraudulent elements are identified). (you can consult it in this link). Furthermore, we would like to highlight the fact that **article 9 of the ePrivacy Directive (not included in the mapping exercise of EU regulation)** prevents the use of location data to fight against fraud, which might be key to blocking certain fraudulent communications. ***Therefore, it needs to be considered if measures implemented in order to prevent fraud shall not be considered in breach of articles 5, 6 and 9 of Directive 2002/58/EC.*** **Following the above referred please see below our drafting suggestion for article 59a, for your consideration** • 5. Where informed by a payment service provider of the occurrence of the type of fraud as referred to in paragraph 1, electronic communications services providers shall cooperate closely **diligently** with payment service providers **to the extent that it is technically and legally possible for providers of electronic communication services while safeguarding** and act swiftly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance

Question	MS reply
	with Directive 2002/58/EC, including with regard to calling line identification and electronic mail address. • 5.a. In order to ensure effective cooperation against fraud between electronic communications services providers and payment services providers, the measures implemented, which must be proportionate to the objective pursued, **shall not be considered in breach of articles 5, 6 and 9 of Directive 2002/58/EC.** Where providers of ECS have deployed technical measures required by national authorities for combatting fraud, the requirement to cooperate diligently with payment service providers shall be considered achieved. Finally, we would like to highlight that cooperation between ECS and PSP should not be limited to cases of bank impersonation fraud, and a similar obligation should, in our view, be included under article 56. FI (MS reply): FI: Yes. HR (MS reply):

Question	MS reply
	We can agree with the proposal for a review clause, but something should already be done in the PSR to strengthen the role of ECSPs. In our opinion, the proposal in the IE non-paper is a good way forward. HU (MS reply): We believe that more ambitious steps are needed than the review clause, and that the ideas of the Irish delegation in their non-paper could be a useful basis for meaningful progress. IE (MS reply): Recital (81a) & Article 108(1b) – we can support the insertion of a review clause specifically on Article 59 measures which apply to electronic communication service providers. However, such a review clause should not be inserted in place of more ambitious anti-fraud measures related to ECSPs, such as fraud verification as proposed in our non-paper. IT (MS reply): **IT.** We agree with these drafting suggestions. Since the duty of cooperation between PSPs and ECSPs represents a new element in the regulation, it would be appropriate to ask for a report on the impact of the provisions contained in Article 59. LT (MS reply):

Question	MS reply
	We agree with the wording. LV (MS reply): Recital 81a – in general we support is important to strengthen the role of electronic communication service providers in the transaction chain. Regarding the review clause we could agree, but it is not clear whether it would be sufficient to reduce fraudulent transactions. NL (MS reply): As indicated during the working party we support the inclusion of the review clause, but do want to explore whether additional obligations for ECSPs are possible given the important role these parties play in tackling payment fraud. PT (MS reply): Despite supporting the inclusion of the review clause under Article 108(1b), and the draft of Recital 81a, PT would seek further clarifications to be introduced in Article 59(5) regarding the means on how the collaboration between PSP and ECSP should be based, what is expected, and even previewing possible noncompliance measures. In our view, progress in this regard can be achieved by including the proposals of the colleagues from IE, contingent on the assessment being carried in collaboration with the COM, whose availability to work in the Council in this regard was manifested in

Question	MS reply
	the CWP, to address challenges surrounding interplay between sectoral legislation, proper enforcement of imposed obligations, and reliance on its supervision by the respective competent authority. RO (MS reply): We strongly support drafting suggestions to Recital 81a and Article 108(1b) PSR. SE (MS reply): We think that the proposal from the Irish delegation should be considered as well, alongside the suggestions made by DG CONNECT. SI (MS reply): We agree. SK (MS reply): We support the review clause.
Presidency Discussion Note **Interplay between PSD3/PSR and MiCA and treatment of payment transactions with EMTs under PSD3/PSR**	

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
WK 2067/25	
Q1. Do Member States agree with the Presidency's assessment and proposals on recital 16 PSD3 and on recital 29 PSR?	**ECB**: On recital 16 PSD: In our view custody and administration of crypto-asset on behalf of clients where it relates to E-money tokens should be covered as payment services. Otherwise, there is an important gap in the security of the payment chain. AT (MS reply): Yes. BE (MS reply): BE: We would prefer a thorough analysis of the crypto-asset services that can legally be qualified as payment services. For dual qualified "crypto-asset service" and "payment service", it should be determined which provisions of PSD3/PSR and MICAR legally apply. Based on this analysis a policy decision can be made as to what requirements CASPs and/or PIs can be exempted from. We think that the Commission is best placed to conduct this mapping exercise. BG (MS reply): We agree with the Presidency's assessment and proposals on recital 16 PSD3 and on recital 29 PSR.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	CY (MS reply): We have no comments regarding the proposed drafting suggestions to recital 16 PSD3 and on recital 29 PSR. CZ (MS reply): In general, we can agree. Unfortunately, the lack of legal clarity regarding the transfer of EMTs remains an issue. We understand that PSD3/PSR cannot cover all possible business cases, but it should be clearly stated which regulation prevails if the transfer can be qualified as a payment service. Additionally, we still lack guidance on how to stipulate that a transfer is a transfer of crypto-assets versus a payment service which is of the utmost importance at this stage. We should also consider what the nature of e-money services is. In Recital 16 PSD3 + Recital 29 PSR second sentence – "unless otherwise stated" – it should be also added "in this Directive/Regulation or Regulation (EU) 2023/1114". **We have a general comment regarding MiCA. It should be clearly stated in one of the recitals that the redemption of e-money/EMTs by their issuer is not a crypto service 'exchange of crypto-assets for funds'. In this case, it is not a crypto service, but an activity that the issuer of e-money/EMTs is obliged to provide to the holder.**

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	DE (MS reply): Our comments to this PCY Note are still subject to a scrutiny reservation, as we are still in the process of analysing the proposals. We support the direction of travel of the PCY note to clarify the scope of the interplay between MiCAR and PSD 3 / PSR. In particular, we agree with the approach to keep in the scope of PSD3/PSR payment transactions with EMTs in certain constellations. However, in our assessment EMTs cannot to be understood as a subset of e-money in the scope of PSD3 / PSR. In particular, according to Article 3 para. 1 no. 7 MiCAR, the qualification of a crypto asset as an EMT does not require third-party acceptance, which by the definition of Art. 2 para. 32 PSD 3, however, is a prerequisite for the qualification of a means of payment as e-money. The importance of the feature of third-party acceptance for the qualification as e-money was just recently the subject of an EBA Q&A (https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2022_6336). Hence, the drafting of Rec. 15, 16 PSD3, Art. 2(23) PSD3 and Rec. 28, 29 PSR, Art. 3(30) PSR that would qualify all EMTs – regardless of their design – as e-money in our view would essentially give up on the current necessity of having a third-party acceptance in order to qualify as e money. Further, following our aforementioned arguments, the changes proposed regarding the definition of "funds" would not constitute a mere clarification, but would lead to an extension of the funds concept. We should be very careful about such extension and hence, we disagree with the drafting of Rec. 15, 16 PSD3, Art. 2(23) PSD3 and Rec. 28, 29 PSR, Art. 3(30) PSR

Question	MS reply
	that would qualify all EMTs – regardless of their design – as e-money and hence, include them in the "funds" concept. Besides, we support the PCY's approach to clarify the specific categories of EMT services that shall be considered as payment services. In this regard, we particularly support that "custody and administration of crypto-assets on behalf of clients" alone does not constitute a payment service. However, the current wording could still include custodial wallets that are used only in the context of trading of crypto assets. Including such constellations would significantly widen the scope of application and would go against the intuition of the proposed recital 29a PSR. Hence, we would argue for a change of wording here in order to make sure to exclude those constellations from the scope. DK (MS reply): We agree that payment services carried out with EMTs should be covered by the PSR and PSD3 to ensure a level playing field. However, we want to underline that the importance of not tipping the balance in a way that creates disproportionate burdens for CASPs offering services with EMTs nor too complex regulation with unintended consequences. Further scrutiny is necessary. For example, it's crucial to make sure that CASPs are not subject to double regulation for the same activity under MiCA and the delegated acts, and PSR/PSD3.

Question	MS reply
	Furthermore, in light of the intention of MiCA to supplement existing regulatory frameworks, an initial question is for example whether it is adequate to equate transfers of EMT to the payment service defined in PSR/PSD3? Was a double license initially not meant to cover situations where CASPs also offered payment services, as for example both offered exchange services and execution of payment transactions with EMT? No matter the approach, more specific work on clarifying what constitutes the variety of payment services in a DLT-infrastructure as well as how to ensure that specific requirements are operational and not disproportionate is necessary. EL (MS reply): We agree. ES (MS reply): As a general comment, **we would have preferred to modify MICA, to avoid cross references to a repealed e-money Directive.** However, we are not opposed to the way of travel of compromise of the presidency. HR

Question	MS reply
	(MS reply): We have a different approach as regards the transfer of EMTs since we consider it a crypto-asset service that should be provided under the MiCAR. The issue of interplay between MiCAR and PSD3/PSR and the treatment of transfer of EMTs is of key importance in terms of the burden that will be imposed on CASPs due to the application of two regimes to the same activity. This issue is even more burdensome in Member States where separate national authorities are competent for PSD and MiCAR, in relation to the authorisation process as well as for the supervision of the entities with dual licences. However, in case that the proposal will continue to develop in the proposed direction, we would support any proposal that minimizes the burden for CASPs and competent authorities. Given that there is a possibility in Article 60 MiCAR that some financial entities (including EMIs) can provide specific crypto-asset services by way of notification to the competent authority, without seeking an authorisation as a CASP, we propose to consider the introduction of a similar possibility in PSD3 for CASPs providing the transfer of EMTs. This would enable CASPs to provide certain payment services associated to the transfer of EMTs without PSD3 licence, upon notification to the competent authority and under the conditions that would be regulated in PSD3/PSR. Such an approach would level the playing field for entities providing the same activities. HU (MS reply): We believe that the way of travel regarding MiCA and the treatment of EMTs is going in the right direction. The content of the drafting proposals is still under discussion with

Question	MS reply
	our NCA as regards the adequacy of the content. If we identify any problems with the text, we will report it to you. IE (MS reply): Recital (16) PSD3 – Agree, Recital (29) PSR – Agree. IT (MS reply): **IT.** As a general comment, it is crucial that MiCAR services that are to be considered as payment services are clearly identified. Having said that, in principle we agree with the proposed approach. However, we would like to seek some clarification on the treatment of custodial wallets enabling the transfers of EMTs to and from third parties. The Presidency refers the identification as a payment service under PSD3 only of transfer services for crypto-assets in relation to EMTs, thus including, as stated in the recitals, the case of CASPs offering custodial wallets enabling transfers on behalf of its clients. Therefore, as the Presidency is proposing to refer the identification as payment services under PSD3 only to transfer services with EMTs, the words "in particular" should be removed from recitals 16 and 29, as no other services would be identified as payment services. In light of the above, the service of custody and administration of EMTs would not be considered a payment service per se, but the identification as a payment service would apply to the additional service of enabling transfers to and from custodial wallets. Is our understanding correct? This interpretation would be consistent with ESMA Q&A 2071/2024, which states that transfer services, when offered along with other crypto-asset services (including custody and

Question	MS reply
	administration), are self-standing services subject to authorisation under Article 59 of MiCAR. In line with this reasoning, we suggest the following amendments in recital 16 PSD3, in green. Please note that the word "in particular" should be removed also from recital 29 PSR. ***Recital 16 PSD3*** […] ***This concerns ~~in particular~~ transfers by crypto-asset service providers, on behalf of their clients, of electronic money tokens corresponding to transfer services for crypto-assets on behalf of clients under Regulation 2023/1114.*** […] ***By contrast, the service of custody and administration of crypto-assets on behalf of clients or the service of placing of crypto-assets, as defined Regulation (EU) 2023/1114, do not constitute by themselves a payment service. This is without prejudice to the qualification of the provision of transfer services of electronic money tokens in connection with custodial wallets as the payment service "execution of payment transactions".*** […] LT (MS reply): In general, we accept the proposed direction as regards PSD3 and MiCA interplay. LV (MS reply): We could agree with the Presidency's proposal. NL (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	We are overall positive on the proposal but we do have some remarks. Our first remark relates to the proposal to keep transactions with EMTs when used to pay for goods and services in the scope. We wonder what this mean for EMTs kept in non-custodial wallets used for payment transactions.. Do those fall within the scope? Our second and also last remark relates to the level 1 text and the 10 types of crypto services. We understand that level 1 text might not be the must suitable place for such detail, but further harmonised guidance is relevant and important. Is there a possibility for another kind of guidance, for example RTS or Guideline? PT (MS reply): PT agrees with the proposals on Recital 16 of PSD3 and on Recital of 29 PSR, favouring the alignment with Recital 90 of MiCA. Nonetheless, while PT welcomes the clarification that the services of *"custody and administration of crypto-assets on behalf of clients"* and *"placing of crypto-assets"* do not, by themselves, constitute a payment service, we question if this reference provides sufficient legal certainty/clarity as it appears to lack criteria for determining when such services do constitute a payment service, or where such criteria can be found. As a general comment, surrounding any final amendments to be introduced in PSR/PSD3 regarding interplay with MiCA and treatment of payment transactions with

Question	MS reply
	EMTs, PT believes those should take in consideration the contents of EBA's *"No-Action Letter on the interplay between PSD2 and MICAR in respect of CASPs transacting EMTs"*, which shall soon be published. RO (MS reply): We continue to consider problematic a double authorization requirement of the same activity. In our opinion, providing services with all crypto assets (including EMTs) should remain exclusively on MiCA in order to ensure a "level playing field" principle among all European legislation. Otherwise, how could we explain the difference in treatment compared to MIFID II, where the financial intermediation activity carried out does not require authorization under PSD2? Furthermore, having in mind the proposal to apply PSD3 and PSR to payment transactions with EMTs where EMTs are used as a mean of payment, but to exempt them from the safeguarding requirements in PSD3 (considering that they benefit from the protection offered by MiCAR), in this situation, we are of the opinion that we would apply the PSD regime without one of its basic requirements, thus, ending up applying a formal regime without substance. This would imply the PSD amendment would be, rather, a bureaucratic approach with no added value. In addition, the differences between the two safeguarding regimes should be observed, from a prudential perspective. SI (MS reply):

Question	MS reply
	We are of the opinion that (i) providing transfer services for crypto-assets on behalf of clients, (ii) providing custody and administration of crypto-assets on behalf of clients" and additionally (iii) exchanges of EMTs for funds or crypto-assets - where the CASP acts as an intermediary between the seller and the buyer, and handles the payment in funds from the buyer to the seller- could also qualify as a payment service. SK (MS reply): We support MSs which call for the systemic approach. It is necessary to map the activities clearly before drafting the exemptions.
Q2. Do Member States agree with the Presidency proposals as regards the exclusions in Art. 2(2) PSR, related recitals and the following editorial changes to Article 1(3) PSD3?	**ECB**: On self-hosted wallets, as due to the proposed exclusion the payment service user (PSU) would not be protected, the payer's PSP should be required to inform the payer about the risk and obtain the payer 's explicit consent that to transfer to an unhosted wallet prior to executing the transactions. We disagree to the proposed exclusion in recital 29 a of EMTs where they are used for investment or trading purpose. EMTs are token established for redemption 1:1 at par value and granting interest is prohibited. Thus, they are not designed for investment or trading purposes other than to settle related transactions. Moreover, the definition of "payment transaction" is agnostic to any underlying obligations between the payer and the payee. We should keep this important principle and treat all EMT transactions conducted on behalf of clients equally irrespective of the clients underlying motivation. On Article 2(2) we see an obligation for the issuer to take a decision whether or not to allow self-hosted addresses and to warn payment service users prior to the transfer to such addresses.

Question	MS reply
	On h1, we see no reason why to deprive payment service users for from their rights when exchanging EMT for funds or vice-versa. These are comparable to services to place or withdraw cash from an account which requires a license. Who would take to responsibility for fraud in these cases? On l1, we are fine to exclude payment transactions of CASPs or their branches for their own account. AT (MS reply): Yes. BE (MS reply): BE: we support the changes BG (MS reply): We agree with the Presidency's proposals as regards the exclusions in Article 2(2) PSR, related recitals and the following editorial changes to Article 1(3) PSD3. CY (MS reply): We have no comments for the exclusions in Art. 2(2) PSR. CZ

Question	MS reply
	(MS reply): We can agree with the proposal. However, we would not delete the exemption in points (g) and (h) as the proposal from December was reasonable from our perspective. One of the impacts of MiCA is the alignment of the approach to investment instruments and crypto-assets. Although 'securities' may not always equate to 'investment instruments,' we believe that in the case of certain exceptions, this will generally be the case. DE (MS reply): Recital 29a PSR We support the direction of travel here. However, we should try to align those exclusion as much as possible with the exclusions regarding transfers in the scope of MiFiD. Recital 29b PSR In our view, the decisive distinction here is the existence of a power of disposition of a third party involved. In decentralised blockchains transfers between self-hosted wallets would not qualify as payment services given that there is no power of disposition of a third party, however, the situation might already be different for blockchains with a central provider. Ad 2(2)(a1) PSR In our view, the decisive distinction here is the existence of a power of disposition of a third party involved. In decentralised blockchains transfers between self-hosted

Question	MS reply
	wallets would not qualify as payment services given that there is no power of disposition of a third party, however, the situation might already be different for blockchains with a central provider. Ad 2(2)(h1) PSR We could support this exclusion. However, it is noted that EBA proposes that "*exchanges of EMTs for funds or crypto-assets, where the CASP acts as an intermediary between the seller and the buyer, and handles the payment in funds from the buyer to the seller, qualify as a payment service regulated under PSD2 unless an exemption under Article 3 PSD2 applies to those payment transactions*". Ad 1(3) PSD3 We could support the text proposed under what is considered as Art. 1(3) PSD 3 in the PCY note. However, we were under the impression that Art. 1(3) PSD 3 would still read "Unless specified otherwise, any reference to payment services shall be understood in this Directive as meaning payment and electronic money services." DK (MS reply): We agree with the amendments, and we believe that it's necessary to further define in the recitals which transactions involving EMTs should be covered, and which should not, as it's no secret that both the actors involved and the way these activities are carried out are significantly different from what we know from the traditional payment infrastructure

Question	MS reply
	EL (MS reply): We agree. ES (MS reply): We welcome the provisions aiming at streamlining the authorisation process. We also support the proposed wording on recital 6 of PSD3, which addresses our previous concern regarding the reference to Directive 2009/110/EC (the EMD) since it is being repealed and, over time, any references to it could be difficult to trace back and understand. We would like to suggest the following amendments to the new recital 29a of PSR: "*Given the market evolution since the adoption of Directive (EU) 2015/2366, and in order to avoid disproportionate requirements for crypto-asset service providers that provide services with electronic money tokens in accordance with Regulation (EU) 2023/1114, and also to ensure legal clarity as regards the scope of application of this Regulation and Directive xx [PSD3] to services with electronic money tokens, it is appropriate to exclude from the scope of application of this Regulation and Directive xx [PSD3] certain types of payment transactions with electronic money tokens ~~where~~*

Question	MS reply
	~~*electronic money tokens are used for investment or trading purposes.*~~ *This concerns in particular the exchange by crypto-asset service providers of electronic money tokens for funds or crypto-assets, including where* ~~*regardless of whether*~~ *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.*~~ *This exclusion should cover in particular exchanges of electronic money tokens as part of the provision of the service of exchanging crypto-assets for funds, exchanging crypto-assets for other crypto-assets, operating a trading platform for crypto-assets, receiving and transmitting orders for crypto-assets on behalf of clients or executing orders for crypto-assets on behalf of clients, as defined in Regulation (EU) 2023/1114. However, the exclusion should not include transfer services where electronic money tokens are used to pay for goods or services, for peer-to-peer payment transactions or payment transactions between payment accounts held by the same person*". The first amendment is justified by the difficulties to understand which situations an EMT would be used for investment or trading purposes. MiCA does not make any difference on the "uses" of EMT. The second amendment is justified by the fact that the exchange of EMT for funds or other EMT is a service that CASPs provide in their own name with their own capital, in accordance with MiCA. Therefore, we consider that the paragraph would be unnecessary and should be removed, as it is included in the expression "*This concerns*

Question	MS reply
	in particular the Exchange by crypto-asset service providers of electronic money tokens for funds or crypto-assets." FI (MS reply): FI: In general, the drafting regarding the interplay between PSD3/PSR and MiCA has gone into right direction and we generally happy with it. However, we would have one remark from drafting and clarification point of views for your consideration. Namely, it could be considered to clarify in the recitals whether PSR recital 29a and Article 2(2)(h1) are only intended to cover transactions where an EMT is the actual object of the trade or exchange (i.e. an EMT is bought or sold or exchanged); or whether the recital and Article are also meant to cover transactions where EMTs are otherwise used to complete a transaction involving crypto-assets (i.e. pay for the transaction) but where an EMT is not the object of the trade or exchange. We believe that the exclusion should only cover cases where an EMT is the object of the trade or exchange. We would further note that the use of "funds", as defined in the PSR/PSD3 regime, by crypto-asset service providers is not restricted to EMTs. All of the services mentioned in PSR recital 29a could also be provided with, for example, scriptural money. Thus, the need for clarity over what type of activity involving funds (cash, scriptural money, regular e-money and EMTs) amounts to payment services or payment transactions goes beyond EMTs.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	HR (MS reply): As already stated in our reply to Q1, we have different approach as regards the transfer of EMTs. However, in case that the proposal will continue to develop in the proposed direction, we would agree with the proposed exemptions and with clarification that payment transactions where EMTs are used for investment or trading purposes are excluded from the scope of application of PSD3/PSR. IE (MS reply): Article 2(2) PSR – Agree, Article 1(3) PSD3 – Agree. IT (MS reply): **IT.** We agree with the proposed wording of letters a1), g), l) and l1) of Article 2(2) PSR. For letter h): what would be the treatment of payment transactions where EMTs are used to pay for the distribution of rewards and other forms of income related to other crypto-asset services and activities (e.g. staking, yield farming)? Given the return to the original wording of the Commission's proposal, would they be considered to fall within the scope of PSD3/PSR? For Letter h1) of art. 2(2) PSR and recital 29a (and proposed removal of let. h2), we can agree on the proposed approach provided that a further clarification is given as regards the following: we understand that payment transactions with EMTs from a user to a CASP for custody purpose would be excluded, as custody services do not constitute by themselves a payment service under PSD3 (as stated by the Presidency). Is our understanding correct?

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	For the new Recital 29b PSR, we suggest the following amendment that, in our view, is important to ensure clarity and avoid divergent interpretations and application (see proposed amendment below in green). **New Recital 29b** ***Since Directive (EU) 2015/2366 also included a specific exclusion regarding payment transactions made exclusively in cash directly from the payer to the payee without any intermediary intervention, it is appropriate to include a similar exclusion regarding transactions with electronic money tokens carried out without any intermediary involved. This should include transfers of electronic money tokens between two self-hosted addresses, where there is no intermediary involved, ~~either~~ both on the side of the payer ~~or~~ and on the side of the payee, and should not include payment transactions between a custodial wallet and a self-hosted wallet.*** LV (MS reply): We could agree with the Presidency's proposal. NL (MS reply): We have some comments on these articles. Article 2(2)(a1) PSR - Do you mean that a transaction between a custodial wallet and an NC-wallet/self-hosted address would fall in scope of the AMLR obligations (etc.)?

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	Article 2(2) point h2 PSR – is the purpose to make explicit that custodial EMT services are not a payment services? We would recommend then also explaining it in a recital. Elaboration on this could be relevant. Article 1(3) PSD3 - in principle this Directive applies to (entities) providing a set of services as defined in the Annex. 'Cases' does not seem an entirely adequate term. Article 2(2) does not describe cases, this word does not seem adequate. Please consider another term, for example transactions. PT (MS reply): PT generally agrees with the proposals regarding Articles 2(2) and 1(3) of the PSR. RO (MS reply): - SI (MS reply): All transfer services, related to EMTs, regardless their underlying motivation, should be treated equally, therefore as payment services.
Q3. Do Member States agree with the Presidency's reasoning and proposals on the Art. 3(3a) PSD3 , definition of funds, and clarification in recital 6 PSD3?	**ECB**: On article 3(3a), PSD3 it should be clarified that it needs to be the same competent authority (as the CA might differ) and that the information is not only up to-date but also includes payment services specific information.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	AT (MS reply): Yes. BE (MS reply): BE: We agree with the Presidency proposal but note that the Recital 6 PSD3 clarification is a "nice to have" as the notion is already clear in MiCAR. What should be clarified however is that a PI – whether or not issuing EMT- requires a CASP licence for providing EMT transfer services. BG (MS reply): We agree with the Presidency's reasoning and proposals on the Article 3(3a) PSD3, definition of funds, and clarification in recital 6 PSD3. CY (MS reply): We have no comments for the proposal made under Art. 3(3a) PSD3. CZ (MS reply): We agree. With regard to Recital 6 of PSD3 and the amendments leading to further legal clarity, it should also be made crystal clear that when MiCA speaks about an e-

Question	MS reply
	money institution, it is now considered as a payment institution providing e-money services. DE (MS reply): Definition of funds See our answer to Q1. Ad Recital 6 The clarification "The wording proposed by the Presidency in Recital 6 PSD3 takes into account the comment received from one Member State which suggested avoiding referring to Directive 2009/110/EC (the EMD) since it is being repealed and, over time, any references to it could be difficult to trace back and understand" should be adapted and mirrored in Article 9. Ad Art. 3(3a) PSD3 As argued in the last working, we acknowledge the efforts of the POL PCY proposal to streamline the authorisation process for CASPs providing payment transactions with EMTs. However, the proposal of the POL PCY would still lead to a dual licence regime. Such a dual licence regime would constitute a large burden especially for small CAPs and hence, pose a risk to the emergence of a market for EMT payments in the EU. Further, a dual licence regime would undermine the technology neutrality approach. Hence, we need to consider more carefully how to reduce the administrative burden of the authorisation regime. In this regard, we could envision to pair a lighter form of

Question	MS reply
	registration for CASPs providing transactions with EMTs only (comparable to the registration duty of ATM deployers in Art. 38 PSD 3) with a well-timed review clause regarding those duties. By doing so, we could enable the sector to emerge and potentially tighten the licensing standards based on a thorough impact assessment at a later stage. At the same time, we would like to emphasise that CASPs wishing to offer payment services that go beyond payment transactions with EMTs should apply for a regular PSD3 licence and should not be privileged over the licensing process for other financial institutions, in order to maintain a level playing field. DK (MS reply): We agree with the presidency's proposal EL (MS reply): We believe that the change to Art. 3(3a) is in the right direction but is limited in the sense that it covers only the case where the competent authority for MiCAR and PSD are one and the same, which is not always the case. We recommend to take into account the EBA approach in the no-action letter that it is preparing for refinement of the respective provision. We disagree with the clarification in recital 6 PSD3. Title III of EMD2 does not directly correspond to Title III of PSD3. Title III of EMD2 is related to conduct matters (e.g. prohibition of interest, issuance and redeemability) while Title III of PSD3 relates to the delegated acts. Title III of EMD2 rather corresponds to Art. 30 of Title III of PSR.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	ES (MS reply): We suggest the following amendments to the new article 3(3a) of PSD3: "*Competent authorities shall not require undertakings that apply for authorisation to provide payment services under this Directive to provide any information referred to in paragraph 3 that they have already received under the respective authorisation procedures in accordance with Articles 62 and 63 of Regulation (EU) 2023/1114 provided that previously submitted information or documents are still up-to-date*". The amendment is justified by the convenience of specifying that the information already provided (and which does not need to be reiterated to the NCA when payment services are to be provided) is the information provided to obtain an authorization as a CASP. It should be noted that there is another authorization procedure in MiCA, referring to ART issuers who are not credit institutions. HR (MS reply): Please see our answers to Q1 and Q2. In case that certain services associated to the transfer of EMTs are considered payment services, we would strongly support introducing a notification regime for CASPs similar to the one provided in Article 60 MiCAR for financial entities providing certain crypto-asset services. However, if it is determined that in some cases dual licensing will indeed be necessary, we would support the streamlining of the authorization process. IE (MS reply): Article 3(3a) PSD3 – Agree, Recital (6) – Agree.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	IT (MS reply): **IT.** The Discussion note does not address the most relevant issues: how to deal with the case of CASPs providing services with EMTs that are at the same time crypto-asset services under MiCAR and payment services under PSD3/PSR? A solution is needed to avoid creating a regulatory gap and excessive burdens for NCAs and market participants. It should also be examined whether this proposal could also work in cases where NCAs are different for CASPs and PIs. In any case, we should clarify whether the CASP should be considered (i) both a CASP and a PI, or (ii) as a CASP authorized to provide certain payment services with EMTs. This clarification is essential for several reasons, not least for delineating the allocation of competencies between NCAs, especially when they are different for CASPs and PIs. LV (MS reply): Article 3 (3a) – We support the drafting proposal Recital 6 – we support the drafting proposal NL (MS reply): Yes. Especially in favour of streamlining the authorisation procedure considering proportionality and innovation aspects. PT (MS reply):

Question	MS reply
	While agreeing with the principle of preventing duplications and unnecessary burdens, PT would favour framing the introduction of this provision while addressing the possibility for cooperation between NCAs. Please consider the following adjustments: *"(3a) Competent authorities shall not require undertakings that apply for authorisation to provide payment services under this Directive to provide any information referred to in paragraph 3 that they have already received under the respective authorisation procedures in accordance with Regulation (EU) 2023/1114 provided that previously submitted information or documents are still up-to-date. Competent authorities may exchange such information amongst themselves, where appropriate, and if solicited by another Competent authority."* Additionally, PT considers unnecessary the changes proposed to the definition of funds since the adjustments to Recital 15 PSD3 already provides the intended clarification. Moreover, we agree with the alignment proposed by the PRES PL through the amendments introduced in Recital 6 of PSD3. On a final note, PT fears the risk of increased administrative burden with the adoption of a dual licensing regime. In our view, a balance should be sought to ensure proper imposition of supervisory requirements in an efficient manner. A simplified authorisation/notification procedure for institutions with a MiCAR authorisation could strike that balance. Notwithstanding, to avoid circumvention of PSD/PSR provisions,

Question	MS reply
	it must be ensured the institutions in question comply with the relevant PSD2 requirements regarding the transfer of e-money tokens, especially provisions concerning consumer protection, such as safeguarding/safekeeping requirements and execution time of transfers. RO (MS reply): - SI (MS reply): We agree.
Q4. Do Member States agree with the Presidency's reasoning and proposals on safeguarding – Article 9(1) and recital 31 PSD3 – and initial capital/own funds requirements?	**ECB**: In our understanding, the MiCAR Article 70 explicitly differentiates paragraph (1) safekeeping requirements for CASPs which related to the ownership rights clients, especially in the event of the crypto-asset service provider's insolvency, and to prevent the use of clients' crypto-assets for their own account, and safeguarding requirements in paragraphs (2) and (3) which explicitly apply only to crypto assets other than e-money tokens and do not apply to payment and e-money institutions. Thus, with respect to CASP services there is no overlap on safeguarding requirements with PSD2/EMD. Comparing e-money tokens with the treatment of other funds under the Payment Services Directive, it is equitable to uphold the principle that any entity in possession of funds must safeguard these funds by the end of the business day. Failure to do so would contravene the principle of technological neutrality. Under PSD, safeguarding is not limited to payment institutions engaged in issuing. The requirement for the issuer to redeem the funds does not protect the client from the risk of

Question	MS reply
	misappropriation. Crypto-Asset Service Providers (CASPs) have the option to enter into an agent relationship with a payment service provider. Therefore, it is justifiable and adequate that CASPs must safeguard funds held beyond the end of the business day following the day on which the funds were received, delivered to the payee, or transferred to another payment service provider. It is moreover consistent with MICAR which requires safeguarding other crypto assets. Thus, we suggest maintaining safeguarding requirements for CASP under PSD3 consistent with any other funds. On initial capital /own funds requirements where a dual license would be required we agree these funds are cumulative and should remain in line with the respective sectoral requirements Option 1. AT (MS reply): Yes. BE (MS reply): BE: As highlighted in Q1, all services that are likely to be qualified as both “crypto-asset service” and “payment service” should be mapped against PSD3/PSR requirements that are likely to apply to then determine, based on policy considerations, what exclusions can be made. Tackling only some issues, such as safeguarding, is not sufficient to create legal certainty. A deeper analysis and debate should be presented to the Council working party. The forthcoming “No-Action” letter likely to be published by EBA at the request of the Commission could serve as a starting point for the aforementioned analysis. It

Question	MS reply
	should be noted that this no-action letter will likely include recommendations for the co-leglislators and EC to consider in the drafting of PSD3/PSR. BG (MS reply): We agree with the Presidency's reasoning and proposals on safeguarding – Article 9(1) and recital 31 PSD3 – and initial capital/own funds requirements. CY (MS reply): We have no comments regarding the proposals of Article 9(1) and recital 31 PSD3. CZ (MS reply): We are flexible. We would only suggest splitting Article 9 to two separate articles as Article 9 is getting very complicated and difficult to read. DE (MS reply): <u>Ad 9(1) PSD3</u> It should not apply "instead". Firstly, PIs can issue EMT and provide other payment services on top of that. In this case, Article 9(1) should still apply. Secondly, Article 54 MiCAR stipulates that the safeguarding requirements pursuant to Art. 7(1) EMD2 apply and that issuers of EMT should comply with additional safeguarding requirements. Article 9(1) should therefore also apply, and for PIs issuing EMT

Question	MS reply
	Article 54 MiCAR should apply as well, with the same reasoning as above regarding the clarification of Recital 6 (EMD2 will be repealed). The wording proposed by the Presidency in Recital 6 PSD3 takes into account the comment received from one Member State which suggested avoiding referring to Directive 2009/110/EC (the EMD) since it is being repealed and, over time, any references to it could be difficult to trace back and understand. This should be mirrored here, akin to: "where a payment institution issues electronic money tokens, it shall also comply with the additional provisions laid out in Article 54 of Regulation (EU) 2023/1114." Finally, what about the case of the issuance of "significant e-money tokens" with regard to Art. 58 MiCAR. Would we need to import the specific regulations for those cases as well? DK (MS reply): We agree with the presidency's proposal EL (MS reply): We agree. Furthermore, the concept of "safeguarding" EMTs is not clear to us considering that the tokens are on the blockchain – does it mean having custody of the relevant cryptographic keys? ES (MS reply):

Question	MS reply
	We suggest amending the proposal to introduce a new paragraph at the end of Article 9.1 of PSD3, which reads as follows: *"By way of derogation from subparagraph 1, where a payment institution issues electronic money tokens, it shall comply with Article 54 of Regulation (EU) 2023/1114".* As we observe, this proposal aims for payment institutions (currently, EMIs) that issue EMTs to be subject to the safeguarding requirements set out in Article 54 of MiCA, in relation to funds other than the EMTs they issue, and not to the safeguarding requirements set out in Article 9.1 of PSD3. In our view, whether the proposal (reproduced above) establishes that the payment institution issuing EMTs must comply with Article 54 of MiCA, this provision is also referring to the safeguarding of funds in Article 7 of EMD2. In other words, the new paragraph at the end of Article 9.1 of PSD3, which aims to exclude the application of Article 9 of PSD3, nevertheless leads to the application of this latter provision to payment institutions issuing EMTs, because this follows from the reference in Article 54 of MiCA to Article 7 of EMD2. If the intention is to prevent Article 9 of PSD3 from applying to payment institutions issuing EMTs, Article 54 of MiCA should be amended to remove the reference to Article 7 of EMD2. HR

Question	MS reply
	(MS reply): In our opinion, these issues should be considered after it is clearly established whether a PSD3 license will be needed for CASPs providing transfer of EMTs, and if so, specifically for which services such a licence would be required. IE (MS reply): Article 9(1) – Agree, Recital (31) – Agree. We support option 1 for initial capital/own funds. IT (MS reply): **IT.** We agree with the proposals on safeguarding by CASPs providing payment transactions with EMTs (Article 9(1) and recital 31 PSD3). As regards capital and OF requirements, we have some issues regarding the own fund requirements in the case of dual authorisation (under MiCAR and under PSD3), which we would like to clarify to ensure uniform application and convergence. With reference to initial capital/own funds requirements, the proposal does not clarify, in practice, how to calculate the initial capital / own funds that CASPs should hold to provide services related with EMTs that qualify both as crypto-asset services under MiCAR and as payment services under PSD3, as well as the composition of those capital / own funds. In the discussion note, the Presidency settles the issue by stating that capital / OF requirements "would cumulate/add up" in the case of dual authorization. Taking into account that capital / OF requirements under MiCAR and under PSD3 are calculated differently, and that they shall be met with capital/OF that have different composition in the two frameworks, we see merit in clarifying how the cumulated /

Question	MS reply
	adding up approach should work in practice, to avoid duplication of requirements for operators and possible inconsistent application of the rules. Therefore, we see merit in clarifying: first, if the "cumulation / adding up" means that a building-block approach shall apply or instead if it requires that specific activities/elements are carved out from the application of one of the two frameworks; second, how the requirements shall be calculated and apply in practice; and third, how the total aggregate capital / own funds shall be composed. As said, we believe that this aspect should be clarified appropriately, since it is crucial from both a licensing and an ongoing supervisory perspective. In particular, when assessing the actual IC/OF requirements for market operators, according to the current version of the proposal, both applicants and NCAs may struggle to identify, for example, the portion of transfer service falling under MiCAR rules and the ones falling under PSD3 rules, in order to appropriately apply the relevant capital requirements. In this sense, we acknowledge a high risk of duplication of own funds requirements and regulatory uncertainty, and we believe the PSD3/PSR framework constitutes the most suitable legislative instrument to address those issues. We would also submit to the consideration of the Polish Presidency a request for clarifying the following point, **regarding the calculation of OF requirements under PSD3 only**. Since in PSD3 the definition of e-money refers only to "issuance" of e-money (and not anymore to transfer and maintenance of e-money), in our understanding a **PI performing e-money services** should calculate the requirement under PSD3 using: i) Method D referred to in art. 8 PSD3 for the amount related to the **issuance** of e-money, and ii) Method B referred to in art. 7 PSD3 for the corresponding amount relating to e-money volumes transferred or maintained. Could you please confirm if our understanding is correct? This clarification would be important for us in

Question	MS reply
	order to be able to assess the potential impact of the new rules on our market and PIs/EMIs business models. LT (MS reply): Although capital/own funds requirements stemming from 2 regulations – MiCA and PSD3 – would add up, there should be a single capital/own funds requirement statement/reporting. The template could be defined by relevant NCAs. LV (MS reply): Article 9 (1) - We support the drafting proposal Recital 31 – In general, we support the drafting proposal. However, to avoid any misunderstanding, we would prefer that the recital also contained the reference to the Settlement Finality Directive, i.e. "*without prejudice to requirements of the Settlement Finality Directive*", in the last sentence of the Recital 31. NL (MS reply): We agree with the proposal to exempt CASPs providing payment transactions with EMTs to safeguard the EMTs themselves, if our interpretation is correct that the CASP in question is required to safeguard al asset belonging to third parties based on article 70 MiCAR. PT (MS reply):

Question	MS reply
	PT agrees with the approach proposed on safeguarding and does not wish to provide additional relevant remarks at this time. RO (MS reply): - SI (MS reply): Firstly, NCAs should also have the discretion to perform risk based adjustments. Secondly, explicit exclusion of the application of PSD3 safeguarding requirements to CASPs that hold EMTs could be acceptable.
Q5. Do Member States agree with the Presidency's proposals on Art. 70(2), recital 146 PSR and the provided definitions?	**ECB**: We suggest adding in Article 49 that in the case of transfers to an self-hosted address, the payer's Payment Service Provider (PSP) is required to inform the payer about the associated risks and obtain the payer's explicit consent prior to executing the transaction. AT (MS reply): Yes. BE (MS reply):

Question	MS reply
	BE: We agree. BG (MS reply): We have no specific opinion on this question. CY (MS reply): We have no comments regarding the proposals of Art. 70(2), recital 146 PSR. CZ (MS reply): Regarding maximum execution time, we are concerned that Article 70(2) solves only a part of the problem. What about other situations including transfer of EMTs? It is related to more general issue when transfer of EMTs is a payment service or crypto-asset service. We are flexible as regards definitions and Recital 146 PSR. DE (MS reply): As argued in the last working party, we still see the need for a structured and detailed analysis regarding the question of which requirements of PSR should apply to payment transactions with EMTs. Here, are a few thoughts on this: • Maximum Execution Time of payment transactions (p. 5 PCY Note "No derogations from D+1 were added)

Question	MS reply
	The argument presented by some stakeholders is that – for on-chain transactions with EMT – the PSP does not have control over the distributed ledger. It might be the case that a transaction is not executed in the maximum execution timeframe specified in PSR due to network congestion or due to the fact that the transaction is not picked up by the validators. Given that the PSP hence would not have full control over the execution of the transaction, the provisions regarding liability (e.g. Art. 75 PSR) should be discussed thoroughly. • Ex-ante transparency of fees Given that blockchain fees can vary from transaction to transaction, it would need to be tested, if the PSR requirements on ex-ante transparency on fees need to be adapted to on-chain transactions using EMTs. • Verification of the Payee Concerning the verification of payee service and, in general, the application of Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro (SEPA regulation) to EMT transaction, we would like to point out Article 2(1)(f) of said Regulation. According to this provision, 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. In our opinion, this suggests that the SEPA regulation is not applicable to the transfer of EMTs.

Question	MS reply
	However, given the discussions we had in the working party about extending the scope of the verification of the payee service beyond the scope of the SEPA regulation, we should have a separate discussion as well, whether (and potentially how) the verification of the payee service should apply to transactions using EMTs. • SCA SCA should be required for transfers with EMTs – similar to the regime for conventional payments transactions. We have heard from market participants some doubts regarding the applicability of SCA in an EMT context. We should clarify those issues before concluding on the PSR / PSD 3. In total, we should have a structured and detailed discussion on the application of the PSR requirements in the context of EMT transactions. In those discussion, we could potentially borrow from the results of the current EBA work regarding the interplay of MiCAR and PSD 2. DK (MS reply): We agree with the presidency's proposal EL (MS reply): We agree. ES

Question	MS reply
	(MS reply): We do not object the proposal. HR (MS reply): No comments. IE (MS reply): Article 70(2) – Agree, Recital (146) – Agree. IT (MS reply): **IT.** We agree with the proposed definitions. On the proposed Art. 70(2), we agree in principle. However, from a technical point of view, we would be interested in a deeper insight into the possible difficulties for PSPs/CASPs when transactions are carried out using DLT, i.e. on a network outside the control of the PSP/CASP and with execution times and execution costs that are not necessarily predictable. In particular, should any higher fee (to achieve D+1 execution) be borne by the PSP/CASP alone or, if provided for in the framework contract, be paid by the PSU? Furthermore, it should be clarified which is the liability regime for the "delay", in particular in the case of on chain transactions where the maximum execution time cannot be achieved due to causes not attributable to CASPs but to the DLT.

Question	MS reply
	In general, we should discuss many other provisions of the PSR, to assess whether they can be applied to EMTs without problems or if a specific regime would be warranted, including at least the following topics: unauthorised transaction and liability regime; unique identifier (including the service ensuring verification or IBAN-check); fraud prevention (TMM; exchange of information between PSPs, etc.); spending limits; block of a payment transaction/payment instrument in case of suspicion of fraud; rectification of unauthorised or incorrectly executed payment transactions; etc. Therefore, we deem that a gap analysis should be conducted in order to identify which PSD3/PSR provisions can be applied to EMTs and which cannot (for technical reasons or because it would be economically unfeasible to do so for crypto-operators). LV (MS reply): We could support. NL (MS reply): We agree with both amendments, especially that maximum execution time also applies to payment transactions with EMTs. To ensure settlement finality, we believe the risks of potential blockchain congestion should be the burden of the service provider and not the payer/payee as the payer/payee may not be able to appropriately understand/identify all risks. PT (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	PT welcomes the references introduced in Article 70(2) and Recital 146 PSR and does not wish to provide additional relevant remarks at this time. RO (MS reply): - SI (MS reply): We agree.
Presidency Discussion Note **Safeguarding of funds held in settlement accounts with payment systems** **WK 2162/25**	
Q1. Do you agree that PSU funds held in settlement accounts with designated payment systems should be considered as safeguarded for the purpose of Article 9(1) of PSD3 subject to the above conditions?	**ECB:** This proposal (that funds held in settlement accounts with designated payment system should be considered as safeguarded for the purpose of art 9(1) of PSD3 subject to the conditions outlined in the paper) would blur the distinction between safeguarding account and settlement accounts – which is a formal one. In so doing, it disregards the Eurosystem's competence and stated intentions. The Eurosystem policy – adopted in July 2024 – and Decision* – adopted in January 2025 – on non-bank PSPs access to central bank operated payment systems and accounts, clearly states that the Eurosystem will not provide accounts to non-bank PSPs for safeguarding users' funds at central banks. As per international best practice (PFMIs)**, the degree and conditionality of access to central bank accounts is left to the central bank's discretion. The discretion of the ECB under the PSD2 (as well as under PSD3/PSR)

Question	MS reply
	should not be contested. Moreover, the proposal could have undesired side effects on the distinction of deposits from payment accounts. Coming to the proposal's substance – merely for the sake of argument – we note that there are different obligations that would apply to fiduciary account holders – so qualifying an account as safeguarding is not a trifle matter devoid of legal and operational consequences. When fiduciary account structures are permitted, the operator and participants of an SFD designated system such as TARGET should know what additional operational (incl. legal) risks are introduced to the system. This is why, legally speaking, by default, i.e., in the absence of an explicit agreement as to the nature of an account, account holders with an SFD-designated system are deemed to be dealing as principals, not agents. The Eurosystem explicit decision not to offer such accounts to non-bank PSPs was triggered by important institutional (Art. 17 ESCB/ECB Statute***) and policy (avoidance of outsourcing settlement in CBL, impact on price and financial stability) considerations. **ECB Decision on Safeguarding*, *particularly recitals 12 et seq. explaining why safeguarding is not offered.* ** *PFMIs particularly p. 62, footnote 83: "The use of central bank services or credit is subject to the relevant legal framework and the policies and discretion of the relevant central bank."* ****Article 17: Accounts with the ECB and the national central banks. In order to conduct their operations, the ECB and the national central banks may open accounts for credit institutions, public entities and other market participants and accept assets, including book entry securities, as collateral.* AT (MS reply):

Question	MS reply
	Yes. BE (MS reply): BE: We agree that that the funds held in settlement accounts of designated payment systems should be considered safeguarded and support the wording proposed by the presidency and the remarks made by the Lithuanian colleagues for both the new paragraph of article 9 and the new recital (31a) and agree with point made by the presidency that funds held in payment system settlement accounts should be considered as being safeguarded and that this notion should also BE: apply for central bank payment system settlement accounts. We believe that, as outlined by the presidency, this a key component in ensuring that non-bank psps can settle payments on a 24/7 basis in an efficient and competitive manner. BG (MS reply): We agree that PSU funds held in settlement accounts with designated payment systems should be considered as safeguarded for the purpose of Article 9(1) of PSD3 subject to the said conditions. CY (MS reply): We remain sceptical of the proposal made under Article 9(1). CZ (MS reply):

Question	MS reply
	We fully support the proposal of the Presidency. From our perspective, it is important measure to support non-banking PSPs and their willingness to access SFD payment systems. Currently, the approach taken by some SFD payment systems forces PSPs to in fact double the amount of funds held. This would significantly help not only the small market participants. DE (MS reply): We have understood the concerns of the ECB against the proposed amendments to Art. 9 PSD 3. We would need to analyse these comments carefully before giving a definite answer. Therefore, we still apply a scrutiny reservation here. DK (MS reply): We would caution against allowing funds held in settlement accounts with designated payment systems to be considered safeguarded. It is our experience that the courts when deciding whether funds are in fact safeguarded or whether they should be considered part of the wider bankruptcy estate will look at quite strictly whether the funds can be said to be earmarked to specific users and not comingled with funds of the PSP itself.

Question	MS reply
	It is our assessment that this will very seldom be the case for funds held in settlement accounts. Hence, we see some risks in going down this road. We have two additional comments on article 9(1) which we find very important. Firstly, it should be possible to safeguard with government bonds in art. 9(1, second subparagraph)(b) which we also heard support for in the WP during the Hungarian presidency, and secondly since the funds are received commingled it will not be possible to live up to the requirement in art. 9(1, first subparagraph)(a). Art. 9(1, second subparagraph)(b): It could also be government bonds – hence *"issued by institutions authorized in a Member State"* should be deleted – or changed to ***"issued by highly rated institutions, governments or government agencies"***. We believe this amendment would be very important since it would not be possible to use government bonds for safeguarding with the current wording. Art. 9(1, first subparagraph)(a): Given the way the international card schemes operate, this requirement cannot to our mind be fulfilled at all times prior to safeguarding occurs. The funds will be received commingled, and PIs will often receive less funds than what they owe their customers (e.g. due to chargebacks etc). Thus, the requirement cannot be fulfilled before the

Question	MS reply
	funds are actually safeguarded. There should therefore be included some kind of timeframe for the safeguarding to occur. We have inserted "as soon as possible" but "without undue delay" or another timeframe indication could also be reasonable. Drafting suggestion: "(a) those funds shall **be safeguarded as soon as possible and once the safeguarding has occurred those funds shall** not be commingled at any time with the funds of any natural or legal person other than the payment service users on whose behalf the funds are held;" EL (MS reply): EL: We propose that the final outcome of the Q&A 7165 related to article 10 of PSD2 should be taken into consideration in drafting suggestions of article 9 of PSD3.Since this is a topic currently being analyzed for the purposes of finalizing the above-mentioned Q&A, feedback from both EBA Sub Group of Payment Services (SGPS) members and EBA and European Commission legal services has been requested. The EBA staff will update the draft answer of the Q&A 7165 and submit it for final comments and review to EBA SGPS members and EBA SUPRISC. Then the Presidency shall propose similar adjustments in article 9 of PSD3. ES (MS reply): If the legal safeguarding of funds in a settlement account in a payment system designated under the SFD is foreseen, we wonder if this legal safeguarding also

Question	MS reply
	applies when that settlement account is managed by the Central Bank operating the payment system. The proposed new Article 9.1a does not expressly establish this, but the new recital 31a of PSD3 does. Specifically: Article 9.1a: *"Funds of payment service users held by a payment institution in settlement accounts with payment systems designated under the Settlement Finality Directive shall be considered as safeguarded for the purpose of paragraph 1 if those funds are not commingled with the funds of any natural or legal person other than the payment service users. Member States shall ensure, without prejudice to requirements of the Settlement Finality Directive, that funds of payment service users held in settlement accounts with payment systems are insulated in accordance with national law in the interest of the payment service users against the claims of other creditors of the payment institution, in particular in the event of its insolvency."* Recital 31a: *"Where a payment institution has been granted access to become a direct participant in a payment system designated under the Settlement Finality Directive,* ***including a payment system operated by a central bank****, funds of payment service users held in a settlement account with such payment system should be deemed to be safeguarded provided that those funds are not commingled with the funds of any natural or legal person other than the payment service users. This is necessary to enable payment institutions to*

Question	MS reply
	ensure, in an efficient manner, sufficient liquidity in the settlement accounts to facilitate uninterrupted processing of outgoing and incoming payments, including instant payments. To facilitate protection of funds of payment service users held in settlement accounts with designated payment systems in the event of the insolvency of a payment institution, Member States should ensure that those funds are insulated in accordance with national law in the interest of the payment service users against the claims of other creditors of the payment institution." It should be noted that one possible interpretation is that settlement accounts must necessarily be considered safeguarding accounts, for which national legislation must provide that the "*funds of payment service users held in settlement accounts with payment systems are insulated in accordance with national law in the interest of the payment service users against the claims of other creditors of the payment institution, in particular in the event of its insolvency*." If this interpretation is confirmed, it would not only go against the discretion granted to the Central Bank itself to safeguard (or not) the funds in its accounts, according to Article 9.1 of PSD3, and the policy expressed by the ECB, but it would also create serious application problems in payment systems operated by Central Banks, as well as in the application of Monetary Policy by the ECB. FI

Question	MS reply
	(MS reply): FI: We agree on the principle that such funds would be considered as safeguarded. However, we would have a concern regarding drafting on the proposed subparagraph 1a, namely on the duty of MSs to ensure that funds are insulated in accordance with national law in the interest of the payment service users against the claims of other creditors of the payment institution in particular in the event of its insolvency. It remains unclear what actually would be the actual duty of MSs in this regard, would the general national insolvency legislation be adequate and thereby we should only stipulate on the segregation of funds, or should there be some specific clauses in the insolvency laws. This would also imply harmonisation of national insolvency laws, where we would advice caution. In addition, what would be the other events than the insolvency (it is stated that …"in particular in the case of insolvency"). These may become an issue for interpretation at the transposition phase. Also, we would have a question what would be the interplay between the proposed addition of new paragraph 1a, and the last subparagraph of paragraph 1 which contains the same duty for payment institutions. This is also a question of what is the base text because in HU compromise proposal that particular sub-paragraph is amended to cover both MSs and payment institutions. In any case we would see that the duty to insulate should be vested with the payment institutions and thereby propose to revert back to the original COM proposal in this respect. HR

Question	MS reply
	(MS reply): No comments. HU (MS reply): Yes, we agree. IE (MS reply): We agree that PSU funds held in settlement accounts with designated payment systems can be recognised as being in line with the requirements of Article 9(1)(a). However, we would note that the prohibition on commingling of funds doesn't arise under the conditions of Article 9(1)(b), where insurance or a similar guarantee is applied as the method of safeguarding. We might suggest that the draft Article 9(1a) and Recital 31a should cater for both methods of safeguarding, Article 9(1)(a) and (b), even if use of (b) is rare. IT (MS reply): **IT**. In our opinion, the question should be analysed with respect to central bank-operated systems and private-sector systems. As for the former, beyond the legal feasibility of the proposed approach, we note a possible inconsistency with the discretion for central banks whether or not to open accounts to non-bank PSPs as per article 9 of PSD3 Proposal (similar to what foreseen in MiCAR). We recall that the Eurosystem's policy and decision on the matter are also based on such discretion.

Question	MS reply
	Against this background, the provisions should ensure fair treatment irrespective whether a non-bank PSP would access a central bank-operated system or a private-sector system, with solid grounds to justify any different treatment between the two cases. Overall, the new regime should allow non-bank PSPS to operate on a level playing field with banks, again with solid grounds to justify any different treatment between the two types of entities. LT (MS reply): • **We strongly support the proposal**, it aligns with the EU's Retail Payments Strategy to foster competition and innovation for which instant payments are foreseen as main enabler. However, current restrictions on using client funds for settlement in payment systems create significant operational challenges for non-bank PSPs, and also make it burdensome to fulfil safeguarding requirements. Without the possibility to efficiently use these funds, many non-bank PSPs struggle to provide seamless services, ultimately limiting competition and innovation. • To effectively participate in payment systems and provide payment services, payment institutions must be able to use client funds for client payments without excessive restrictions. A strict requirement to deposit funds separately for safeguarding purposes—outside the payment system—significantly limits a payment institution's ability to operate efficiently. As highlighted in the discussion paper, maintaining sufficient and readily available funds in settlement accounts 24/7 is particularly crucial for instant payments.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	• **The Presidency's proposal strikes a crucial balance**. Proposed conditions—ensuring that client funds are not commingled and remain insulated from creditors' claims—adequately secure client assets. As a result, these funds should be recognized as safeguarded under the regulatory framework. So, these provisions ensure strong safeguards for client funds, at the same time grants PSPs the necessary conditions to operate efficiently by having the necessary liquidity in the payment system. • **Risks are managed.** We hear comments that non-banks' funds in payment systems' accounts raises different risks. But funds held within payment systems, particularly in central banks, will be limited to what is essential for payment execution, and that effectively manages and minimizes risks related to financial stability and monetary policy. Moreover, caps for settlement account balances can also be reviewed periodically based on real circumstances. • **When addressing risks, we must prepare for crisis situations without unnecessarily restricting the daily operations of payment institutions**. For instance, central banks should have the option to implement back-stops on flows from payment institutions to central bank accounts in the event of a potential bank run. • Finally, we see the **EBA's upcoming RTS on safeguarding as an opportunity to clarify practical aspects** of funds insulation and prevent regulatory arbitrage, ensuring a more stable and competitive payments ecosystem. • Several MSs mentioned that it might be difficult to comply the requirement to not comingle client and own funds, e.g. in case of received fees for their services. Earned fees are closely related to the provision of payment services, therefore do not pose risks, and could go

Question	MS reply
	through a settlement account in the payment system. Also, as proposed by one MS in the meeting, it could be required in such cases to ensure separation without undue delay. This issue could be included into the EBA mandate on safeguarding, where concrete explanations regarding fees or other situations are provided. LV (MS reply): We support, it will promote competition and not overburden PIs/EMIs. We would like to reiterate the importance of the reference to the Settlement Finality Directive in the proposed text of Article 9 (1a). This reference will ensure that the funds within the system are still available for the system to be used as a collateral security according to Article 4 of the Settlement Finality Directive. NL (MS reply): Although we are welcoming steps towards a solution, we are hesitant if this is the right one. We understand that this brings benefits to non-bank PSPs and we would like to see a workable solution for the safeguarding issue. However, we also see how this goes against a level playing field compared to banks. Moreover, we see a risk of non-bank PSPs advertising themselves as “central bank money backed” without have the same amount of safety and thus occurring safter to the public than what they actually are. It is also not in line with the Eurosystem policy which takes into account important topics such as financial stability. On the other side, we also see how this could benefit non-bank PSPs and thus also innovation and competition.

Question	MS reply
	PT (MS reply): PT does not follow the assumption that funds held in the settlement account need to be subject to the rules established in Article 9 PSD3, given the fundamental differences between the purpose of a safeguarding and a settlement account. The proposed alignment overlooks the primary purpose of placing funds in such accounts, which is to meet settlement obligations, and should be limited to the amounts necessary for this purpose, as highlighted by the ECB in its *"Policy on access by non-bank payment service providers to central bank-operated payment systems and to central bank accounts"*. RO (MS reply): - SE (MS reply): First of all, it should be possible to safeguard with government bonds in art. 9(1, second subparagraph)(b), hence we support the proposal from the Danish delegation that *"issued by institutions authorised in a Member State"* should be deleted, or changed to *"issued by highly rated institutions, governments or government agencies"*. Secondly, we see that the two types of funds have quite different purposes that may be difficult to combine – one is that the non-bank PSP should have quick access to funds and be

Question	MS reply
	able to make transfers, and the other is that the funds should be protected in insolvency. We suggest to rephrase the new paragraph (1a) in article 9 of PSD3 as follows: "*Funds of payment service users held by a payment institution in settlement accounts with payment systems designated under the Settlement Finality Directive* ***~~shall~~ may*** *be considered as safeguarded…"* SK (MS reply): We agree.
IE Non Paper: Fraud prevention measures - PSD3/PSR WK 2069/2025	
Q1. Do Member States agree with the proposals on fraud prevention measures?	AT (MS reply): We strongly support the aims and measures proposed in the revised IE non-paper and ask for their implementation in the PSR framework. Social platforms play a vital role in the emergence of fraud and their obligations should therefore be adequately addressed. BE (MS reply): BE: regarding the dedicated communication channel, we refer to our response in Q10. Regarding the verification of the identity of the advertisers and their authorised status, we can be flexible. BG

Question	MS reply
	(MS reply): We agree with the proposals on fraud prevention measures provided that they do not create problems with the sectoral legislation. CY (MS reply): We support the proposed drafting suggestions made to Article 59 and the requirement to establish dedicated communication channels for PSPs in order to both report fraud and take action in response to the reports made. We see merit in the suggestions made for the 'Verification of advertisers of financial products' and support exploring how these very large online platforms and online search engines could play a part in preventing the dissemination of advertising an unregulated financial service/ financial service provider. CZ (MS reply): In general, we are hesitant to support IE non-paper. The co-operation duty in Article 59 should be different from blocking access or blocking or removing content. Similar obligations in relation to content already exist in the DSA and in the interests of legal simplicity and clarity, these obligations should not be disintegrated into more regulations. On the other hand, for some part of the ECSPs (see the issue of this definition above) it is not possible to remove any content from communication. For blocking access to websites or internet access by ISPs, a solid basis needs to be provided to the obliged operators for such conduct. On dedicated contact channels - this could be too burdensome for smaller ECSPs. However, we could support this provision in relation to VLOPs and VLOSEs. We would also like to point out that a similar obligation also exists under the DSA.

Question	MS reply
	According to Articles 10 and 11, all intermediary services have to designate a single contact point. According to the European Commission, several investigations are already underway into breaches of the DSA, including fraudulent advertising and other scams. The CZ NCA believes that similar measures described in the non-paper can actually reduce fraud. On the contrary, colleagues responsible for the DSA warn that we should use existing tools and not go beyond the DSA. We also question whether this provision would introduce a general monitoring obligation. If it is possible, we would like to ask the Council Legal Services for their opinion. For the reasons stated above, we would like the European Commission to clarify which of the proposed obligations can already be derived from the DSA. Obligations from the DSA should not be duplicated in other regulations. We would also ask countries where voluntary or statutory restrictions on online advertising apply to share their experiences on this topic. DE (MS reply): We support the IE non-paper on fraud prevention measures. The amendments to Article 59(5) provide a promising avenue to integrate ECSPs on a more robust basis in the fight against payments fraud. As this newly established collaboration between PSPs and ECSPs is a cornerstone in fraud prevention, there should be a close monitoring of the success of this collaboration – either in the platform on combating payment fraud or in the context of a review clause. With regard to the "verification of advertisers of financial products" we do see the necessity to work on the text in order to increase legal clarity. First, the provision

Question	MS reply
	could benefit from more clarity regarding the timing of the verification – e.g. shall the platform check the status of the advertising company on an ongoing basis or only before entering a contract with the advertising company? Second, on what basis should the verification take place? We would see merit here to link the provision to the registers published by competent authorities – for payment institutions the register of Article 17 PSD 3. Finally, compatibility of the provisions proposed in the IE non-paper with other sectorial regimes, in particular the DSA, need to be checked. We have understood the reasoning of the IE delegation, however, would support an additional check by EU COM here. DK (MS reply): Regarding the suggestions for a new article treating advertisers of financial product we agree with the Irish suggestions. We find the Irish arguments compelling and agree that the solution seems workable in practice as well. On the suggestions for article 59 we would suggest a slightly alternative approach. In the drafting it is suggested that ECSPs should either remove or block fraudulent content, however, technically there is a difference between what the telcos can do and what the digital platforms can do.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	For telcos: it is not possible for telcos to remove specific fraudulent content on any website. Telcos can technically remove access to a website, however, an obligation to do so would not be in conflict with the principles of the EU legislation on net neutrality and the EU approach that all online traffic should be treated equally and openly without discrimination, blocking, throttling or prioritization. It is the Danish position that telcos should not be obligated to remove access to websites without a prior decision from the courts (as was for instance the case with The Pirate Bay which was banned after being convicted in court for ongoing copyright infringements). For the digital platforms: it is not technically possible for digital platforms to remove other websites. They can, however, remove content on their own platforms which include advertisements. According to the Digital Services Act (DSA), digital platforms are already liable for illegal content on their platform if they do not take immediate steps to remove the illegal content when made aware of such. For these reasons we are opposing the wording in the non-paper for art. 59. Below and in our answer to Q5 in the Presidency note we have provided alternative suggestions. We generally believe that DG CNECT should be consulted in strengthening the role of telcos and digital platforms.

Question	MS reply
	Solutions We believe that digital platforms could contribute in a way which might be aligned with the intention of the Irish suggestion. For Digital Platforms, we could ensure a more efficient removal of fraudulent advertisements or content posted on their platforms. This could be done by allowing PSPs to become trusted flaggers under the DSA. In that case, a PSP would get direct access to the digital platforms and make aware of specific fraudulent content which should be removed. Moreover, such inquiries by trusted flaggers should be prioritized by the digital platforms. Further, stronger measures could be considered for the very largest online platforms (VLOPs). We could support making VLOPs liable for fraudulent content, so they would no longer be protected by the limited liability in the DSA. According to the DSA, online platforms can only be held liable if they do not take immediate steps to remove fraudulent content when made aware of such. The PSD3/PSR could make digital platforms liable for fraudulent content, effectively requiring them to monitor and remove such content of their own account. VLOPs are better positioned to scan for and remove fraudulent content than smaller platforms and often have a role in promoting problematic content based on their algorithms.

Question	MS reply
	For Telcos: We would suggest a flexible obligation for telcos to cooperate with PSPs both after a fraud has taken place and in order to prevent fraud, in line with our comments to Q5 to the Presidency note. Definition Since we see very different requirements for telcos and digital platforms, we also believe it would be important to split up the definition of ECSPs into two separate definitions – one for telcos and one for digital platforms. And then clearly specify the requirements for each of them. EL (MS reply): EL: We agree with the drafting suggestions introduced in article 59 by the IE non paper. Regarding the verification of advertisers of financial products, we are in favour of introducing a link between the PSR and the DSA in order to engageVLOSEs in the effort to combat fraud mainlyperformed through phishing sites in search engines. However, we believe that the DSA requirements under article 34 are enough to reduce the "dissemination of illegal content" and probably a drafting suggestion is needed to define that "illegal content" might be a phishing site impersonating a legitimate financial entity. ES (MS reply):

Question	MS reply
	We strongly support the IE non paper on fraud preventive measures. FI (MS reply): FI: In principle, we support the aim of these proposals but believe that a more appropriate way forward would be through a review clause as proposed by the Presidency to allow for a impact assessment and a thorough analysis as regards the proposal's relationship to the ePrivacy Directive and possible future ePrivacy instrument to be proposed by the Commission. We are of the opinion that the measures entailing the processing of communications (meta)data by providers of electronic communications services should be regulated in the context of ePrivacy. As regards the IE non paper however, we note that a too-detailed proposal on ECSPs' obligations could be problematic without a proper impact assessment. The proposed introduction of dedicated communication channels, removing or blocking access to content (or where inappropriate, explaining the reasons) could, depending on the definition of an ECSP, as well on whether the proposal in intended to cover the processing of contents of communications, entail several problems: • As the obligation would concern (especially) bank impersonation fraud, it could particularly involve **phone call, text message, or email scams**. In this respect, we find the wording "*remove or block access to content*" ill-suited to describe the blocking of calls or text messages based on their falsified sender data. While the proposal continues to give calling line identification and electronic mail address as

Question	MS reply
	examples, the proposal in unclear as to whether it would also cover processing of contents of communications (in addition to traffic data), such as filtering based on harmful links in SMS for instance. It appears to us that technical measures legally available for providers of electronic communications services would vary among Member States, because the ePrivacy Directive is unclear on the extent of allowed processing traffic data for security purposes and because it seems that national legislation based on Article 15(1) of the Directive would be required to enable the processing of contents of communications; this issue could be more appropriately managed in the context of the ePrivacy reform. Secondly, preventing spoofing and impersonation is not technically straightforward, requires cooperation also among providers of electronic communications services, and there will always be coverage gaps in the blocking. Thirdly, although some measures for detecting possibly falsified email addresses exist, their use requires that the financial sector also implements necessary security techniques such as SPF, DKIM or DMARC. Moreover, in the case of end-to-end encrypted messaging services like WhatsApp or Signal, it is not technically possible to analyse the content of the messages at all. • **As regards the possible blocking of internet addresses and domain names, if intended to be included in the proposal**, this would create tension with the Open Internet Regulation, which strictly regulates when internet traffic restrictions can be imposed. Internet service providers would have to decide themselves when to implement DNS or IP blocking (the latter being particularly prone to blocking of legitimate services at the same time), or to explain why the action was not taken

Question	MS reply
	(potentially a significant burden). Normally, such blocking measures are ordered by a court. HR (MS reply): We support the proposal, provided that it is consistent with the DSA. HU (MS reply): Prevention is the best tool to fight fraud. We believe that the IE proposals can serve as a good basis for further improvements on fraud prevention. IE (MS reply): N/A. IT (MS reply): **IT.** In principle we appreciate the fraud prevention measures suggested in the IE non-paper, however: - in relation to art. 59(5)(ii) and (iii) it should be clarified which is the competent Authority for the enforcement of those measures imposed on ECSPs. Indeed, we remind – as previously pointed out in previous rounds of comments – that ECSPs currently fall outside the remit of national authorities which are competent for the payment sector - with regard to the suggested new provision, we support that this kind of horizontal provision should be a cross-sectoral legislation, since this type of fraud in the payment sector in some

Question	MS reply
	countries concerns a minority of cases (in Italy e.g. around 8%). We appreciate that according to the new wording the duty is clearly imposed only on VLOPSEs. Moreover, there would be the need to identify the competent authority for verifying the fulfilment of obligations imposed on ECSPs. LT (MS reply): We agree. LV (MS reply): In general, we support the proposed additions, we welcome the legal clarity of the PSU funds' safeguarding status within the settlement system. The communication channel between operators is supportable, but probably more efficient would be one common channel where PSP could report the fraud rather than to each operator. For example, also it could be effective if the main server of the communication channel would be under supervision of a regulatory authority. Regarding the advertisement – theoretically it sounds effective, but it is not clear how effective it would be in practice. NL (MS reply): In general, we support the direction of travel of this paper and we welcome the broadening of the scope of 59(5) to other types of fraud than just bank impersonation fraud. We do have some specific comments and questions:

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	- It is not clear to us whether Internet service providers and platform providers are also part of the definition of ECSPs in this case. This should be clarified. - We can follow the statement that checking the identity/status of advertisers is not in itself the same as monitoring traffic for illegal content, and therefore fits under DSA article 8. However, we would like to hear what the EC lawyers think about this. - How can VLOPSEs effectively verify if an advertiser is indeed a registered financial services provider? Do they have access to public databases? Without such infrastructure, how can platforms execute the required verification process? - What enforcement mechanisms are available against VLOPSEs in cases where bad actors circumvent the verification process by initially not indicating their intention to place financial advertisements, but subsequently posting fraudulent content? This could potentially bypass the requirement that platforms 'verify that it is an authorized financial service provider'. And who is supposed to enforce this obligation? The European Commission as the primary regulator for very large online platforms under the DSA? - We suggest clarifying the conditions under which it would be inappropriate for electronic communications services providers to act swiftly, as mentioned in Article 59. For instance, when blocking access to information might also affect access to legitimate content, or when a more targeted measure is possible (e.g. directed at an online platform). This could for example be done by introducing an accompanying recital. PT (MS reply):

Question	MS reply
	PT is conceptually in favour of expanding the collaboration described in Article 59(5) to other fraud instances besides bank impersonation cases and would not oppose the suggested establishment of dedicated communication channels, and the expansion of obligations expected from ECSPs, as envisioned in the IE non paper. We hold the same view on the possible introduction of a new article on verification of advertisers of financial products. However, PT would seek further analysis by the Council in this regard with the cooperation of the COM on guarantying interplay between sectoral legislation, proper enforcement of imposed obligations, and reliance on its supervision by the respective competent authority. RO (MS reply): We support Ireland's proposal for art. 59 para (5) with amendments that aim to prevent the reappearance of fraudulent content that has already been removed. Therefore, we propose the following alternative wording (added a new point iii)): (5) To facilitate the reporting of ~~Where informed by a payment service provider of the occurrence of the type of~~ fraud, including that ~~as~~ referred to in paragraph 1, by payment service providers, electronic communications services providers shall establish dedicated communication channels. Once in receipt of such reports, electronic communications services providers shall cooperate closely with payment service providers and act swiftly to

Question	MS reply
	(i) Ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC, including with regard to calling line identification and electronic mail address. (ii) Remove or block access to content of relevance to the cause of the reported fraud; **(iii) Take all necessary actions to prevent the reappearance of the fraudulent content that has already been removed**; and (~~ii~~iv) Where it is inappropriate to take such action, as mentioned at (ii) and (iii), electronic communications services providers shall explain the reasons. Regarding Article XX - while we agree with proposal referring to the responsibility of the online platform to verify that the entity that intends to become an advertiser is an authorized financial service provider, we believe that this requirement should not be addressed in PSR/PSD3 but rather in the dedicated regulatory framework, respectively within Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). SE (MS reply): We support the proposals. Investment fraud is the type of fraud generating the highest crime profits in SE. However, we wonder why the reporting requirement/communication channels are limited to electronic communications services providers? In our understanding, this does not cover online platforms or search engines. We also support the broadening of the obligations in article 59 to all types of impersonation fraud.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	SI (MS reply): We agree in general. SK (MS reply): In principle we agree with the aim of the IE non-paper. However, regarding the second proposed element concerning advertisements we are not convinced that such measure would not be in conflict with Article 8 of DSA. Verification of the identity of the advertisers would, in our understanding, lead to the active seek of circumstances in the second step, as they would need to verify in cases of non-authorised advertisers if given advert can be considered financial product advertisement. In the light of the comments made by DG Connect during the last Working Party, we would welcome legal opinion on what is in this regard achievable within PSR/PSD3 scope, without being in conflict with Article 8 of DSA.
DE Non Paper: Proposals for Simplification in PSR / PSD3 regarding reporting and notification obligations WK 2068/2025	
Q1. Do Member States object to any of the proposals to remove specific reporting and notification obligations presented in the non-paper? If so, please provide the justification.	AT (MS reply): We support the efforts to delete the reporting obligations in Article 48 para. 6 and 7 PSR, Article 81 para. 1 subparagraph 3 PSR and Article 39 PSD 3. We also ask for a

Question	MS reply
	reintroduction of well-suited powers for NCAs to act against non-licensed activities, as already foreseen under PSD2. BE (MS reply): BE: We do not object BG (MS reply): We do not agree with the proposed deletion of Article 39 of PSD3, as the exclusions concerned represent large-scale activities and therefore the notification obligation should be preserved. In addition, we would to note that the reference in Article 39(2) of PSD3 should be corrected, insofar as the latter should refer to the exclusion under Article 2(1), point (k) of PSR (payment transactions by a provider of electronic communications networks as defined in Article 2, point (1) of Directive (EU) 2018/1972). Nevertheless, we strongly support the deletion of Article 81, paragraph 1, subparagraph 3 PSR, regarding the reporting of a "comprehensive assessment of the operational and security risks relating to the payment services, as proposed in the DE Non-Paper. CY (MS reply): We do not object the proposed amendment regarding Article 32 We do not object the proposal to delete Article 48 para. 6 (and 7) PSR. We do not object the proposal to delete Article 81 para. 1 subparagraph 3 PSR and Article 83a para. 4 PSR.

Question	MS reply
	We remain sceptical of the proposal to delete Article 39 PSD 3 in its current form. CZ (MS reply): We would like to thank our DE colleagues for a very interesting non-paper. We can fully support simplification in terms of reporting and notification, and for this reason we can preliminarily support proposals to remove such notification and reporting requirements as proposed in the DE non-paper. We particularly welcome proposal regarding Article 81 PSR and DORA. As an important simplification, we also support complete deletion of Article 39 PSD3. DE (MS reply): We understood from the working party that a majority of MS supports our proposals regarding the deletion of the reporting obligations of Art. 32(7) PSR, Art. 81(1) PSR and Art. 83a(4) PSR. However, we heard diverging feedback regarding the proposed deletion of the reporting obligation of Art. 48(6) PSR and the notification obligation of Art. 39 PSD 3. Hence, we would like to once again stress our position on those provisions: Art. 48(6) PSR We have more than 1,300 ASPSPs in Germany. Rolling out a new general reporting obligation to them regarding the data on access by AISPs and PISPs as required by Art. 48(6) is a large-scale IT project that would tie up significant resources in the roll-out phase for our NCA as well as for the ASPSPs. As a result of the reporting obligation of Art. 48(6), we would obtain a full data set on access by AISPs and PISPs, which has its merits. However, we

Question	MS reply
	could envision to derive a similar value of information from running a well-crafted survey among AISPs and PISPs regarding their ability to access data and accounts from ASPSPSs at much lower costs. Given their own business interests, we would be optimistic that payment institutions would cooperate on such project given. As a result, we really question the necessity of the reporting obligation of Article 48(6) PSR and argue for its deletion. <u>Art. 39 PSD 3</u> Article 39 PSD 3 essentially requires Member States to introduce notification obligations for service providers whose activities are explicitly excluded from the scope of the Directive. From our supervisory experience those notification obligations will only be met by compliant and well-informed service providers. In contrast, service providers who have specifically redesigned their business models so that the payment activities offered would fall outside the scope of PSD 3, or who do not apply for a license due to a lack of knowledge, are typically not complying with the notification obligations. The competent authority needs clear and reliable supervisory powers to investigate on those service providers. However, these powers should be based on clear prohibitive provisions – in line with Article 37(1) PSD 2 – and not on the breach of a notification duty. We have made concrete drafting proposals in our written comments to the last working party. When taking those supervisory powers on board, there is no need for the notification obligations of Article 39 PSD 3 anymore. In total, this change of approach – away from notification duties towards clear supervisory powers – would lead to a more effective supervision with regard to non-licensed activities, while decreasing the supervisory costs for compliant PSPs and competent authorities. We refer to our non-paper for more details and stand ready for any discussions on this subject.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	DK (MS reply): We agree with all of the German suggestions for PSR. Regarding the suggestion for article 39 of PSD3. Denmark does not agree with the proposal to remove the obligation for companies to justify being specifically excluded from the scope of the directive. However, DK agrees with the suggestion of introducing the wording from Article 37(1) of PSD2, granting the NCA the authority to independently assess whether a business model falls under the regulation. EL (MS reply): EL: No comments. ES (MS reply): Although we can accept the proposal of simplification regarding Article 83a.4 of PSR, in general, we do not agree with the elimination of reporting obligations.

Question	MS reply
	In particular, the risk assessment included in the payment directive does not have the same scope as that of DORA, as it includes operational risks, which may or may not be ICT-related. Regarding the reporting of AISP/PISP access data, the information, which should be collected by the PSP as part of its daily operations, could be of supervisory interest. On the other hand, some communications are very exceptional. This would be the case for the notification of participation in fraud information exchange agreements or those related to limited networks exceeding one million euros in operations, so we do not see excessive impact on PSPs. FI (MS reply): FI: As a general remark, as the information requested is such that would be needed by the NCAs at some point of time, deleting reporting requirements merely shift the burden to NCAs. Thus, some general caution would be advisable. On the detailed proposals, we would prefer to retain art. 83a par. 4 of PSR and Art. 39 of PSD3. On the former, this kind of a notification to an NCA is not major burden and provides NCA with information whether PSP is participating to an information sharing arrangement and to which. On the latter, this assists NCAs to focus on service providers most likely be in breach of regulations. Regarding non-compliance with the notification duty stipulated by this

Question	MS reply
	Article, it is a legal requirement which can be sanctioned. Thereby, if there is non-compliance, it is rather a matter of sanctioning than deleting the requirement. HR (MS reply): We agree with the proposal to remove the obligations in Articles 37(2), 81(1) subparagraph 3 and 83a(4) of the PSR. On the other hand, we propose to keep the reporting obligation in Article 48(6) PSR and notification obligation in Article 39 PSD3 because they provide valuable information about open banking/information from the market about excluded activities. HU (MS reply): We have scrutiny reservation . We are currently discussing this topic with our NCA. IE (MS reply): Overall we support most of the papers proposals and support the goal of simplification. That being said we do not support the removal of Article 39. IT (MS reply): **IT.** With regard to **Article 32 of PSR**, we have no objection to the German proposal, since credit institutions are already obliged to notify the NCA of the closure/withdrawal of the account. Regarding **Article 48(6) of PSR**, while we are aware of the burden on the system (PSPs and authorities) associated with these obligations, we believe that the information received could be

Question	MS reply
	very useful for improving OB services in terms of efficiency and competitiveness, to the benefit of the system as a whole. Therefore, we do not agree with the German proposal to remove the obligation under Art. 48(6), which seems to result from a specific national situation that differs from the experience of the EC, the ECA and the Italian context. Having said that, in an attempt to minimise the impact of the new reporting requirement and to avoid duplication, we have tried to intervene with some drafting suggestions on the text of Art. 48 PSR (in green below) to better specify and circumscribe the type of data to be requested from ASPSPs (and possibly PISPs and AISPs) in order to improve open banking services (especially in terms of performance). *PSR, Article 48* *1. Competent authorities shall ensure that account servicing payment service providers**: i)** comply with their obligations in relation to the dedicated interface referred to in Article 35(1) and Article 38(1), (2), (3), (4) and (5)**~~:~~; ii)make sure ~~and~~** that any identified prohibited obstacle listed in Article 44 is removed as soon as possible by the relevant account servicing payment service provider, **iii) make sure the dedicated interface meets high level requirements in terms of performance and functionalities**. *Where such **inadequate performances or** noncompliance of the dedicated interfaces with this Regulation or obstacles are identified, including on the basis of information transmitted by payment initiation services and account information services providers, the competent authorities shall take without delay the necessary enforcement measures and impose any appropriate sanction.* *[…]*

Question	MS reply
	6. Account servicing payment 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. ***Such data set include at least: i) statistics on the availability, unplanned unavailability and performance of their dedicated interface, in relation to art. 35(5), ii) statistics related to the response time of the dedicated interface to account information service providers' and payment initiation service, providers' access requests, in relation to art. 36 (1c), iii) statistics regarding the transaction volumes of their dedicated interface.*** ***Competent authorities can include in the data set other data regarding the existence of obstacles and the compliance with obligations in relation to the dedicated interface referred to in Article 35(1) and Article 38(1), (2), (3), (4) and (5).*** *Competent authorities may also, where appropriate, require account information service providers and payment initiation service providers to provide any relevant data on their operations.* *In accordance with its powers pursuant to Article 29, point (b), Article 31 and Article 35(2) of Regulation (EU) No 1093/2010, the EBA shall coordinate that monitoring activity by competent authorities, avoiding data reporting duplication.* *The EBA shall report every two years to the Commission on the size and operation of the markets for account information services and payment initiation services in the Union. Those periodical reports may, where appropriate, contain recommendations.* *7. The EBA shall develop draft regulatory technical standards specifying the data to be provided to Competent Authorities pursuant to paragraph 6 as well as the methodology and periodicity to be applied for such data provision**, including website representation and***

Question	MS reply
	Competent Authority data reporting referenced in Article 35, paragraph 5, concerning statistics on performance and availability. On the proposed changes to **Article 39** of PSD3, we agree that it would be appropriate to reintroduce in PSD3 the prohibition contained in Article 37(1) of PSD2 and a reference in the provision to the powers, already referred to in recitals 37, 49 and 58 of the proposed PSD3, that would allow national authorities to act against unlicensed activities. On the other hand, we do not support the proposal to remove the notification requirement, currently contained in Article 37(2) and (3) of PSD2 and replicated in Article 39 of PSD3, because in our experience the notification requirement has contributed to the disclosure of many cases of limited network exemptions and their providers not previously known. In fact, prior to the entry into force of PSD2, only few operators had submitted their business models to us for assessment; for these reasons, while we understand and share your position on the burdens on NCAs in assessing notifications and maintaining up-to-date lists, we believe that the objectives of knowledge of the payments market for the authorities and transparency to consumers must prevail. Regarding **art. 81(1) subparagraph 3 of PSR**, we agree with the proposal of removing the obligation of the annual reporting related to the comprehensive assessment of the operational and security risks relating to the payment services. We are in favour of reducing the quantity of assessment reporting about risks that are required to all PSPs, in line with the objective of containing the burden of additional reporting requirements also pursued in the SSM. On **Art. 83a(4)**: we do not oppose its deletion, provided that such arrangements can be easily found through other means (e.g., by requiring both the arrangements and the list of adherents to

Question	MS reply
	be made public) or, in any case, that the NCA can obtain this information based on the powers granted under Art. 91 PSR. LT (MS reply): Article 32 para. 7 PSR, de-risking – we agree with the proposal, sharing the motivation of refusal would be more useful. Article 48 para. 6 PSR – OB reporting. Agree. Worth analyzing available information in Payment statistics collected under the ECB regulation, it might be sufficient for the OB market evaluation. Article 81 para. 1 subparagraph 3 PSR – op. risk reporting. Agree. Article 83a para. 4 PSR – notification of joining info sharing mechanisms. Agree Article 39 PSD 3 – LNE reporting. Agree. It is an excessive process that does not give added value or safeguards to consumers, but imposes an assessment burden on the NCA. There was no such registry before PSD2, we do not see improvements after it was introduced with PSD2. It would be enough to regulate what is considered as limited network exception, i.e. when it is not necessary to obtain a license; and the obligation should stay with the service provider to self-assess if it fulfills LNE conditions. If someone acts without a license, without the right to do so – then relevant measures should apply. Therefore, as mentioned by several MSs – powers of NCAs in case of unauthorized activities should be clear. LV (MS reply): We support the proposal, if it is possible to simplify then it is the right direction.

Question	MS reply
	NL (MS reply): We are in favor of the proposed removals except for Article 39 PSD3. In the Netherlands, the notification obligation under PSD2 helps identify unlicensed service providers. The enforcement approach of our NCA is heavily dependent on signals from the field. The notification obligation and the public register help reporters check whether a provider is known to our NCA. Without this obligation, this check is missing, which can reduce the quality of signals about unlicensed service providers. PT (MS reply): PT would favour the consideration of retaining Articles 48(6) and (7) PSR, as well as Article 39 PSD3. On Articles 48(6) and (7) PSR, PT authorities already receive the information under concern by ASPSP, considering it useful to address the penetration status, evolution and pertinence of these services in the national market. We also see it as valuable to enhance harmonization across MS, boosting comparability and facilitating a broader European assessment of the activities performed by AISP and PISP, believing the proposed EBA RTS will contribute to this regard. On Article 39 PSD3, PT notes that its removal may exempt certain entities (that facilitate the provision of services foreseen in Article 2(2), point j of PSR) of any notification obligations, including ones with significant market position, which could

Question	MS reply
	increase systemic risks associated with non-authorised activities. We label Article 39 as balanced in terms of covered universe, as it only applies to entities that execute above EUR 1 million in annual transactions. Nevertheless, PT supports enshrining in PSD3 the missing Article 37(1) of PSD2 to guarantee the prohibition norm foreseen in said provision. RO (MS reply): We could accept the proposal. However, as previously stated, regarding the limited network exclusion, we consider that it would be useful to introduce a periodic reporting requirement in order to see the size of the market and asses the possibility to require a PI authorisation for those business that grow in size on a regular base, as we consider that the development of the payment services market through exempted entities could present risks, as the users of such services do not benefit from PSD/PSR protection. Additionally, while we also agree with the proposal to forward to competent authorities their motivation for refusing to open or the decision to close an account to the applicant or account holder, we believe that the sentence should be added at the end of Article 32 para. 3 PSR not para. 4. Further on, we agree with Germany's view and support the deletion of article 81 para 1 subparagraph 3 PSR given that this obligation is already under DORA regulation, and the corresponding article 95 from PSD2 was already amended by DORA Directive EU 2556/2022

Question	MS reply
	Finally, regarding article 83 para. 4 PSR, we do not agree with Germany's view regarding the deletion of Article 83a para. 4 PSR mainly because there is a supervisory benefit that arises from having an overview of the participants. We believe that this benefit arises from the ability of planning topics to be discussed within the information sharing, depending on the participants that take part in the information sharing agreement and also allows NCAs to be informed with regards to the identity of PSPs or other relevant stakeholders that might miss relevant information that is being disseminated within the information sharing agreement. SE (MS reply): We are positive towards the proposals. Our main concern would be on the suggestion in article 32 para 4, specifying that a notification should be made by mail. We are concerned that it might be burdensome for the competent authority to handle and sort so many mails. The format should be left to national discretion. SI (MS reply): We agree with the proposals. SK (MS reply): We support simplifications suggested by DE with the exception of the deletion of Article 39 PSD. Reporting under this Article is of importance for our NCA. In this regard we would also support reintroduction of powers for NCAs to act against non-licensed activities.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
FR Non Paper: Transparency on payment card schemes fees and rules **WK 2324/2025**	
Q1. Do Member States agree with the proposals on transparency of fees and rules of payment card schemes?	AT (MS reply): While we share the intentions expressed by the FR delegation, it seems that the matter could also be left to a more comprehensive revision of the Interchange Fee Regulation. In any case, we support the implementation of an additional review clause regarding the evolution of payment card fees. BE (MS reply): BE: We agree with the proposal. BG (MS reply): We agree with the proposed approach of the FR Non-Paper. However, we would prefer to see the amendments being made in Regulation 2015/751. CY (MS reply): We support the proposal for increasing transparency in payment card scheme fees and rules. CZ (MS reply):

Question	MS reply
	We could support the transparency proposal, but we are not sure if this should be solved in PSR. We think it would be better to handle this in the revision of the IFR. DE (MS reply): We are still analysing the non-paper and hence, need to apply a scrutiny reservation. DK (MS reply): Denmark appreciates the French initiative, and the opportunity to have a discussion on the topic of reported opaque fees and rules of payment card schemes. In Denmark card acquirers have raised similar concerns, that is concerns on the lack of a clear link between a charged fee and provided service. Acquirers have e.g. reported "fines", that is "behavioral" scheme fees, imposed by schemes to nudge a change or a practice. However, acquirers report, that they sometimes do not have the insight to change their practice or advise their customers, the payees, on how they should change a practice or update equipment. Denmark believes that the suggested new article 31a may be difficult to enforce according to the intention of the French proposal in its current wording. Card schemes

Question	MS reply
	will likely point to their extensive price and rule books and claim transparency. Though it would not be actual transparency. We would therefore suggest to elaborate on what "a transparent manner" could be or how it is to be understood. A suggestion could be to require a headline grouping, categorization, classification of fees with clear indication to scheme or processing (switching) service provided. If the article and/or recitals are to loosely formulated, enforcement will be difficult. <u>Notification period:</u> Denmark has a suggestion with regards to the length of the "notification" period. There could be a risk of price signaling if the period is too long: A possible effect or impact of long notification periods is that card schemes may use these as test on how competitors will react, and if they will also announce similar increases in fees or introduce new fees or not. Competitors can in this way signal their (future) prices to one another. Therefore, Denmark suggests a shorter period than the one in the suggested article 31a. Regarding the proposal for a ***New paragraph 3 added to Article 108 of PSR.*** Denmark supports such a report as it would increase the knowledge on fees in both the

Question	MS reply
	Commission and Member States, however, we would suggest that the report should not be made public but only be shared with NCAs. With competition in mind: Publishing such detailed information on fees and rebates, which is suggested, that the Commission is to collect, may lead to even higher fees. In Denmark we have seen such examples in the past in other markets where the publication of prices leads to higher prices. Therefore, publication of prices/fees may dampen the competition among card schemes. Schemes may be inspired by other schemes possible increases in fees to increase own fees. Thus, publication of such sensitive and confidential price information can only be published/disclosed if confidentiality of the individual fees charged by different card schemes can be maintained. This is especially relevant in member state where only two schemes operate. In short, Denmark notes the risk, that the Commission by collecting and publishing a report on fees and rebates might dampen competition, by making it easier for card schemes to identify the competitor's prices and rebates etc. An alternative suggestion is, that the Commission collects the information and share it with National Competent Authorities but do not publish a report. The NCA's then have

Question	MS reply
	detailed information reported every second year, for them to supervise and enforce the suggested article 31a. EL (MS reply): EL: We think that should be included to Interchange Fee Regulation – IFR ES (MS reply): We strongly agree to include transparency provisions under the PSR. Although it could be argued that IFR is a better place to regulate the referred fees, it is unknown when and if the referred file will be reopened, and this issue could be efficiently tackled under the PSR transparency provisions. We find it necessary to clarify the term "payment service business end-users" (does it refer to merchants?) by detailing the reasons for their inclusion. Additionally, it should be noted that the proposed notice period of 9 months may constitute an excessively intrusive and burdensome restriction for card schemes, especially in a context of price instability. Therefore, this period should be sufficiently justified and based on the time it may take for a PSP to adhere to a new scheme. To reconcile both objectives, it might be considered to maintain a sufficiently long notice period, along with the possibility of applying the corresponding change retroactively if finally accepted by the PSP.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	FI (MS reply): FI: We support the French proposal to add to the transparency of card scheme fees. However, the proposed review clause seems a bit too far-reaching, particularly points d and e (capacity to challenge rules and fees as well as the competition constraints), perhaps these should rather be considered as part of IFR-framework. HR (MS reply): In our opinion, this issue should be considered under the Interchange Fee Regulation. HU (MS reply): As we expressed in the CWP, we support to conduct further investigations on this matter, but we believe that this should not be addressed in PSR but in IFR. IE (MS reply): We agree with these proposals. IT (MS reply): **IT.** We can support this proposal. For the new proposed Article 31a PSR, we would like the following clarification: does the term "payment service business end user" refer to merchants (also taking into account that the merchant's contractual relationship is typically with the

Question	MS reply
	acquirer and not with the payment card scheme)? If this is the case, a clarification should be added in the recital. LT (MS reply): Proposed requirements seem to pose administrative burden to NCAs in supervising if new requirements are implemented. Therefore, we do not support. Moreover, card scheme fees transparency should be addressed under the Interchange fee regulation. LV (MS reply): We are aware of the problems indicated in the recent report of the European Court Auditors. We are not opposed to transparency in card scheme payments. NL (MS reply): We agree with the proposals but we do have some comments. Regarding the proposed new Article 31a PSR, paragraph 2: It requires card schemes to communicate their rules and fees to end-users, in addition to issuing and acquiring PSPs. This seems redundant since acquiring PSPs already handle this under Article 9(1) of the IFR. Regarding the proposed new paragraph 3 of Article 108 of the PSR: It states that the EC must report on the 'rebates and incentives' that acquirers and issuers have received from the card

Question	MS reply
	schemes. This information provides insight into competitive information and includes sensitive details, particularly for issuing PSPs. Therefore, it may be advisable for the EC to report this information at an aggregated level by country. PT (MS reply): PT follows the urgent need to enhance transparency fees and rules imposed by ICS, without necessarily imposing additional limits or controls. Notwithstanding, we question whether the obligations foreseen in the newly proposed Article 31a PSR should not be better considered in a future review of IFR, namely because, in our view, the payments package under negotiation tends to be mostly dedicated towards norms applicable to PSP in relation to their PSU, not evolving card schemes and their business model. We also question whether the inclusion of the article as is guarantees proper supervision and enforcement of these new obligations. However, PT supports the inclusion of the review clause as a minimum approach to address this matter in the current file. RO (MS reply): We support the FR proposals since, in our opinion, additional EU proposals/measures that can help to increase transparency on fees and rules in order to reinforce a clear view over the card payments market and also for reducing the costs associated with accepting cards should be in general supported. We appreciate that such measures are necessary to increase electronic payments usage and also for reducing the informal economy.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	SE (MS reply): We support the initiative. SI (MS reply): We agree. SK (MS reply): We support reinforcement of the transparency in general, but in the non-paper we miss the details on what would happen in the case on non-compliance. Also we would like to point out that in our view main issue with the fees is competition on the market. Two international card schemes are not enough to bring the competitive forces fully to the market and thus put pressure on the fees. It would also be beneficial from the resilience point of view to have additional pan-european solution.
EL Non Paper: Proposal for Regulating the Operational Framework of ATM Deployers **WK 2090/2025**	
Q1. Which of the following options do you prefer for regulating ATM deployers? • *Option A: Ensuring clear wording that defines collaboration between the ATM deployer and an authorized PSP for cash withdrawal.*	**ECB:** We agree with both with options A to require a contractual agreement with a PSP or option B licensing for cash-withdrawal services. For simplifications, it could also be clarified that these are 'agents'. 'agent' means a natural or legal person who acts on behalf of a payment institution in providing payment services;

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
• *Option B: Requiring ATM deployers to be authorized Payment Institutions for cash withdrawal services, eliminating the need for separate registrations in each Member State.* • *Option C: Granting the EBA a mandate to define the exact conditions for ATM deployer registration.* • *Option D: None of the above.* *Please indicate your preferred option and the reasoning behind your choice.*	Option C, while fine in principle it would mean to overburden EBA with another mandate AT (MS reply): We prefer option D and suggest sticking to the progress made by the (former) PCYs so far. BE (MS reply): BE: We prefer option D. Based on our market observations we do not see a need to change the regulatory landscape for ATM deployers. If option D is not a possibility we would prefer option B. BG (MS reply): We prefer Option C: Registration with an EBA Mandate that will define the exact conditions for ATM deployer registration. We prefer Option C, as Options A and B create an additional burden that does not correspond to the nature of the services provided. CY (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	We see merit in Option A and support providing further clarity on the collaboration between the ATM deployers and the authorized PSPs. We are supportive of these services being offered by legal persons only. CZ (MS reply): We support option d) – none of suggested options. DE (MS reply): In current supervisory practice in Germany ATM provider need a licence as a PI/CI or to have a contract with a PI/CI that is legally responsible for the operation of the ATMs. Given that this supervisory framework works well for Germany and, hence, we do not see any need for changes to the system, we would prefer the options closest to the current German system, which would be Option B (preference 1) or Option A (preference 2). However, with regard to option A, we would feel that the definition proposed for Article 2(35) is too strict by excluding the ATM provider to be himself a PI. Irrespective of the concrete choice between the options for us the two most important prerequisites of a future supervisory framework on independent ATM deployers are: 1. There is legal certainty about who is the obliged entity with regard to AML law (either the ATM deployer himself or the legally responsible PI/CI).

Question	MS reply
	2. There is legal certainty about who is the obliged entity with regard to Article 6 of "Council Regulation (EC) No. 1338/2001 of 28 June 2001 laying down measures necessary for the protection of the euro against counterfeiting". Those two prerequisites must be met by any framework in the area of independent ATM deployers. DK (MS reply): Denmark would like to thank Greece for the non-paper. It is an important topic, and we welcome the focus on privately owned ATM's. We believe that the response to our own non-paper indicated that there was no appetite for an authorization requirement. And with the addition of an explicit possibility to withdraw or deny a registration, we believe that should be sufficient powers for the NCAs. This leads us to believe that neither options A nor B are viable, as option A in a sense would make the entire set-up superfluous – it would in the final instance be the PSP operating the ATM. We are not quite sure what exactly the EBA would be mandated to do – but we strongly believe in harmonization and could thus support an EBA mandate if it is believed by other member states to bring value.

Question	MS reply
	In any event, we do not think that ATM deployment should be passportable, no matter which option is chosen. Registration should occur in the host member state. EL (MS reply): EL: In Greece, the issue of ATM deployers has been a major concern, which is why we drafted a non-paper outlining our proposals. Our goal was to establish a clear regulatory direction that eliminates room for multiple interpretations by different supervisory authorities. As highlighted in our non-paper, under PSD2, the exemption for ATM deployers in Greece is only granted if they collaborate with a licensed Payment Service Provider (PSP), who retains the ultimate responsibility for the cash withdrawal service. Option A under PSD3 was specifically drafted to ensure this condition remains clear and unambiguous. However, following the European Commission's position expressed during the meeting on February 21, it has become evident that the existing regulatory framework under PSD2 - despite requiring cooperation with a PSP - has been highly problematic. Its interpretation by both providers and supervisory authorities has failed to ensure proper compliance. The Commission's proposal, by integrating ATM deployer services into the supervisory framework and establishing a clear registration regime with adequate and tailored requirements, appears to offer a more structured approach.

Question	MS reply
	Given these developments, we tend to accept Option D. However, we recommend that recital 63 be amended to clarify that: 1. The new approach, whereby ATM deployers are subject to a registration regime instead of being required to collaborate with a PSP, is appropriate. Instead of excluding them entirely from the regulatory scope, they should be subject to a specific prudential regime adapted to the risks they pose, with registration as the sole requirement. 2. ATM deployer services - which enable cash withdrawals from ATMs without providing a payment account - do not fall under any of the licensed services listed in Annex I, particularly service (1): "Services enabling cash to be placed on and/or withdrawn from a payment account."This makes them a hybrid service, for which registration is deemed sufficient. 3. This registration should not be passportable across Member States. Instead, ATM deployers should be registered separately with each national authority. We believe that these clarifications will help ensure legal certainty and an appropriate supervisory approach for ATM deployers under PSD3. ***-Drafting Suggestion-*** *Recital (63): Directives 2007/64/EC and 2015/2366/EU conditionally excluded from their scope payment services offered by certain deployers of automated teller machines (ATMs). That exclusion has stimulated the growth of ~~independent~~ATM services in many Member States, in particular in less populated areas, supplementing bank ATMs. However, this exclusion has proven difficult to apply due to its ambiguity with regard to the entities covered by it. To address*

Question	MS reply
	this issue, it is appropriate to make explicit that previously excluded ~~independent~~ATM deployers are those which do not service payment accounts and that their activities do not constitute any of the licensed services listed in Annex I, particularly service (1).Taking into account the limited risks involved in the activity of such ~~independent~~ATM deployers, it is appropriate, instead of excluding them totally from the scope~~, to subject them to a specific prudential regime adapted to those risks, requiring only a registration regime~~ to be subject to a registration regime tailored to the specific risks they present. Furthermore, to ensure proper implementation, registration should be required in each jurisdiction where an ATM deployer operates, without the possibility of passporting across member states. ES (MS reply): We would only oppose Option B, since we consider an authorisation regime to be disproportionate to these effects. Our preferred option is option A, followed by D, then C. FI (MS reply): FI: We prefer option D, which is the currently proposed registration framework. We strongly object to placing any further requirements on ATM-operators, as this would very negatively impact their current business models and they would reconsider their willingness to continue to provide cash-withdrawal services. As ATM-networks are key for providing cash to the

Question	MS reply
	public, the withdrawal of ATM-services would be highly detrimental to the availability of cash. As of the option A, this is actually a requirement to have an agent-principal -relationship, which is too far-reaching. It may also impact competition negatively, as the entry of a ATM-network would be conditional on their ability to find a principal, with appropriate terms of contract. Option B is too far reaching, the current registration requirement appropriately responds to risks and facilitates supervision. Regarding option C, it remains unclear what would the exact requirements to be drafted by EBA, the requirements should be established at Level 1. HR (MS reply): We prefer option D because we agree with the current proposal for the registration of ATM deployers in the PSD3. HU (MS reply): We prefer Option A. IE (MS reply): Our preference is for Option D, do not amend draft Council text. Options A and B are unduly onerous on existing ATM deployers and hence could push existing ATM deployers into exiting the sector. Such an outcome would damage consumers access to cash both in Ireland and across

Question	MS reply
	the EU. In regard to option C we are of the view that existing draft provisions for registration of ATM deployers are sufficient, there is no need for an EBA mandate here. IT (MS reply): **IT.** As previously said, our first best is the inclusion of ATM deployers among payment institutions (**Option B**), being authorized for cash withdrawal services, and consequently their submission to a full licensing/authorization regime as PSP, with the consequence, inter alia, in terms of full application of AML/CFT safeguards. However, with regard to Option B an express clarification is required on how to define ATMs located in Member States other than the one in which the authorisation is granted, in order to eliminate any ambiguity on the applicable AML regime and which supervisory authority is responsible for it. In this regard, we believe that such ATMs should be considered as a form of establishment other than branches, in accordance with recital 27 AMLR which clearly classifies in such terms ATMs providing for crypto-asset services. As a result, ATM deployers would be clearly subject to the AML regime and to the supervision of the State of that establishment. Alternatively, as second alternative with regard to Option B, ATMs located in Member States other than the "Home" ones should be defined as a form of "other types of infrastructures" pursuant to art. 38 AMLD6, through which the authorized Payment Institution operates under the freedom to provide services in other Member States; also this option should allow AML supervision of the "Host" authorities on such ATMs under the conditions of art. 38 AMLD6. The above-mentioned clarification is pivotal in the AML/CFT perspective as in both cases the central contact points under Article 41 AMLD6 should be established.

Question	MS reply
	If option B is not accepted, we are even open to discuss option A) although it seems complex because the ATM Deployer would be a sort of agent operating on behalf of a PSP but would still be subject to registration (the responsibility for AML controls and cash recirculation would lie with the PSP). To complement such option, we reiterate our previous comments to underline that art. 38 should be amended: 1. including in par. 2 a reference to art. 3, par. 3, point (m)(ownership structures); 2. as already pointed out for option B, however clarifying that ATMs located in Member States other than the one in which the PSP is authorized should be considered as a form of establishment other than branches (according to recital 27 AMLR) or at least classified as "other types of infrastructures" (pursuant to art. 38 AMLD6); in any case the establishment of a central contact point should be required according to the Article 41 AMLD6; 3. clarifying how the distribution of competences among Home and Host authorities would work as regards granting, denying and withdrawing the registration; to this regard we note that Art. 38, par.1, sets out that deployers '*shall register with a competent authority of the home Member State*' while par. 3 mentions that '*competent authority of the Member State where the ATM is being deployed may deny a registration according to paragraph 1 or may later withdraw the registration'* Finally, we would not support option C because we believe the issue should be addressed at L1. In any case, we strongly advocate for a clear definition on the regime applied to ATM Deployers according to Art. 38, par. 4, for the purposes of AML/CFT laws and for legal framework regarding the protection of the euro against counterfeiting under Council Regulation (EC) No. 1338/2001.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	LT (MS reply): Option A covers only one possible scenario, i.e. when ATM deployer has clear relationship with at least one PSP (provides services on behalf of it). But in the market exists also a model where ATM deployer provides services in its own name, without collaborating with specific PSP. E.g. Euronet network. Regulation should cover this case also. It should not be required to ATM deployers, which act as acquirers, to necessarily have a contract with another PSP. In case ATM deployers charge a fee directly, it should be ensured that PSU does not face double charging for the same transaction. D. We support the requirement of registration in countries where cash services are provided. LV (MS reply): In our experience, we have not experienced any problems with ATMs. In fact, customer dissatisfaction, complaints about ATMs have significantly decreased. We are one of the few EU countries where banks are obliged to coordinate essential outsourced services with the responsible supervisory authority. Option A: In our view, the registration rules are too burdensome, as they require a very large number of documents, and the registration would be valid only within national borders. Option B: We would support this option insofar as it would at least provide the possibility of passporting, but it would still be a disproportionate burden on these providers. Perhaps,

Question	MS reply
	however, a cross-border option could be added to the registration regime if it is decided to do so. We would be in favour of maintaining the status quo that these providers do not need to obtain any authorisation from the NCA. NL (MS reply): We prefer option D, but could also live with option C. Our reasoning per option will follow below. Option A: We do not think that it is proportionate to demand a contractual obligation between an ATM deployer and a PSP regarding offering payment services. Option B: We also think that this is not proportionate and we do not have sufficient information/the impact assessment of the European Commission does not give sufficient evidence to require authorization. Option C: We think that this is a good step forward. Option D: our preference.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	PT (MS reply): PT supports Option A of the presented scenarios, agreeing with the clarifications envisioned in a new Recital and adjustments to Article 2(35) Regarding the adjustments introduced in Article 38(1), we believe certain amendments should be introduced as to further clarify PSP liability while representing an ATM deployer. The suggestion bellow is inspired in what is foreseen in other legislation, such as the outsourcing regime under AMLR. Additionally, we question the amendments introduced in Article 38(5) which seem to foresee the ATM deployers need to be PSP, aspect that seems inconsistent with the rationale described in the non-paper. Please consider the following adjustments: *"(1) Legal persons providing cash withdrawal services by means of ATMs as referred to Annex I, point 1, and who do not service payment accounts, do not provide other payment services referred to in Annex I and cooperate based on a contractual agreement with one or more authorized payment service providers, shall not be subject to authorisation but shall register with a competent authority of the home Member State before taking up activity, on condition that the payment service provider remains fully liable for all acts, whether of commission or omission, in connection with the cash withdrawal services provided by the ATM deployer on its behalf. The payment service provider shall be able to demonstrate to the competent*

Question	MS reply
	authority the fulfilment of its obligations under this directive and Regulation [PSR] regarding the withdrawal services provided by the ATM deployer on its behalf.~~ensures the fulfilment of its supervision obligations towards the competent authority.~~ *(…)* *~~(5) Legal entities providing the services referred to in paragraph 1 of this Article shall be exclusively payment service providers.~~"* On a final note, and as previously manifested, PT believes Article 38(3) should envisage additional criteria for the refusal or withdrawal of the registration, as it only refers to the non-adequation of the information provided to ensure the sound and prudent management of the ATM deployer. Furthermore, we reiterate that Articles 34 and 36 should also identify the situations where the withdrawal of a registration may occur, so as to avoid legal uncertainty. In this vein, we propose the following amendments: **Article 38 (3)** 3. The competent authority of the Member State where the ATM is being deployed may deny a registration according to paragraph 1 or may later withdraw the registration ~~if it is not satisfied that the information provided according to paragraph 2 is adequate to ensure the sound and prudent management of the ATM deployer.~~only where:

Question	MS reply
	(a) the person providing the services referred to in paragraph 1 has explicitly renounced to the registration; **(b)** the person providing the services referred to in paragraph 1 no longer meets the conditions for granting the registration or fails to notify the competent authority on major developments in this respect **(c)** the person providing the services referred to in paragraph 1 has obtained the registration based on false statements or any irregular means; the person providing the services referred to in paragraph 1 falls within one of the cases where national law provides for such withdrawal. Article 34 (new number) (xx) Competent authorities of the home member state may withdraw the registration only where: **(a)** the person exempted benefitting from an exemption under paragraph 1 has explicitly renounced to the registration; **(b)** the person benefitting from an exemption under paragraph 1 no longer meets the conditions for granting the registration under paragraph 2; **(c)** the person exempted benefitting from an exemption under paragraph 1 has obtained the registration based on false statements or any irregular means;

Question	MS reply
	(d) the person exempted benefitting from an exemption under paragraph 1 has breached its obligations in terms of money laundering or terrorist financing prevention under Directive (EU) 2015/849; **(e)** the person exempted benefitting from an exemption under paragraph 1 falls within one of the cases where national law provides for such withdrawal. Article 36 (new number) (xx) Competent authorities of the home member state may withdraw the registration only where: **(a)** the person referred to in paragraph 1 has explicitly renounced to the registration; **(b)** the person referred to in paragraph 1 no longer meets the conditions for granting the registration or fails to notify the competent authority on major developments in this respect; **(c)** the person referred to in paragraph 1 has obtained the registration based on false statements or any irregular means; **(d)** the person referred to in paragraph 1 falls within one of the cases where national law provides for such withdrawal. RO (MS reply):

Question	MS reply
	Considering that the recital 63 provides a minimum explanation for this regime (i.e. "independent ATM services … this exclusion has proven difficult to apply due to its ambiguity with regard to the entities covered by it ... it is appropriate to make explicit that previously excluded independent ATM deployers are those which do not service payment accounts. Taking into account the limited risks involved in the activity of such independent ATM deployers, it is appropriate, instead of excluding them totally from the scope, to subject them to a specific prudential regime adapted to those risks, requiring only a registration regime"), we are of the opinion that, until the objectives of this regime are clarified and substantiated, we cannot support either the authorization or the registration of independent ATM providers. If the main risk identified is related to AML/CFT, we do not agree that this issue should be dealt with in the PSD framework. However, **if PRES keeps the registration proposal, it must be very clear which type of prudential regime these entities are subject to.** Furthermore, it should be clarified if these independent ATMs could provide only cash withdrawal or also cash deposits given that, according to Art. 38 para. (1), natural or legal persons providing cash withdrawal services through ATMs as referred to Annex I, point 1, and who do not service payment accounts and do not provide other payment services referred to in Annex I, shall not be subject to authorisation. However, according to the provisions of para. (2), sub-para (2) of the same Article, the natural or legal person registering shall provide a description of its audit arrangements (…) to ensure continuity and reliability in the performance of the payment service as referred to in point (1) of Annex I. In addition, we see merit in clarifying that those independent ATMs that provide exclusively foreign exchange services with cash do not fall within this category and, consequently, are under no obligation to register under PSD3.

Question	MS reply
	Moreover, for the first proposal, we see the need for further details regarding the cooperation framework, as well as clarifying if the activity is outsourcing, if the DORA requirements are applicable etc. SE (MS reply): We would prefer the authorisation requirement in option B. Our authorities see elevated ML risks with this type of ATM deployers. Cash services is always a high-risk area. SI (MS reply): We prefer Option B (requirement for licensing eliminates different approaches throughout the MSs and consequential forum shopping and enables easier supervision (one NCA as opposed to current solution with multiple possible registrations and thus NCAs). However, it is necessary to check the implications to existing text (definition of payment services, principle of proportionality). SK (MS reply): We would strongly oppose option B, which would allow passporting of ATM deployers. We do not have strong opinion on the other options, however any regulatory measure could impact existing business models greatly, and thus we are leaning towards option D.
Q2. Do you agree with the recommendation to remove the term 'independent' to prevent potential misinterpretations of the ATM	AT (MS reply):

Question	MS reply
deployment use case, avoiding confusion with scenarios where 'a deployer' is responsible only for the installation and the operational maintenance of ATMs?	We are open to it. BE (MS reply): BE: It should be clear from the text that the targeted deployers of ATMs are the legal entities which have no contractual relations with the card holders. BG (MS reply): We have no specific opinion on this question. CY (MS reply): We agree with the recommendation to remove the term "independent". CZ (MS reply): We have many times called for deleting the word "independent" as it is redundant and misleading. However, we can see substantial differences in the "installation and the operational maintenance of ATMs" and operation of ATM deployer. The installation and the operational maintenance of ATMs is a technical service which is not connected to providing payment services. DE (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	- DK (MS reply): We would prefer to keep “independent” in the wording. However, we can be flexible in this regard. In our view it would be significant to set proper requirements to the deployer in all cases disregard if the wording contains “independent” or not. EL (MS reply): EL: We believe that the term 'independent' should be removed to prevent confusion with cases where an entity is solely responsible for the installation and maintenance of ATM equipment. ES (MS reply): Yes, we agree to remove the term “independent” for the reasons stated by the presidency. FI (MS reply): FI: As there seem to be a value in term of “independent”, we would prefer to retain it. HR (MS reply): We agree. HU

Question	MS reply
	(MS reply): We are open to the deletion of 'independent' from the term 'independent ATM deployer'. IE (MS reply): We can agree with removal of the term "independent". IT (MS reply): **IT.** We could agree to remove the adjective "independent" either if solution A passes (because the ATM would be an agent acting on behalf of the PSP and therefore it lacks independence), or if option B passes (because the ATM would be equated with an IP). LT (MS reply): Agree LV (MS reply): We agree with EL proposal to remove the term 'independent'. NL (MS reply): Yes. PT

Question	MS reply
	(MS reply): PT does not oppose the suggested removal of the term *"independent"*. RO (MS reply): - SE (MS reply): Yes. SI (MS reply): We agree. SK (MS reply): No strong view, but some adjective could be useful to differentiate from other entities deploying ATMs.
BE Non Paper: Security of Banking Applications **WK 2361/2025**	
Q1. Do Member States agree on the proposal to add a measure aimed to enhance the security of mobile application, i.e. an additional activation step?	AT (MS reply): In general yes. However, it must also be possible for the actual payment service user to change their contact details (i.e. telephone number, e-mail) in a sufficiently easy way.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	BG (MS reply): We believe that since the re-activation of mobile banking applications is subject to strong customer authentication through two independent elements, the additional measures proposed by the BE Non-Paper would create an additional burden for payment service providers, without increasing security. CY (MS reply): We see merit in the proposal to add a measure aimed at enhancing the security of mobile applications. CZ (MS reply): We believe the SCA is sufficient, so we do not agree with adding an additional activation step. It could cause more problems and in reality, reduce a security. The general rules for SCA are applicable also to activation of mobile banking etc. DE (MS reply): We consider it more efficient to avoid frauds in the first place than to argue about the liability afterwards. In general, we are open to discuss the introduction of an additional activation procedure when installing a mobile application for the first time and / or onto a new device.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	DK (MS reply): While we in general are sympathetic to all steps that could enhance security of payments and mobile applications, we are not quite sure whether this is in fact needed or whether current requirements of SCA are enough. It is our general view that requirements here need to be flexible enough to allow PSPs to adapt to an ever-changing environment. If other member states are convinced that this adds value, we will not oppose. EL (MS reply): EL: We support the introduction of additional requirements to enhance the security of mobile application registration. Drawing from our experience in Greece, where regulatory pressure has led PSPs to implement stronger security measures - such as time delays and enhanced alerting procedures - we believe similar improvements should be considered more broadly to strengthen fraud prevention.Specifically, we propose that device registration should include a mandatory delay before enabling transaction approvals via biometrics or quick PIN, ensuring a more secure activation of the possession element. Additionally, an enhanced notification system should be implemented, where PSPs send multiple notifications through different channels to inform PSUs about upcoming device activation.Lastly, we suggest introducing a limit on the number of registered devices per user for PSP mobile applications, further mitigating security risks. ES

Question	MS reply
	(MS reply): Given the special implications of fraudulent enrolment of devices linked to an account, and the limitations of SCA against some particularly relevant fraudulent practices in these operations, we consider it very appropriate to incorporate an additional security measure, as long as it does not introduce excessive friction. The option of a cooling-off period, while the payment service user does not confirm the installation, seems suitable for these purposes. Additionally, it should be noted that we see similar risks in the installation of a mobile application as in the enrolment of devices linked to the account or the addition of a new card to an x-pay. Thus, we consider this measure appropriate in all these cases. FI (MS reply): FI: Preliminarily we are supportive of the proposal in general as such measures could be useful from a fraud prevention point of view. HR (MS reply): We support the proposal. HU (MS reply):

Question	MS reply
	We can support any initiative that strengthens payment security. At the same time, it is necessary to formulate future-proof solutions, therefore, we believe that general rules applicable to all payment methods are necessary, instead of regulations providing separate solutions for different payment methods and technologies. IE (MS reply): We are not against the proposal but have some concerns. The proposal doesn't appear to consider digital banks whom complete the application and on-boarding process all in app. In these cases, a user whom downloads a banking app may not already have an account so how would the digital bank already have their mobile number to send a code to. It needs to be clarified in drafting that this requirement wouldn't apply in cases where a user downloads a digital banks app and sets up their bank account in the app as opposed to in a bank branch, the requirement could then apply for any subsequent digital bank app installations on new devices. Additionally, we would query how this activation requirement would interact with Article 85 on SCA. Article 85 of the Commission proposal already requires PSP to apply SCA when a PSU accesses their payment account online. Presumably this captures instances when a banking app is installed and an attempted log in is made. So how would this requirement substantively increase security and would it not in effect duplicate this requirement in Article 85? In terms of the proposed notification requirement, how would a notification be sent at the exact point when an app is installed? Presumably the app on any given device can only linked to a

Question	MS reply
	PSU once there is an attempt to log into the app on a new device, hence the trigger for a notification to be sent to a PSU would be an attempted log in not the installation itself. Furthermore, notification triggered from attempted log in would cover instances of attempted sign in through web-page too. If the trigger for a notification is in fact an attempted log in then wouldn't this be covered under Article 85 which requires SCA to be applied when the payer accesses its payment account online? IT (MS reply): **IT.** We are not sure we fully understand the proposal. To begin with, under the Italian interpretation of PSD2, the installation of a mobile banking app and its activation for payment initiation require the application of SCA, as it is considered an "*action through a remote channel which may imply a risk of payment fraud or other abuses*" [art. 97(1)(c) PSD2; soon art. 85(1)(d) PSR]. Is the proposed "additional activation step" distinct from SCA? If so, what advantages does it offer compared to applying SCA? Having said that, we have a number of doubts about this proposal. First, the proposal seems to address a specific national situation, while we are not aware that this type of fraud is relevant in Italy or in other EU countries. Secondly, we fear that the proposed solution based on an "*additional activation step*" would be too general and its overall effectiveness is questionable, given that at present frauds are typically based on deceiving the customer (phishing, scam, etc.) rather than on technology. Moreover, this solution may not be very workable: it refers to an additional activation step via SMS or WhatsApp but such channels (used to send the activation links or code) could already be used in the "normal" activation procedure or exposed to other risks (e.g. SIM SWAP). Finally, if it is decided to explore this approach in any case, we believe

Question	MS reply
	that the solution should be defined after a thorough analysis of this type of attack and should be defined not in an L1 text (being too detailed for L1), but through EBA RTS (to be drafted) or referencing available or market standards (such as Open Worldwide Application Security Project - OWASP in the mobile market). Anyway, as we expressed in previous rounds of comments, we are in favour of a real time alert system, if properly regulated. Therefore, we are in favour of the proposal to require the PSP to notify the PSU of the installation of a mobile device. LT (MS reply): We agree with the proposal. Also, alongside these additional drafting proposals we suggest including some general notions that were future-proof, i.e. directed not only specifically at mobile applications but also at any digital solutions that might be created and offered by PSPs to PSUs. Mainly, it would entail PSPs' obligation to test any new digital solution to access payment account/use payment services remotely against the threats of fraud before launching it, e.g.: 'Any changes to the procedures for the provision of payment services by PSPs, and the introduction of new services that require and use an authentication tool, should be tested prior to the entry into force of the respective updates/changes or the launch of the new services, and, from the perspective of the secure use of this authentication tool, the potential risks of fraud should be assessed and the ways to eliminate these risks should be considered and adapted.' LV (MS reply):

Question	MS reply
	We agree about additional steps. NL (MS reply): We support the proposal to enhance banking app security by requiring PSPs to have an additional activation step for using new apps, but we have a few remarks on the wording. PT (MS reply): Despite conceptually seeing no evident constraints at this time to oppose the BE approach to enhance the security of mobile applications, namely the suggested additional activation step, as foreseen in new Article 51(5a), PT believes this topic should be further debated and analysed by MS before introducing these measures in PSR, given this embodies an entirely new security domain not yet discussed that would perhaps benefit from an impact assessment to evaluate its value added, as well as possible repercussions on user experience and on PSP's service offering. We remain eager to collaborate in this regard to fully understand the pertinence of the adjustments proposed. RO (MS reply): While we agree with the intention behind this proposal, we do not find it necessary to be included in the PSR because the scenario already falls under the requirements of SCA. More specifically, in accordance with art. 85 of PSR, SCA must be applied by the PSP whenever the

Question	MS reply
	PSU carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. However, we support the notification aspect of the proposal. More specifically, we believe that there is value in having the PSP notify the PSU whenever the banking application has been enrolled to a new device, via a more traditional communication channel, such as SMS. SE (MS reply): We do not recognise a need to regulate this but do not oppose the general idea of the proposal. However, the proposal seems to be blueprinted on a procedure that we do not recognise, and we are **concerned about the level of procedural detail in the proposal,** as this may not fit the model used by Swedish banks. An additional activation step is already standard procedure when logging into a bank application, however not necessarily when installing the application onto a new device. The applications are usually generic, with no link to a specific payment account. The linking is provided on each occasion when logging into the application, by means of a separate identification application provided by the bank. Therefore, we would **suggest a more general phrasing**, see Q2. SI (MS reply): We agree. SK

Question	MS reply
	(MS reply): No strong view, but it should be based on data assessment as we should not overburden PSPs with protective measures while making the process of installation too complex for users. If PSP identifies the risk, it could take the preventive measures on its own initiative. In our view it should not be regulated in Level 1.
Q2. Do Member States agree on the wording of the proposal? Please, provide drafting suggestions.	AT (MS reply): Yes. BG (MS reply): We support the idea behind Article 51, paragraph 5b PSR. However, we believe that this would be more appropriate for an RTS. CY (MS reply): We have no comments regarding the wording of this proposal. CZ (MS reply): We do not agree with the proposal. In paragraph 5a, we wonder what the meaning of “additional step” is? Also, we are not sure what "not using the same channel" means. If the proposal would be supported by other MS, the drafting should be made clear.

Question	MS reply
	Regarding para 5b - today, the notifications are sent to the app. According to the latest security requirements it is not appropriate to force PSP to communicate by email and SMS. On paragraph 5c, it is not clear what time limit there will be. What happens in case of late notification? After that you should be prevented from using the app. DE (MS reply): Please see our preliminary comments: With regard to Art. 51 (5a): *5a. Where the payment service provider offers the **payment service user the** possibility to execute payment services by means of a mobile application, the payment service provider shall have an additional activation ~~step~~ **process** in place in the procedure for installing the **mobile** application onto ~~a~~ **each** new device. **For this purpose, the payment service provider shall send an** ~~When sending the~~ activation ~~process~~ **code or link** to the payment service user, ~~the payment service provider shall not use~~ **using** the same channel that has been used for the installation of the **mobile** application onto a new device. The data and contact information of the payer used for this communication shall be agreed in the framework contract. The payment service provider and the payment service user may agree in the framework contract on a reasonable notice period for the activation of the **mobile** application ~~**entering into force**~~ **becoming operational**.* With regard to Art. 51 (5b) 3: *The procedure for the notification as referred to in **this** paragraph ~~5~~shall be agreed between the payment service user and the payment service provider.*

Question	MS reply
	With regard to Art. 51 (5c): *Where the payment service user notifies the payment service provider that he ~~have~~ **has** not installed the mobile application linked to its payment account in accordance with the procedure as referred to in paragraph 5b, the payment service provider shall ensure that the intended mobile application does not allow to access the payment account of the payment service user nor to execute payment.* With regard to Art. 51 (5d): *Paragraphs 5**a**, 5~~d~~**b** and 5c shall be without prejudice to the right of the payment service user to deny having authorised a payment transaction.* In addition we suggest to define the terms „mobile application“ and „activation code“. The procedure of the additional activation process should be described in a recital. DK (MS reply): As above. EL (MS reply): EL: We agree with the suggestion. ES (MS reply): We agree. HR (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	It is not clear which wording this question refers to. IT (MS reply): **IT.** Please see Q1. In any case, we are not sure we fully understand the expression: "*the PSP shall not use the same channel that has been used for the installation of the application onto a new device*". Does it mean, for example, that the additional security credential cannot be sent via SMS if the customer received the app download link through the same channel? Or does it mean that the mobile device itself cannot be used to receive the additional security credential (e.g. by SMS), as it was used to install the app? LT (MS reply): Yes. In addition to, to make the proposal more clear, we would advise to include some examples of 'additional activation step' in the brackets. LV (MS reply): We agree on the wording. NL (MS reply): The proposal speaks of "the procedure for installing the application onto a new device". Note that installation of an application is always possible. The article should specify it towards the activation or logging in process of the application.

Question	MS reply
	Instead of defining the process for the secure activation of this new device, the scope of SCA can be broadened to include the activation/registration of a new device/app as the "possession" aspect of SCA. Drafting suggestion: "Where the payment service provider offers the possibility to execute payment services by means of a mobile application in which this mobile application acts as the "possession; something the user has" as part of SCA, the payment service provider shall require strong customer authentication to activate this application. ~~have an additional activation step in place in the procedure for installing the application onto a new device~~." Furthermore, PSUs should be notified if there is a login in any online banking environment from an unknown device independent of mobile or web-based interfaces. PT (MS reply): PT does not have any additional significant drafting adjustments to be considered at this time in this regard. RO (MS reply): We agree with the proposals for Art. 51 (5b), (5c) and (5d), but we consider that 5a should be deleted as the scenario is already covered by art. 85 PSR, while we can support that when a PSP

Question	MS reply
	is sending the activation process to the PSU, the PSP shall not use the same channel that has been used for the installation of the application onto a new device. SE (MS reply): We would **suggest a more general phrasing** of article 51.(5a), with less procedural detail: *"Where the payment service provider offers the possibility to execute payment services by means of a mobile application, the payment service provider shall have an additional activation step in place in the procedure for installing* ***and activating*** *the application on~~to~~ a new device.* ~~*When sending the activation process to the payment service user, the payment service provider shall not use the same channel that has been used for the installation of the application onto a new device. The data and contact information of the payer used for this communication shall be agreed in the framework contract.*~~ *The payment service provider and the payment service user may agree in the framework contract on a reasonable notice period for the activation of the application entering into force."* SI (MS reply): We agree.
Q3. Do the Member States agree on the integration of this amendment in Article 51 PSR?	AT (MS reply): Yes.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	BG (MS reply): We support the idea behind Article 51, paragraph 5b PSR. However, we believe that this would be more appropriate for an RTS. CY (MS reply): We have no comments regarding the integration of this amendment in Article 51 PSR. CZ (MS reply): No, see above. DE (MS reply): In general, yes. However, we suggest to supplement Art. 20 (d) PSR with regard to the means of communication for the additional activation process and Art. 20 (e) PSR with regard to the specific notice period for the activation of the application becoming operational. DK (MS reply): As above. EL (MS reply): EL: We agree with the suggestion to be included in article 51.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	ES (MS reply): We agree. HR (MS reply): We support the proposal. IT (MS reply): **IT.** Please see Q1. LT (MS reply): Yes. LV (MS reply): We support. NL (MS reply): We refer to our response to Q2. A part of the amendment could be achieved by broadening the scope of the SCA. PT

Question	MS reply
	(MS reply): PT does not have any additional relevant remarks at this time, highlighting our stance described in response to Q1. RO (MS reply): Partially we support the proposals as described above. SI (MS reply): We agree.
Q4. Do Member States agree on the drafting suggestion in Article 53(2)?	AT (MS reply): Yes. BG (MS reply): We agree with the Presidency's drafting suggestion. CY (MS reply): We do not oppose requesting payment service providers to use security credentials for the activation of payment instruments. CZ (MS reply): No, we do not agree even with Article 51(5a).

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	DE (MS reply): We propose the following changes to Art. 53 (2): *the payment service provider shall bear the risk of sending a payment instrument or any personalised security credentials relating to it, including* ***~~security credentials~~*** *an* ***activation code or link*** *used for the activation* ***~~procedure~~*** ***process*** *as referred to in Article 51 (5a), to the payment service user.* DK (MS reply): As above. EL (MS reply): EL: We agree with the suggestion to be included in article 53. ES (MS reply): We agree that the use of a mobile application could be compared to the use of a payment instrument, such as a card, so that the installation process could be compared to the process of sending a card. HR (MS reply): We support the proposal. IT (MS reply):

Question	MS reply
	IT. Please see Q1. LT (MS reply): Yes. LV (MS reply): We support the drafting NL (MS reply): Yes. PT (MS reply): PT understands the parallelism between securing both the PIN code for payment cards and app activation codes, and welcomes the amendment introduced in Article 53(2), if there is consensus in adopting the amendments to Article 51. RO (MS reply): In our opinion the requirements regarding the confidentiality of the security elements should be covered under the EBA mandate envisaged under Article 89 to issue RTS on authentication, communication and transaction monitoring mechanisms, and so the amendments proposed by the BE delegation should be covered accordingly into the future EBA RTS.

Question	MS reply
	If the MS agree to further develop Art 53 (2) we can support the BE proposal. SI (MS reply): We agree.
Q5. Do Member States are in favour of the possibility to agree on a cooling off period?	AT (MS reply): Yes. BG (MS reply): We support the inclusion of the possibility to agree on a cooling off period. However, we believe that this should be optional to payment service providers. CY (MS reply): We have no comments regarding the cooling off period. CZ (MS reply): There could be cases where you need to install an application on a new device very quickly, so we are afraid that in the case of a mandatory cooling off period, you could be without your working application when you need to do something with your account (e.g. send an important transaction). DE (MS reply):

Question	MS reply
	We are in general supportive of a cooling-off period in order to protect the PSU. However, we would like the PSR not to be too prescriptive and leave enough room for discretion for the PSU, in particular for non-consumer PSUs. DK (MS reply): As above. However, in case of e.g. change of mobile phone (if the old one is damaged, e.g.), a cooling off period could leave the PSU without access? EL (MS reply): EL: We support the introduction of a cooling-off period, as mentioned in our response to Q1. Additionally, we recommend complementing this measure with a notification system that informs the PSU through multiple channels (e.g., email and SMS). ES (MS reply): It can be considered to include a short cooling off period, given the punctual need of installing an application. HR (MS reply): We support the proposal. IT (MS reply): **IT.** Please see Q1.

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	LT (MS reply): Yes – moreover, (having in mind that a contract between PSP and PSU is based on standard contract terms prepared in advance by PSPs and PSUs have little to no possibility to change them) we suggest that a reasonable cooling off period should be the go-to option unless PSP and PSU agree differently in the contract. A 'reasonable' cooling-off period is necessary to give PSUs enough time to become aware of the fact that a mobile application has been created on PSUs' name and take actions to block their payment instrument. LV (MS reply): We support the inclusion of cooling off period. NL (MS reply): We support the slow banking amendment as a default option in the framework contract, but PSUs should be able to change this at any time. PT (MS reply): Despite preliminary seeing the merits of implementing cooling off periods before the activation of the banking apps, PT would welcome attempting to limit such periods to the minimum indispensable as not to hamper user experience of said apps. That reality

Question	MS reply
	must be included in the framework contract as to clearly notify the client of such occurrence. RO (MS reply): Yes, we support this initiative. SI (MS reply): We agree.
End	AT (MS reply): ***End*** BE (MS reply): ***End*** BG (MS reply): ***End*** CY (MS reply): ***End*** CZ (MS reply):

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	End DE (MS reply): ***End*** DK (MS reply): ***End*** EL (MS reply): ***End*** ES (MS reply): ***End*** FI (MS reply): ***End*** HR (MS reply): ***End*** HU (MS reply): ***End***

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

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

Presidency questionnaire following the WP meeting on 21 February 2025

From: ECB, AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, HR, HU, IE, IT, LT, LV, NL, PT, RO, SE, SI, SK **Updated: 06/03/2025**

Question	MS reply
	(MS reply): ***End*** SI (MS reply): ***End*** SK (MS reply): ***End***