Council of the European Union
General Secretariat

PUBLIC

Brussels, 03 April 2025

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

WK 4443/2025 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.

REQUEST FOR CONTRIBUTION

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 of comments to the Questionnaire on the Presidency Discussion Notes (WP on 19 March), Ddl 26 March 2025 Replies from 20 MS

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
Presidency Discussion Note on fraud prevention measures (WK 3365/25)	
Q1. Could Member States accept the proposed drafting of Article XXX and Recitals XXX, XXY and XXZ PSR?	MT (MS reply): Malta agrees with the proposed wording in Article XXX and Recitals XXX, XXY, and XXZ of the Payment Services Regulation (PSR) to establish a dedicated platform aimed at combating fraud in the area of payment services within the Union. Furthermore, Malta supports conducting appropriate consultations that actively involve the relevant stakeholders. SI (MS reply): We could accept the proposed drafting. SE (MS reply): We support initiatives on public-private cooperation in combatting crime. One important use of such cooperations is to spread knowledge and best practices between the industry and authorities and to develop common capabilities. However, the proposal focuses on **advising** the Commission, signalling a considerable focus on the role of the Commission as the central problem solver. We think the participants of the platform could be given a more active role in advising each other as well, sharing best practices and presenting initiatives and ideas of cooperation formats to combat fraud. We would therefore suggest that

Question	MS reply
	point (c) and (d) in para 2 is changed from *"~~advise the Commission on~~"* to *"share information on"*. This would signal a more active role for participants to come up with initiatives and solutions without the direct involvement of the Commission. Furthermore, it is important with flexibility to continuously develop and adapt the platform to new circumstances, and to focus its efforts to the most pressing issues currently at hand. We welcome that the latest proposal is less detailed and that the list of participants is in-exhaustive, but would prefer an even less detailed proposal. RO (MS reply): We agree with the proposed drafting of Article XXX, Recital XXX, XXY and Recital XXZ. PT (MS reply): PT broadly agrees with the text of Article XXX and the Platform's suggested mandate. However, we would prefer maintaining Article XXX(5) since, in our view, the principle of transparency should govern the Platform's work. The regular publication of the Platform's discussions and outputs may be

PUBLIC

Question	MS reply
	relevant for market stakeholders to accommodate decided best practices and emerging techniques to combat fraud. On the drafting of the Recitals, PT would only suggest the following minor amendment to Recital XXX, to avoid over reusing the same text portion, which can hamper the smooth understanding of the idea conveyed. Please consider the following adjustment: *"(XXX) (...) Consultations should build on the advice of both public- and private-sector experts who have proven knowledge and experience in the relevant areas. For that purpose, the Commission should set up a Platform on combating fraud (the 'Platform'). The Platform should be composed of experts representing* ***the referred sectors*** ~~***both the public and private sectors***~~*. (...)"* NL (MS reply): • In general we can agree with the presidency's proposals. • We previously raised the issue of participation by representatives of Member States, we are not sure whether this is clear now. Our question what the role will be of MSs in the platform still remains. We also still need further clarification on the effect and interplay of the platform on national fraud policies and strategies.

PUBLIC

Question	MS reply
	• We also believe that it is important that the work of the Platform is transparent and we would therefore be in favor of maintaining the former paragraphs 5 and 6 which state that meeting minutes/documents will be published and that the Platform will report annually to the European Parliament and Council. • The drafting proposals can be enhanced by incorporating output expectations for the platform, such as: annually publishing a public report on fraud trends and recommendations for the European Commission, attracting media attention. LV (MS reply): We support the development of such a platform and particularly welcome the idea of involving the different sectors that play an important role in reducing fraud. We do not object to the proposed versions. LT (MS reply): It is not entirely clear why the particular parts in Article XXX were removed - if this is due to the fact that these aspects of the Platform would be regulated by L2, it is fine. The crossed out parts of Article XXX define very important aspects of the Platform (e.g. 2(d) and (e) with respect to fraud prevention and, therefore,

PUBLIC

Question	MS reply
	should not be omitted completely. Other corrections are fine. IT (MS reply): We welcome the new article XXX and in particular: - there reference to the cross-sectoral cooperation; - the removal to the reference of transparency in relation to publishing the minutes of the meetings; However, as stated in our previous round of comments for the 20th January WP, we provide some suggestions in relation to the current wording. In particular: (a) in our view it would be preferable to name the platform "a forum for public-private cooperation", which better reflects the mandate of this body; (b) with reference to the members of the European System of Central Banks, it should be specified which functions would be represented (e.g. oversight); (c) with reference to PSPs (vii) and TSPs (viii), they could be represented by industry associations or sectoral CERTs, in order to ensure uniform representation of individual operators and avoid any possible conflict of interest with national competent authorities supervising these entities. So,

PUBLIC

Question	MS reply
	the wording might be "industry associations or sectoral CERTs representatives of PSPs and TSPs" (d) with respect to para. 2 (b), it should be added "Information on individual transactions shall not be shared". IE (MS reply): We support the proposed establishment of a dedicated platform on combatting fraud. Given the multi-faceted nature of fraud, a horizontal, cross-sectoral response including technology companies (search engines, social media platforms) and the payments sector, among others, is required to adequately address the fight against fraud. HU (MS reply): Yes, we agree with most of the PRES drafting suggestions. Nevertheless, we would support to reintroduce para. 6 on the annual reporting of the Platform which we deem useful. HR (MS reply): We have no particular opinion nor preference on this matter.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	FI (MS reply): FI: In principle, we have a positive stance on the suggestion. We also suggest considering the inclusion of dispute resolution bodies in the platform. We believe that especially ADR bodies could bring significant value to the group. EL (MS reply): **EL:** We fully support the proposal and the creation of a dedicated platform to combat fraud. We agree that bringing together experts, the representatives of ECSPs, consumer organizations and stakeholders involved in the fraud chain will facilitate the development of new tools to enhance fraud prevention and mitigation efforts. We also agree regarding the observatory role of the EBA in the platform. DK (MS reply): We are skeptical that the formation of such a platform would be beneficial in the fight against fraud. This is a highly dynamic area, which is much more dynamic than e.g. sustainability.

PUBLIC

Question	MS reply
	We thus do not support the proposal on Article XXX and Recitals XXX, XXY and XXZ. We find it somewhat difficult to see the advantages of having a platform, as the work could just as well take place within the EBA or the Joint Committee. DE (MS reply): • We generally support the concept and the drafting. However, we would have two important remarks: o The anti-fraud platform should not duplicate, but support the activities of other (current or future) national or European initiatives to combat fraud, in order to gain from synergies. Such collaborative set up of the platform should be enshrined in the recitals. We suggest the following drafting to Recital XXZ (changes in green): "The Platform should advise the Commission on the development, monitoring the implementation of legal acts aimed at combatting fraud in the area of payment services. The Platform should also share information on and analyse trends in fraud in the area of payment services. The Platform should advise the Commission on measures to combat fraud in the area of payments services, including mitigation measures, as well as on ways to improve

PUBLIC

Question	MS reply
	cross-border and cross-sectoral cooperation on the means of combatting fraud in the area of payment services. In its work, the Platform should take into account the work done by existing initiatives to combat payment fraud, while avoiding duplication, and cooperate with them closely." ○ We do not agree with the deletion of paragraph 6 – the duty to report annually to the EP and the Council. Both EP and the Council should be regularly informed about the work of the platform, in order to judge its effectiveness alone. The provision of paragraph 6 allows for enough flexibility in the type of reporting, so we do not consider it overly burdensome. Hence, Article XXX par. 6 should be retained. ○ It should be clarified that Union institutions, bodies, offices or agencies (e.g. Europol) taking part in the platform may contribute to its work within the limits of their respective mandates. CZ (MS reply): CZ still believes that there are already several expert groups that can address the issue of payment fraud prevention, e.g. ERPB working group on fraud, Subgroup on Payment Services (SGPS) and we also have well-functioning CEGBPI for experts from Member States. We would welcome some analyses why are these platforms not enough. Moreover, as the Commission mentioned, the Commission can establish some platform without empowerment in the proposal.

PUBLIC

Question	MS reply
	We also think that if the platform is established, it should include experts from the Member States, e. g. as observes. However, in order to find a compromise, we are flexible in creating the platform. CY (MS reply): We are supportive of the proposed drafting suggestions of Article XXX and Recitals XXX, XXY and XXZ of PSR. BE (MS reply): BE: We welcome the creation of a platform aimed at ensuring consultations and cooperation between all the actors involved on the fight against fraud. Regarding the composition, we are concerned by the observer status for NCAs. In our opinion, the participation of NCAs in the Platform would be appropriate and useful. National authorities have usually substantial experience and knowledge on the payment market and frauds that they could share with the other members of the Platform. However, we believe that the effectiveness of the discussions would be compromise if there are too many representatives around the table. We therefore suggest to integrate in PSR the possibility for Member States to designate at the national level one representative of their competent authorities as a full member of the Platform. In order to keep the representative manageable, we also suggest looking at language used in AMLA regulation where we encountered a similar issue.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	AT (MS reply): While the new drafting on Art. XXX para 1 letter b seems fine, it could still be clarified in Recital XXX that experts should, in particular, represent card schemes, merchants, providers of online platforms, telecommunication providers and internet service providers. Also, the transparency provisions in Art. XXX para 5 should be kept.
Q2. Could Member States accept the proposed drafting of Recital XX and Article 51 (1,1a,1b) PSR?	MT (MS reply): Malta also agrees with the proposed drafting of Recital XX and Article 51 (1, 1a, 1b) of the PSR, which addresses spending limits and cooling-off periods. SI (MS reply): We could accept the proposed drafting. SE (MS reply): We welcome that spending limits and cooling off periods may be used as a default. To ensure that spending limits can be used both per-day and per-transaction simultaneously, “or” should be changed to “and” in para 1. Furthermore, it

PUBLIC

Question	MS reply
	should be clarified that PSUs should be able to personalise and adjust cooling off periods if needed (*"Payment service users shall have the right to adjust or opt out of the application of a delay period."*). RO (MS reply): We agree with the proposal. PT (MS reply): PT agrees with the way forward and does not currently wish to provide additional relevant remarks. NL (MS reply): • We are happy to see that spending limits and cooling-off periods are becoming the default. • As we have often noted, this is one of the most important measures against fraud. We are more in favour of making the cool-off period obligatory, so that consumers wont opt-out easily. Consumers can be tricked easily into opting out of this, so preventive measures should be in place in case a consumer chooses to opt out.

PUBLIC

Question	MS reply
	• We also do not agree with the maximum 12-hour delay. This period does not appear to be based on data or best practices and the time period should be a minimum. • Perhaps we could make this more targeted. In practice, we most commonly see a minimum 4-hour delay period. LV (MS reply): We support the drafting proposal. LT (MS reply): We would be in favor of the proposed amendments, however, they raise doubts of their potential conflict with the requirements uof IPR. IT (MS reply): We broadly agree with the proposal, particularly with the requirement that the framework contract should establish "default" limits. However, we have the following observations. We think that paragraph (1a) should provide that the PSU shall not unilaterally *change* (and not just increase) the spending limits agreed with the PSU. We also propose that the limits should be set *at least* on a per-day and/or per-transaction basis, rather than being restricted to these alone. This approach would

PUBLIC

Question	MS reply
	ensure flexibility, allowing the parties to agree on additional limits, such as per-month limits. To eliminate any ambiguity, we should also clarify that different spending limits can be set for instant and non-instant credit transfers, as it is not necessarily clear that they qualify as distinct "means of payment". This is particularly important given that instant credit transfers have a significantly higher fraud rate. It's unclear to us whether the expression "*PSPs shall not unilaterally change the spending limits agreed with their PSUs*" is also intended to exclude the possibility of modifying the framework contract via Article 22 PSR. We would not agree with such an interpretation. In our opinion, the PSP should be able to propose "unilateral" changes to spending limits through art. 22. The proposal requires PSPs to offer PSUs the possibility of setting limits "*for each means of payment, including for credit transfers, and for each payment instrument*". However, also considering the broad definition of "payment instrument" (art. 3(18): "*device…and/or set of procedures...which enables the initiation of a payment transaction*"; see also ECJ, decision C-287/19 - *DenizBank*), this requirement could be interpreted as covering also the different channels for the initiation of payment transactions, hence forcing each PSP to implement an excessively large set of options. Moreover, the term "means of payment" is not defined, further contributing to interpretative uncertainty and potentially expanding the range of options that must be guaranteed by the PSP.

PUBLIC

Question	MS reply
	For example, there could be separate limits for credit transfers made via home banking, mobile apps, or ATMs, etc.; as well as different limits for instant credit transfers. Card payments could have different limits depending on the payment network and whether they are initiated online, at a POS terminal, or through a digital wallet, etc. Such a system would be costly for PSPs and overly complex for the PSU. A possible solution might be to allow PSUs to change (not all potential limits) but only those agreed in the contract and, at the same time, require PSPs and PSUs to agree on spending limits for all payment transactions (e.g. a general limit and additional specific limits for certain payment instruments and/or initiation channels). On the "cooling off period", we have the following observations: - We would like to know the criteria used to determine the 12-hour duration. - We would prefer that the delay be explicitly agreed upon in the framework contract. Under the current proposal, it is unclear whether and how the PSP has to disclose the length of the delay to the PSU and whether its modification would require, for example, a proposal under art. 22 PSR or if the PSP could adjust it at will and at any time. - While we understand the rationale behind requiring a "delay for opting out of the delay", we are not sure if the proposal aligns with the principle

PUBLIC

Question	MS reply
	in paragraph (1) (i.e. that the payer "*is able to modify the spending limits set prior to the placing of a payment order*"). - We should also clarify that, after opting out, the PSU retains the ability to "opt in" again. See our drafting proposal in Q3 of the Presidency Note on fraud, discussed in the WP of January 25th. See also the following amendments to the Presidency proposal in the note discussed in the WP of March 19th. *Article 51* Spending limits, blocking of the use of the payment instrument and the secure activation of a mobile application *1. The payment service user and the payment service provider shall agree in the framework contract on a limit of a maximum amount* ***for all payment transactions. These limits can be specific*** ~~*that can be sent*~~ *for each means of payment,* ~~*including for credit transfers, and*~~ *for each payment instrument* ***and for each payment initiation channel. A specific limit shall be set for instant credit transfers***. ~~*It shall be possible for the payment service user to set different limits for each means of payment and each payment instrument, which may be on a per-day or per-transaction basis, at the sole discretion of the payment service user. Payment service providers shall ensure that the payer is able to modify the spending limits set prior to the placing of a payment order*~~. ***It shall be possible for the payment service user to change each of the limits agreed between the parties***. *An increase of the spending limit by the payer, if done*

PUBLIC

Question	MS reply
	remotely, shall require the application of strong customer authentication in accordance with Article 85 (1)(d). ***[Without prejudice to article 22,] payment service providers shall not unilaterally ~~increase~~ change the spending limits agreed with their payment service users.*** *1a. ~~Payment service providers shall not unilaterally increase the spending limits agreed with their payment service users.~~ Payment service providers shall require a delay ~~of maximum 12 hours~~ for any resulting increase in spending limits to come into effect.* ***The payment service providers and the payment service user shall agree on the duration of the delay in the framework contract, which shall not exceed 12 hours.*** *Payment service users shall have the right to opt out of the application of a delay period. Where a delay period is in place, any subsequent opting out of its application shall be subject to the delay period. The opt-out shall require the application of strong customer authentication in accordance with Article 85 (1)(d).* ***Where a delay period is not in place, the payment service provider shall immediately reinstate it upon the simple request of the payment service user.*** *1b. Payment service providers shall immediately notify payment service users, in an agreed manner, when a spending limit is modified or when the opt-out referred to in the previous paragraph is exercised.*

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	IE (MS reply): We consider spending limits and cooling-off periods to be useful measures for fraud prevention. We are in favour of spending limits being optional, rather than mandatory, noting that PSUs have the option to set limits under the IPR, allowing PSPs to reject only when a PSU attempts to transact above the agreed limit. Although it could be argued that allowing a PSU the ability to choose both types of limits (per-day & per-transaction) simultaneously is means of further protection, the conflict with the IPR may lead to legal uncertainty. We also support optional cooling off periods, noting that as Recital 19 of the IPR states that PSUs should be able to modify and lift individual limits with immediate effect, the *24-hour delay* limit merits consideration and further discussion. HU (MS reply): Yes, we agree. The draft says that a notification to the PSU is required when a spending limit is modified or when the opt-out is exercised or when the mobile application is activated. We suggest that the notification to the PSU should occur through a different channel than the mobile device, if

Question	MS reply
	possible, otherwise the safeguard of the notification can be ineffective and circumvented. Drafting suggestions (written in blue): Article 51(1b) *Payment service providers shall immediately notify payment service users, ~~in an agreed manner~~ via a different channel than that of used for modifying the spending limit, when a spending limit is modified or when the opt-out referred to in the previous paragraph is exercised.* Article 51(5a) *The payment service provider shall immediately notify the payment service user ~~in an agreed manner~~ via a different channel than that of used for the activation of the application, of the activation of a mobile application linked to its payment account on a new device. The notification shall include instructions in case the payment service users have not installed the mobile application themselves.* HR (MS reply): We agree with the proposed drafting except for the possibility in the Article 51 (1a) that the PSU may opt-out from using cooling off period. The purpose of

PUBLIC

Question	MS reply
	cooling off period would have no effect if there would be a possibility for the PSUs to opt-out. FI (MS reply): FI: The provisions and the recital are moving in the right direction, and we thank the Presidency for these changes. However, we have a few remarks to be taken into account: • Article 51(1): We support the change to applying limits by default and not only "upon request of the PSU". We would still aim to clarify the provision to ensure it is clear that limits are available to PSUs both on a per-day and per-transaction basis, i.e. that one does not exclude the other. • Article 51(1a): We support the changes to the provision but have one comment. The provision now requires PSPs to apply a cooling-off period by default which we support. However, the (minimum) length of the delay is left open in the provision which, at least in principle, leads to a situation where the PSP is required to apply a delay between 0 to 12 hours. Such a possibility would make the cooling-off period practically redundant. This should be

PUBLIC

Question	MS reply
	clarified in the text, and if the PSU does not have control over the length of the delay, there should be a minimum period. • Article 51(1b): We support the suggestion but would suggest that the PSP's notification to PSU would also include an explanation of the modified spending limits. For example, adding a new sentence to Article 51(1b): "***The notification shall include an explanation on how the spending limits were modified.***" This way the PSU would be immediately aware of whether the limits have been decreased or increased, possibly by a fraudster. EL (MS reply): **EL:** We welcome the Presidency's proposed amendments and strongly support the inclusion of spending limits and cooling-off periods in the PSR as effective fraud prevention measures. We agree that these limits should be offered as default options, with PSUs having the flexibility to opt out if desired and **apply SCA when change through remote channels.** DK (MS reply): We support the introduction of spending limits and cooling off periods, which we believe can help in the fight against fraud.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	We agree that PSPs should be mandated to offer cooling off periods and spending limits as default options. The drafting suggestions seem reasonable. We also agree with the suggestions regarding daily and transaction-based limits. We do have a question for the Presidency though regarding cooling off periods. As we read the text on spending limits there is a quite significant scope for PSUs to personalize and adjust the limits. Conversely, for cooling off periods we read the text in art. 51(1a) as an obligation for the PSP to offer cooling off periods between 0 and 12 hours since the wording prescribes a maximum of 12 hours. However, here the PSU would only have the option to accept the time period that the PSP has set or opt out completely. At the same time the PSP could in principle set the cooling off period at 0 hours leaving the PSU without this protection and with no way of adjusting it. We wonder if this is the intention with the wording? Or is the wording supposed to be a minimum of 12 hours? Or is the PSU supposed to have the possibility to not only opt out but also to adjust the cooling off period. If the time period cannot be adjusted by the PSU there should probably be a lower limit as well so PSPs cannot set it at 0 hours. A second question for the Presidency regarding spending limits is that in the text describing the proposal it is mentioned that both a per-transaction

PUBLIC

Question	MS reply
	and a per-day limit should be available simultaneously for the PSU. However, in the drafting the word "or" is used, indicating that only one of the two can be used. Is this supposed to be changed? We would support this. DE (MS reply): • In general, spending limits and cooling-off periods in PSR are useful measures for fraud prevention. However, such measures come at the cost of decreasing flexibility in mandating payment transactions that need to be factored in when deciding about such measures. Therefore, we stress again the important point that the mandatory spending limits and the respective delay periods should apply to consumers only, and not to businesses. *spending limits* • In light of this trade-off we would be in favour of voluntary spending limits. At least, the setting of spending limits should be made voluntary for business PSUs, given that the urge for flexibility in mandating payment transactions of different values is even higher in the business context. Business PSUs are free to agree with their PSPs on the setting of spending limits and delay periods in framework contracts on a voluntary basis. Hence, we propose the following drafting (changes in green): Art. 51(1): "The payment service user who is a consumer and the payment service provider…" A sentence could be added to the corresponding recital:

PUBLIC

Question	MS reply
	"Payment service users who are not consumers should be free to agree in the framework contract with their payment service provider on the setting of spending limits." • Further, in terms of flexibility, the Presidency Note seems to be unclear. On one hand, it is said that spending limits should be offered as a default option with the possibility for PSU to opt out if desired. But the "opting out" is not reflected in the proposed text in Art. 51(1). There only seems to be the possibility to opt out of the delay period in Art. 51(1a), but not the spending limits in general. If Art. 51(1) is not restricted to consumers only, at least the possibility to opt out of spending limits should be clearly stipulated. Hence, we propose the following drafting (changes in green): Art. 51(1): "The payment service user and the payment service provider shall agree in the framework contract on a limit of a maximum amount that can be set for each means of payment, including for credit transfers, and for each payment instrument. The payment service user shall have the right to opt out of the setting of spending limits. …" • When it comes to the limits, the PSU should also be able to establish both kinds of limits (per-day and per-transaction) simultaneously. Hence, we propose the following drafting (changes in green): Art. 51(1): "… It shall be possible for the payment service user to set different limits for each means of payment and each payment instrument, which may be on a per-day or per-transaction basis, or both, at the sole discretion of the of the payment service user. …"

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	delay period • While we support the introduction of a delay period in general, we see the need to fine-tune the following points in Art. 51(1a): o Who decides on the length of the delay period? The text just says that the PSP shall require a delay of maximum 12h. This would also allow a delay period of 1h. Should the PSU not be able to choose a specific delay period? o There should be a minimum delay period in addition to the maximum period with minimum 6h so that the PSU can become aware of the notification and respond in good time in the event of fraud. A possibility to reduce the delay period to a few minutes could contradict the goals behind this security measure. o It is also conceivable that the maximum delay period can be extended to 24h (one working day). This allows sufficient time to prevent a possible fraud attack. A higher maximum delay period within the PSR would also have a deterrent effect on the fraudsters in advance. o How does the opting-out of the delay period work in practice? We understand that there are two kinds of opting out, one at the beginning when a delay period is established and one at a later stage when a delay period is already in place. In the latter case it is however not possible to opt out right away but only after the lapse of the delay period. As the reference to an agreement in the framework contract has been deleted,

PUBLIC

Question	MS reply
	how can the PSU opt out of the delay period in practice (is there a difference between new contracts and old contracts)? ○ We suggest to provide further explanation of the functioning of the delay period in a recital. CZ (MS reply): In general, we believe that the system of two types of limits - transaction and daily - is too difficult for PSUs. We propose to have only one daily limit. We would also like to better distinguish between the means of payment and payment instruments differ. The current wording is a bit confusing. For example, will the limits entered in online banking and the mobile app be different for credit transfers? Also we propose to delete word "sent" in 51(1): "*that can be ~~sent~~ for each*", because otherwise the limit would not be possible to use in ATM withdrawals. We also believe that there is no need for a specific reference to SCA in Article 85(1) d) PSR, as this is of course already within the scope of Article 85(1)d PSR. In Article 51 (1a) we suggest to add similiar condition as in 1., i.e. "If done remotely". Cooling-off period makes sence only in case of remote action. CY (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	We do not oppose the proposed drafting suggestion of Recital XX and Article 51 (1, 1a, 1b) PSR. BE (MS reply): We can agree with the presidency proposal. Insofar as spending limits are a significant fraud prevention measure, we are ready to consider amendments aimed at ensuring a high level of consumer protection. Regarding the length of the cooling-off period, we can agree with the maximum 12 hours timeframe, which leaves discretion to the PSPs to set out a shorter period. However, the cooling-off period should not be too short so that the PSU does not have enough time to be able to report a problem and react before the new spending limits takes effect. AT (MS reply): Yes, we agree.
Q2.1 Do Member States consider that the proposed amendments to Article 51, which are not in line with the IPR provisions, should 'override' the IPR provisions or should it be rather explicitly stated that these IPR provisions are lex specialis to the PSR provisions?	MT (MS reply): Malta is of the view that it should be clearly stated that the PSR provisions should override the Instant Payments Regulation (IPR) provisions. SI (MS reply):

PUBLIC

Question	MS reply
	As mentioned in the previous answer, we support a) the proposal to set spending limits by default by removing the reference "at the request of the PSU" in Article 51 (1) – compared to Article 5a(6) SEPA as amended by IPR that includes such a reference and b) the proposal to remove the word "either" – compared to Article 5a(6) SEPA as amended by IPR that includes such a word. We agree that the removal of this word may improve the consumer choice with regard to spending limits. Consequently, this means that there could be a potential conflict between Article 51 PSR and provisions introduced by the IPR in the SEPA Regulation. In order to avoid any doubts, we suggest specifying directly in the PSR that the PSR is to be used in these cases and not the IPR. SE (MS reply): Yes, the cooling off provisions in article 51 should override the IPR provisions. RO (MS reply): We consider that the proposed amendments of Article 51 PSR should override the respective IPR provisions since PSR should be considered lex specialis. PT (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	PT's interpretation of the proposed amendments to Article 51 PSR and the IPR provisions covering the subjects of spending limits and cooling off periods do not envisage a strong contradictory sense between the spirit of both files. On the setting of spending limits, Article 5a(6) of the SEPA Regulation, inserted by the IPR, states the PSP should offer the PSU, upon its request, the possibility of setting transactional or daily limits. That voluntary capability is still preserved with the proposed Article 51(1), since, without prejudice to a preliminary limit being agreed upfront in the framework contract, PSU remains fully capable to freely request different limit adoptions at any time, as intended by Article 5a(6). Moreover, surrounding cooling off periods, we recognize that Recital 19 IPR underscores that limit modification should occur with immediate effect. Nevertheless, the COM's Q&As on IPR implementation (Q68) admits PSU can decide, if the service is available, to request a delayed effect of the newly set spending limit, on a contractual/bilateral basis, which could ultimately be the framework contract. The possible discrepancy here can the detail the IPR may foresee an opt-in approach, compared with a default adoption of PSR, as previewed in Article 51(1a). As to the opt-out, IPR tends to favour immediate lifting of cooling off periods, scenario barred in Article 51(1a).

PUBLIC

Question	MS reply
	Therefore, to ensure maximum legal clarity and certainty, and since PT understands the value added of the PRES PL provisions to enhance client security, namely on the setting of cooling off periods, we would be willing to support highlighting PSR provisions should override the IPR stance on this issue. NL (MS reply): The PSR provisions should override the IPR provisions and this should be stated. Otherwise the IPR will (as lex specialis) override the PSR (as lex generalis) and the changes to Article 51 will then be useless. LV (MS reply): We support legal certainty and explicitly state that these IPR provisions are *lex specialis* to the PSR provisions. LT (MS reply): If proposed amendments to Article 51 'override' IPR provisions, with which they are not in line with, it would signify greater consumer protection from fraud. However, we are not convinced this could be possible from a legal standpoint. Therefore, IPR provisions should be deemed as *lex specialis* to the PSR provisions.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	IT (MS reply): In our view, it is necessary to align the IPR with the PSR to avoid two different and potentially conflicting regimes. The simplest solution would be to delete Art. 5a(6) IPR. In our view, the revised wording of Article 51 fully addresses the underlying objectives of Article 5a(6) while also providing enhanced security for the PSU (particularly important in the case of instant credit transfers, given the higher fraud rate). We propose the following Art. 110a: *(NEW) Article 110a - Amendments to Regulation (EU) No 260/2012* *Art. 5a(6) of Regulation (EU) No 260/2012 is deleted.* IE (MS reply): It is of the utmost importance that any potential conflict between Article 51 PSR and provisions introduced by the IPR in the SEPA Regulation are avoided in the interests of consistency and legal certainty. HU (MS reply): In order to ensure coherence between the two pieces of legislation, we believe that the later, more thoroughly revised payment rules should prevail, i.e. the content of the PSR should override the earlier IPR in

PUBLIC

Question	MS reply
	terms of the provisions restricting and prohibiting the use of cash substitutes. HR (MS reply): In our opinion, the proposed amendments to the Article 51 of PSR should "*override"* the IPR provisions. FI (MS reply): FI: Yes, the proposed PSR provisions should override the IPR provisions. EL (MS reply): EL: Article 51 should "override" the IPR provisions. DK (MS reply): We believe it should be explicitly stated how these two regulations interact (without using the term “lex specialis”). DE (MS reply): • We favour the inclusion of a clarifying sentence stating that the respective provisions in Article 51 shall prevail the IPR provisions. CZ (MS reply):

PUBLIC

Question	MS reply
	The general rule is that SEPA (IPR) is a lex specialis to PSR. Provided that 51 PSR should prevail over IPR we prefer to clearly state it in the regulation (IPR or PSR). CY (MS reply): We have no comments. BE (MS reply): BE: We understand that some Member States see inconsistencies with IPR. In our opinion, IPR (in Article 5a, paragraph 6) could be detrimental to the fight against fraud by hindering the establishment of effective spending limits that fraudsters cannot easily bypass. We should be able to overrule IPR via Article 51 of PSR. In this sense, IPR should not be seen as a lex specialis and PSR should apply to instant payment. AT (MS reply): In order to avoid confusion among PSUs (and cater for the even higher risk sensitivity of instant payments), the proposed amendments to Art 51 should override the corresponding IPR provisions and therefore also be applicable to instant payments.
Q3. Would Member States support the proposed drafting of Article 51(5, 5a, 5b, 5c)? If not, please provide drafting suggestions.?	MT (MS reply):

Question	MS reply
	Malta is in agreement with the proposed drafting of Article 51 (5), (5a), (5b), and (5c) of the PSR concerning the security measures for the installation of a mobile application. SI (MS reply): We support the proposed drafting. SE (MS reply): We welcome that the article has been amended with a more general wording directed at the activation of the application. Generally, we support the proposal but are open to discuss something more technique neutral or level 2 regulation. Perhaps a more general term could be considered instead of *"mobile application"*. RO (MS reply): We support the intention of the proposal. However, similarly to the requirements set out in the proposal for Article 51 (1a), we would like to add that where a delay period is in place, any subsequent opting out of its application should be subject to the delay period. Therefore, we propose the following wording for article 51 (5): *"5. Where the payment service provider offers the payment service user the possibility to execute payment services by means of a mobile application,*

PUBLIC

PUBLIC

Question	MS reply
	the payment service provider shall require strong customer authentication to activate the application on a new device *The payment service provider shall require a delay for the activation of the application to take effect. The payment service user shall have the right to opt out of the application of such a delay period.* ***Where a delay period is in place, any subsequent opting out of its application shall be subject to the delay period****. The opt-out shall require the application of strong customer authentication in accordance with Article 85 (1)(d).”* PT (MS reply): PT agrees with the suggested way forward but would advise the delay for the activation of the application to take effect, mentioned in the 2nd paragraph of Article 51(5), should specify the same reasonable time horizon of 12 hours maximum as presented in Article 51(1a), for the sake of consistency. Further harmonisation with the latter Article might be envisioned as to also state subsequent opting out is subject to the delay period. Please consider the following adjustment: *“The payment service provider shall require a delay* ***of maximum 12 hours*** *for the activation of the application to take effect. The payment service user shall have the right to opt out of the application of such a delay period.* ***Where a delay period is in***

PUBLIC

Question	MS reply
	place, any subsequent opting out of its application shall be subject to the delay period*. The opt-out shall require the application of strong customer authentication in accordance with Article 85 (1)(d).”* NL (MS reply): Yes. LV (MS reply): In general, we could support, but there is still a confusion regarding those consumers that are not familiar with mobile applications, use mobile devices that do not support specific applications. LT (MS reply): We support. IT (MS reply): We have no objections to the revised proposal, as it is in line with our observations on the BE non-paper. We suggest to specify the maximum length of the delay, in line with the proposal regarding the delay for the spending limit increases, and to require that the delay be explicitly agreed upon in the framework contract (see our answer to Q2).

PUBLIC

Question	MS reply
	We therefore propose to amend art. 51(5) as follows: *5. 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 require strong customer authentication to activate the application on a new device.* *The payment service provider shall require a delay for the activation of the application to take effect.* ***The payment service providers and the payment service user shall agree on the duration of the delay in the framework contract, which shall not exceed 12 hours.*** *The payment service user shall have the right to opt out of the application of such a delay period. The opt-out shall require the application of strong customer authentication in accordance with Article 85 (1)(d).* IE (MS reply): We have no objection in principle to enhancing the security of mobile applications in the fight against fraud but is mindful of balancing such measures against cumbersome and unworkable processes for PSUs, particularly as regards accessibility. HU (MS reply):

PUBLIC

Question	MS reply
	Yes, we agree. HR (MS reply): We agree with the proposed drafting except for the proposal in Article 51, paragraph 5 regulating that the payment service user shall have the right to opt out of the application of such a delay period. In our opinion, such opt out would only be acceptable if it was confirmed in direct communication with the payment service user. FI (MS reply): FI: As previously mentioned, we are supportive of the proposal in general as such measures could be useful from a fraud prevention point of view. We have the following remarks on the drafting suggestions: • Article 51(5): Would the length of the delay be decided by the PSP? Some guidance on this would be useful for clarity. • Article 51(5a) and (5b): Preliminarily support. EL (MS reply): **EL:** We strongly support the proposed measures, as they align with recommendations we have put forward in previous rounds of comments. In

PUBLIC

Question	MS reply
	fact, we have already taken steps to encourage PSPs in Greece to adopt these security enhancements for their mobile applications, and they have proven to be effective. We agree that the focus should be on the activation or login process rather than merely the installation of an application, as this is the critical stage where security measures should be enforced. In addition, as we have also emphasized in previous discussions, we recommend the introduction of an enhanced notification system, where PSPs send periodic alerts to inform PSUs about an upcoming device activation. These notifications should be sent between the initial SCA registration of the device and the actual completion of activation, providing an additional layer of awareness and security for users. Furthermore, we propose introducing a limit on the number of registered devices per user for PSP mobile applications or alternatively allowing users to designate a single "master device," through which approval for the registration of additional devices would be required. These measures have proven highly effective among Greek PSPs in enhancing the security of device registration. However, we believe that including such provisions in L2 rather than L1 would be more appropriate, as this would ensure both flexibility in implementation and the ability to update them more frequently in response to evolving scams.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	DK (MS reply): We can support the proposals for article 51(5, 5a, 5b, 5c). We note that the requirements have been worded with a degree of flexibility to allow PSPs to adapt to an everchanging environment. We believe it is important that solutions made in accordance with the eIDAS2-regulation can be used for the purpose of this extra security step. DE (MS reply): • The provision stipulates another obligation for PSPs in the area of fraud prevention. In the context of a balanced compromise, GER could, in general, show flexibility on this provision. However, we should be very careful when continuing to extend the catalogue of obligations to PSPs too much, as all of those obligations will increase bureaucracy (against the current agenda of simplification) and are associated with compliance costs that in sum result in significant burdens, especially for small or medium PSPs. CZ (MS reply): The transaction is not executed through the application, but is **initiated through** the application. Therefore, we do not agree with the wording: "to execute payment services by means".

Question	MS reply
	We also believe that there is no need for a specific reference to SCA, as this is of course already within the scope of Article 85(1) d) PSR. Article 51(5) should contain reference to a delay period. E. g. similar sentence which is in Article 55(1a): "Where a delay period is in place, any subsequent opting out of its application shall be subject to the delay period." In 51(5b) there should be a time limit - e. g. "without undue delay (or immediately) after notification by the user". We also would like to question if this provision is really necessary. To the same effect leads the already existing general duty to block a payment instrument, if a user notifies its possible misuse. CY (MS reply): We are supportive of the proposed drafting suggestion of Article 51(5, 5a, 5b, 5c). BE (MS reply): BE: Based on the written comments of Member States sent to the Presidency after the meeting of 21st February, we note some support for our proposal, although at the same time we also observe that many Member States reported the need to further modify the proposed provisions.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	A few Member States found that it is not necessary for the proposal to be included in the PSR, arguing that the scenario already fell under the requirements of the SCA in Article 85. Another Member State suggested that instead of defining the process for the secure activation of this new device, the scope of SCA could be broadened to include the activation of a new device/application as the 'possession' aspect of SCA. We would like to point out 2 important elements of our proposal. Firstly, it is important in our view to have two steps using SCA for the installation and activation of a banking application. One step for the installation of the app and the connexion with the payment account, and one another step for the activation of the app. The two steps should require the application of SCA in accordance with Article 85. Nevertheless, the requirement to have these two steps is not reflected in Article 85. Secondly, the SCA at each step should take place in a different way, using 2 different communication channels, in order to ensure as far as possible that it is the PSU who is carrying out the procedure and not a fraudster. The activation step should be seen as a second safety net in the event that the fraudster manages to hijack the communication channel used to install the app and connect it to the PSU's account.

PUBLIC

Question	MS reply
	For these reasons, we proposed to explicitly include in Article 51 PSR a requirement for PSPs to have two steps using SCA for the installation and the activation of an application allowing the PSU to access its payment account and to make payment transactions. Moreover, we would like to emphasise that in our view, payment transactions executed through a banking application on a smartphone should be considered as payment transaction requiring SCA in accordance with Article 85 PSR. The "possession" aspect of SCA is the application on the PSU's device and the "knowledge" aspect of the SCA is the PIN code for enter the app and confirm the payment transaction. We also noticed that some Member States were of the opinion that our drafting suggestion is too detailed and should be more general and futureproof, or otherwise not included in L1, but rather in EBA RTS. We can understand these arguments. We could amend the proposal to leave more space and flexibility in the choice of the channel used for the procedure. In this sense, the text could be futureproof and technologically neutral and could leave discretion for the PSPs in implementing the installation and activation process of their applications. This could also prevent any undermining of similar initiatives that already exist in certain Member States.

PUBLIC

Question	MS reply
	However, we still prefer to have in PSR an explicit obligation for the PSP to have such installation and activation procedure in place, using two different communication channels, insofar as we do not think that such requirement could be only on RTS. We therefore suggest to amend our proposal in order to remove unnecessary details that may be in a level 2 text or left the discretion of PSPs or Member States. Finaly, we see a general support for the notification requirement. We also see some support for introducing a cooling-off period with regard to the activation of the banking application on a new device, but more as an option than as a mandatory measure. We would like to add that in our view, the decision to opt-out from the application of the cooling-off period should be taken before the installation procedure and not during the installation procedure, so as not to allow the fraudster to withdraw the cooling-off period by themself. We also noticed that our proposal regarding Article 53 (2) PSR has not been commented on by the Member States. However this is not longer included in the Presidency's proposal. We welcome the drafting suggestions made by the Presidency and by some Member States. Based on these suggestions, we amended our proposal as followed. Since we removed unnecessary details from the suggested text of Article 51, we can consider to have a recital containing further explanations and

PUBLIC

Question	MS reply
	examples (we already prepared a draft proposal if this solution is welcomed by Member States). We also moved paragraph 5d of our initial proposal (regarding the right of the PSU to deny having authorised a payment transaction) in the recital to lighten the text of Article 51. We started from our initial proposal and amend it taken into account the Presidency proposal and some drafting suggestions made by Member States following the meeting of February. The newly-introduced amendments are in red. ***Recital XX*** *As payment services become increasingly digital, many payment service providers are offering payment service users the possibility to use mobile applications to carry out payment services. While these mobile applications are useful and beneficial to PSU, they also present a risk in terms of fraud. Fraudsters can use these applications to easily access their victims' payment accounts. In order to prevent such risk, payment service providers should have two steps in place in the procedure for installing and activating the mobile application on a new device. The installation process and the activation process should require the application of strong customer authentication in accordance with Article 85 (1)(d). When sending the activation code or links to the payment service user, the payment service provider should use a different communication channel from the communication channel that have been used for the installation of the mobile application on a new device. This is aimed at preventing the activation codes or links from being sent to the fraudster in the case where the fraudster misappropriated the payment service user's security credentials and communication channel used for the first installation step. For example, the activation security credential should not be sent to the payment service user by SMS if the payment service user received the security credential for installing the*

PUBLIC

Question	MS reply
	mobile application and connecting it to its payment account through this same channel. *The payment service provider and the payment service user should agree on a delay for the activation of the application to take effect in order to allow the payment service user to intervene if they are not the one who carry out the installation and activation of the mobile application. The payment service user should have the right to opt out from the application of such a delay period. The decision to opt-out from the application of the delay period should require the application of strong customer authentication in accordance with Article 85 (1)(d) and should be agreed by the payment service user before any installation of a mobile application.* *The payment service provider should also notify the payment service user in a safety manner of the activation of a mobile application linked to its payment account on a new device. The notification is aimed at increasing the vigilance of the payment service user and should allow the payment service user to alert the payment service provider if they have not install the mobile application themself. In this case, the payment service provider should ensure that the intended mobile application does not make it possible to access the payment account of the payment service user or to execute payment transactions.* *The communication data used for the activation procedure and for the notification should be agreed in the framework contract.* *While such measures enhance security, it will never completely eliminate fraud. Like payment services, fraud methods are evolving quickly and becoming increasingly sophisticated. Therefore, these measures should be without prejudice to the right of the payment service user to deny having authorised a payment transaction.*

PUBLIC

Question	MS reply
	Article 51. Spending limits, blocking of the use of the payment instrument and the secure activation of a mobile application *[...]* *5. 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 and activating the mobile application on ~~a~~ each new device. The process for installing the mobile application and the process for activate the mobile application shall require the application of strong customer authentication in accordance with Article 85 (1)(d).* *For this purpose, the payment service provider shall send the activation security credentials ~~When sending the activation process~~ 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~~ on a new device. The data and contact information of the payer used for this ~~communication~~ purpose 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.~~* *The payment service provider shall require a delay for the activation of the application to take effect. The payment service user shall have the right to opt out of the application of such a delay period. The opt-out shall require the application of strong customer authentication in accordance with Article 85 (1)(d).* *5a. The payment service provider shall immediately notify the payment service user of the ~~installation~~ activation of a mobile application linked to its payment account ~~onto~~ on a new device. ~~The notification shall be sent to the payment service user in a safety manner by using mobile phone number or e-mail address provided~~*

PUBLIC

Question	MS reply
	~~*by the payment service user.*~~ *The notification shall include instructions in case the payment service users have not installed the mobile application themselves.* *The procedure for the notification referred to in this paragraph* ~~*5*~~ *shall be agreed between the payment service user and the payment service provider.* *5b. Where the payment service user notifies the payment service provider that they have not installed and activated the mobile application linked to their payment account in accordance with the procedure* ~~*as*~~ *referred to in paragraph 5a, the payment service provider shall ensure that the intended mobile application does not* ~~*allow*~~ *make it possible to access the payment account of the payment service user or to execute payment transactions.* *5c.* ~~*Paragraphs 5, 5a and 5b shall be are without prejudice to the right of the payment service user to deny having authorised a payment transaction.*~~ ***Article 53*** ***Obligations of the payment service provider in relation to payment instruments*** *1. […]* *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 used for the installation and activation procedure as referred to in Article 51 (5), to the payment service user.* AT (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	Yes.
Q4. Could Member States accept the proposed amended drafting of Recital 69d and Article 69(2a) PSR?	MT (MS reply): Malta agrees with such amendments. However, Malta requests further clarification on how the process will unfold in the case of an instant payment. Specifically, if a payer's payment service provider (PSP) has executed an instant payment order and debited the payer's account, but the payee's PSP has not credited the payee's account due to reasonable grounds of suspected fraud, what notification should the payer's PSP receive in such a scenario? Given that the payer's PSP would have already processed the payment order, should it be informed that the funds have been sent but are currently "on hold" and have not yet been credited to the payee's PSP? If in the affirmative, Malta is of the view that this should be clearly outlined in the text. SI (MS reply): We could accept the proposed drafting. SE (MS reply):

PUBLIC

Question	MS reply
	We support the proposal on freezing of funds and welcome that the proposal now also refers to other relevant information, not just TMM. RO (MS reply): We agree with the proposals and strongly support the provisions developing the adequate instruments available to the payee's PSP in order to efficiently react based on the TMM results or on any relevant information available to the payment service provider, where are reasonable grounds to suspect a fraudulent payment transaction. We also strongly support the provisions of article 69 (2a) stipulating the possibility for the *payee's payment service provider* to return the funds to the payer's payment service provider, in case the transaction is deemed fraudulent. We also support to have an efficient and transparent notification process from the payee's payment service provider to the payer's payment service provider, and also adequate channels for informing on the assessment that is being conducted by the payee's payment service provider. PT (MS reply): PT agrees with the amendments introduced in Article 69(2a) PSR and cherish the adopted maximum of two working days for the Payee's PSP analysis to take place and the necessity to notify the payer's PSP. On Recital 69d, and as previously highlighted, we disagree with the inclusion of the last sentence since, in our view, expectations in this regard may be dependent on each case and ultimately the courts' intake

PUBLIC

Question	MS reply
	should be expected to be a decisive factor. Additionally, a full liability exemption for PSP may stimulate the usage of these new mechanisms beyond the strictly necessary. Please consider the following adjustment: *"(69d) (...)* ***~~Where the payment service provider has duly justified and reasonable grounds to suspect fraud, a refusal in good faith to execute or the decision to block or postpone a payment transaction should not involve the payment service provider in liability.~~***<*"* NL (MS reply): • We are concerned about the explicit exclusion of the PSP's liability in recital (69d), thereby removing the option for PSUs who incurred financial damages due to unjustified blocking or postponing of payment transactions, to seek compensation through ADR bodies or national courts. We suggest not to exclude the PSP's liability explicitly in the text. It seems to us that the PSP always has the possibility to deny PSUs unjustified claims to compensation through ADR or national courts. • "Without undue delay" should be adequate, as there is a risk that close to 2 days could become the standard for the 'effective'

PUBLIC

Question	MS reply
	maximum execution time including the freezing of funds investigation. • This may affect the efficiency of payments, particularly due to potential divergence with instant credit transfers in terms of timing. • A maximum of one business day would be more appropriate, aligning closely with the maximum execution time for a credit transfer. • At the same time the PSP should be able to conduct an investigation in this time period, so a provision on response time period between the payers and payees PSP could help in this regard. LV (MS reply): We support the proposal. LT (MS reply): We accept. IT (MS reply):

PUBLIC

Question	MS reply
	We broadly agree with the proposal on Art. 69(2a). We agree that the payee's PSP should inform the payer's PSP. In our view, the blocking of a suspicious transaction by both the payer's PSP and the payee's PSP should follow the same fundamental approach. In order to resolve the suspicion, the payer's PSP should contact the payer and the payee's PSP should contact the payer's PSP; conduct an assessment without undue delay, and, in any case, reach a final decision on whether to proceed with the transaction within a set maximum timeframe. The payee's PSP should immediately inform the payer's PSP of its decision. IE (MS reply): It is important that the proposal is balanced in order to prevent non-execution of transactions by PSPs being the default position. There is a risk that what is proposed could adversely affect consumers by causing unnecessary delays to legitimate payments, preventing consumers from accessing fast and reliable payment services. A non-exhaustive list of examples of what comprises "any relevant information" could be included in Recital 69d. We query the origin of the proposed timeframe "…maximum of two working days" in Article 69(2a). HU (MS reply):

PUBLIC

Question	MS reply
	Yes. HR (MS reply): In our opinion, in Article 69(2a) the timeframe of two working days for the payee's payment service provider to ascertain whether the transaction is in fact fraudulent is not long enough, and at least four days should be given instead. Also, in the same Article, in our opinion, funds should not be returned to the payer's PSP before a court or FIU decision is obtained. FI (MS reply): FI: The recital and the provision are going into right direction. We still have a few technical remarks: • Recital 69d: It would be useful to clarify the sentence mentioning that "*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*" by including some examples where these grounds are fulfilled. Also, we would suggest fine-tuning the last sentence as follows: "*Where the payment service*

PUBLIC

Question	MS reply
	provider has duly justified and reasonable grounds to suspect fraud, a refusal in good faith to execute or ~~*the*~~***a*** *decision* ***to postpone a payment transaction or*** *to block* ***a payment instrument*** ~~*or postpone a payment transaction*~~ *should not involve the payment service provider in liability* ~~*of any kind*~~*.*" • Article 69(2a): We support the proposal and thank the Presidency for the amendments. EL (MS reply): **EL:** We accept the amendments in both recital 69d and article 69(2a). DK (MS reply): We generally support the amendments made to recital support 69d and Article 69(2a) PSR. We are happy to see the addition of a reference to other relevant information as a legitimate reason for the freezing of funds as well. However, while we can follow the logic of introducing a timeframe for the freezing, we are not sure whether 2 days would be sufficient. And in case the funds are released, and it was fraud, this would be an extremely unfortunate situation. DE (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	• We support, in general, additional fraud prevention tools for the payee's PSP in case of suspicion of fraud, e.g. the possibility to "freeze" incoming transactions and generally agree with the clarifying drafting suggestions to R69d and Article 69(2a) PSR. • However, the proposal of Art. 65(1a) as it stands raises significant questions with regard to Art. 22 GDPR. • In particular, it seems that the freezing would be based on an automated decision within the meaning of Art. 22 para. 1 GDPR, which is generally prohibited. In this case, the question arises, which exception under Art. 22 para. 2 GDPR should be used as the basis for automated decision-making, in particular whether an exception within the meaning of Art. 22 para. 2 letter b GDPR should be made here. However, this would then require "appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subjects". • Has the PCY or the COM assessed the interplay with GDPR? If so, it would be very important for us to see such assessment before deciding out such provision. Having a clear and legally sound provision here should be in our common interest. CZ (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	We would like to know what it means **not to make funds available**, whether funds are credited to payee's account and cannot be used, or whether they are not credited at all and then the execution time is not met. CY (MS reply): We are supportive of the proposed amended drafting of Article 69(2a) PSR. BE (MS reply): BE: we can agree with the drafting suggestions. AT (MS reply): Yes.
Q4.1 Do Member States see the need to include similar timeframe on the payer's PSP side with regard to transaction blocking?	MT (MS reply): Malta agrees in principle to have a similar timeframe for the payer's PSP. However, Malta kindly requests the same clarifications as outlined above regarding the message that the payer's PSP should send to the payer in such scenarios. Furthermore, Malta queries whether this will create potential confusion for payment service users. Specifically, if the payer chooses to complete the

Question	MS reply
	payment through an alternative channel or instrument, what will happen if the payer's PSP later determines that no fraud was involved, and the payment is subsequently processed automatically? SI (MS reply): / SE (MS reply): We are hesitant towards setting specific time frames in level 1, as these are difficult to calibrate. RO (MS reply): Yes, we support the setting out of a ***similar timeframe on the payer's PSP side with regard to transaction blocking*** that can be beneficial in our opinion due to the fact that it will act as an additional instrument for blocking potential fraudulent payment transactions, and also as an incentive for PSPs to maintain and/or develop efficient communication systems and channels with the PSU. PT (MS reply):

PUBLIC

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	PT supports adopting a similar time frame on the payer's PSP side, considering the previously manifested concerns regarding possible permanent blocking of the funds, which can lead to risks for the regular functioning of payments and to the PSUs' confidence in the payment system. NL (MS reply): See our reaction to question 4. LV (MS reply): We support the proposal. LT (MS reply): Yes (in fact, it is often the case - payer's PSP has reasonable grounds to suspect fraud, however, under PSD2, the possibility to block such transaction or to refuse to execute it is not granted). IT (MS reply): See our previous answer. IE

PUBLIC

Question	MS reply
	(MS reply): It appears logical that if there is a timeframe applied to payee PSPs that an equivalent timeframe should be applied to payer PSPs in the event that they block a transaction. HU (MS reply): Yes, it would be useful to provide similar (or same) timeframe on the payer's PSP side. HR (MS reply): It is not clear what is proposed in this context i.e., what specific situation is covered by this proposal. EL (MS reply): EL: We think it's essential to have a similar timeline on the payer's PSP side. DK (MS reply): As with the timeframe for the freezing of funds, we are not sure whether 2 days would be sufficient with regard to transaction blocking. DE

PUBLIC

Question	MS reply
	(MS reply): • In general, we would support clarifying the timeframe on the payer's PSP side with regard the refusal to execute the transaction (Art. 65(1a)). • In this context, we already asked before about the meaning of the wording "without prejudice to Art. 69 (1)" in Art. 65(1a), subparagraph 3. Does this mean that the PSP would have to contact the PSU to ask for further information and make a final decision whether or not to execute the payment transaction within the time period set out in Art. 69(1) "by the end of the following business day"? • A reference to the time period in Art. 69(1) is also included in Art. 65(2) when it comes to notifying the payer about the refusal to-execute the payment transaction. We suggest to clarify the time periods/timeframe in context of the refusal to execute a transaction in order to ensure legal certainty. CZ (MS reply): There should be a provision for informing the payee. The payer will claim that the money has been transferred, but the payee will still not see it on the balance. Often this can be a problem in trade between physical persons and this delay can lead to undesirable consequences (e.g. buying in a bazaar tickets for a sports match, a ski pass, where a delay of two working days can mean that it will be too late). CY (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	We have no comments. BE (MS reply): BE: We see an added value in setting a timeframe on the PSP as it could prevent any unnecessary transaction blocking or funds freezing in legitimate cases. AT (MS reply): The current requirements seem sufficient to us
Q5. Could Member States accept the wording of Articles 51(2) and 65(1a, 2) PSR?	MT (MS reply): Malta agrees with the wording outlined in Articles 51(2) and 65(1a) and (2) on the blocking of the use of the payment instrument and refusal to execute a payment order in the event of reasonable grounds to suspect fraud. SI (MS reply): We would rather keep previous wording of Article 51 (2), however we could also support deleting the last sentence. SE (MS reply): We generally welcome the amendments, but agree with the Finnish delegation that the word “and” should be changed to “or” regarding the reference to

PUBLIC

Question	MS reply
	"transaction monitoring mechanism *and* any other relevant information" as valid reasons for blocking. Furthermore, we agree with the Romanian delegation that the reference to instant credit transfers in article 65(2) should apply to all MS currencies, not just the euro. RO (MS reply): We agree with the proposal set out in ***Articles 51(2) and 65(1a, 2) PSR***. However, while we agree with the general wording of Article 65 (2) PSR, as a noneuro area MS we would like to emphasise that the notification of the refusal in case of *instant credit transfers should apply to all MS currencies and not only to euro, considering the principle of PSD3/PSR application.* In our opinion considering that for some MS, if for different legal reason the *instant credit transfers is implemented for a currency of a MS other than euro*, those payment transaction should be in the scope defined under Article 2 (3) of the PSR. Therefore, we propose the following wording for Article 65 (2) PSR: *65 (2.) – The payment service provider shall provide or make available the notification in an agreed manner ~~at the earliest opportunity~~ and without undue delay, and in any case within the periods specified in Article 69. In the case of instant credit transfers ~~in euro~~, the payer's payment service provider shall provide or make available the notification of the refusal within 10 seconds of the time of receipt of the payment order by the payer's payment service provider, and provide the reasons for the refusal without undue delay, unless prohibited by other relevant Union or national law.*

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	PT (MS reply): PT agrees with the way forward but would like to underscore the need to clarify what is meant by "any other information available to the payment service provider" on Article 65(1a), namely the sources of such information. NL (MS reply): We think that the de-risking concerns are still valid here. There is a balance to be considered between safety and efficiency, and it is important to discuss how to achieve this balance and address de-risking concerns. The deletion of the last sentence in paragraph 2 in art. 61a could lead to excessive derisking. We also have difficulty following the proposed amendments to Article 65(1a) as regards instant credit transfers. We appreciate the argumentation provided by the Presidency, explaining that certain obligations cannot be imposed on the PSP in the case of instant credit transfers, due to the time limit of 10 seconds. This argumentation supports the exemption from providing the reasons for the refusal to execute a payment order or to initiate a payment transaction, as proposed in Article 65(2). At the same time, Article 65(2), rightly, does oblige the PSP, in the case of instant credit transfers, to provide or make available the notification

PUBLIC

Question	MS reply
	of the refusal within 10 seconds. Why is it therefore necessary to exclude the obligation for the PSP to notify the PSU in case of reasonable grounds to suspect that the transaction is fraudulent, as proposed in Article 65(1a), fourth sub-paragraph? Why do we expect the PSP to be able to provide one notification (Article 65(2)) and not the other (Article 65(1a)) in the case of instant credit transfers? LV (MS reply): We support the proposal. LT (MS reply): Yes. IT (MS reply): We reiterate our previous comments to underline that there are some inconsistencies between recital 69e and articles 51, par. 3 and 65, par. 2. While the first contains a clear reference to the prohibition of disclosure laid down in art. 73 AMLR, the latter only make a general reference to prohibition by other relevant Union or national law. It would be opportune to align these provisions and to insert a clearer reference to art. 73 also in both articles 51, par. 3 and 65, par. 2.

PUBLIC

Question	MS reply
	In the same way, we advocate for a specific reference to art. 71 AMLR in art. 65, par. 1, PSR, instead of the general reference to prohibition by other relevant Union or national law. Moreover, the proposed version of art. 65, par. 1a, PSR, which provides for the obligation to refuse to execute the operation, could rise application conflicts with art. 71 AMLR, which consent to execute the operation after submitting the STR. Please also see our comments and drafting proposals in the "Consolidated Tables PSR" with regard to Articles 51, par. 3 and 65, par. 2, in relation to cross-references to AMLR. We note that the expression "unauthorised or fraudulent use" (already used by the PSD2) is so broad that it could encompass transactions that are not classified as "unauthorised" and therefore would not fall under the PSP's liability under Art. 56 (or, in any case, under Art. 59, if retained). In other words, there are transactions that may be considered as "fraudulent" but not "unauthorized": for instance, a fraud involving the "underlying reasons" of a transaction (e.g. romance scam) could still be deemed "fraudulent" for the purpose of blocking a payment instrument, but would not be classified as "unauthorized" for the purpose of the PSP's liability.

PUBLIC

Question	MS reply
	Even though PSPs should not bear liability in such cases, we think they should still have the ability to block the instrument (and contact the PSU), as this measure enhances PSUs protection. We have some reservations about the wording of Art. 65(1a), third subparagraph, which requires the PSP to notify the payer only when the payer is suspected of being "a victim of fraud". The first subparagraph was amended from "*grounds to suspect fraud against the PSU*" to "*grounds to suspect that the transaction is fraudulent*", in order to cover cases where the PSU act as an accomplice to the fraudster (e.g. money mule). The same rationale should apply to the third subparagraph. Moreover, the same Article states that the PSP shall attempt to contact the PSU and shall notify the payer of the refusal and its reasons. IE (MS reply): We would be of the opinion that blocking of the use of the payment instrument and refusal to execute a payment order should be mandatory in certain circumstances (such as for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument) and not only '*if agreed in the framework contract'*.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	HU (MS reply): Yes, we agree. Please note that the second subparagraph of Article 65(2) refers to 'instant credit transfers in euro' while the 4th and 5th subparagraphs in Article 65(1a) makes an exemption for 'instant credit transfers' in general. We are of the view that the mentioned subparagraphs should be harmonised, and we should use the term 'instant credit transfers' in general. HR (MS reply): We accept the proposed wording. FI (MS reply): FI: Regarding Article 65(1a), we thank the Presidency for the changes. We would still suggest fine-tuning the wording and changing the word "and" in the first subparagraph to "or" as follows: "*...based on the transaction monitoring referred to in Article 83* ~~*and*~~***or*** *on any other relevant information available to the payment service provider...*" There should not be a need to have an indication on potential fraud from multiple sources for this. EL

PUBLIC

Question	MS reply
	(MS reply): **EL:** We agree with the amendments in Articles 51(2) and 65(1a,2). Holding PSPs liable for transactions that were merely suspected of fraud but not blocked could have unintended consequences, particularly by increasing de-risking measures among PSPs. This may lead to overly cautious approaches, potentially disrupting legitimate transactions and negatively affecting users' payment experiences. DK (MS reply): While we can see the worry of excessive derisking, we are not sure this is the right way forward. The PSP should bear the risk, if it does not block a payment where there is suspicion of fraud. This also resonates with the other changes agreed which puts a stronger onus on the PSP to act. Regarding the reference to transaction monitoring mechanism and any other relevant information as valid reasons for blocking, we believe the word "and" should be changed to "or" since if the word "and" is used it would indicate a need for a suspicion of fraud stemming from BOTH the TMM and other sources as well. We think this should be aligned with article 69(2a) where the word "or" is used. DE (MS reply):

PUBLIC

Question	MS reply
	• As we have argued before, the proposal of Art. 65(1a) as it stands raises significant questions with regard to Art. 22 GDPR. • In particular, it seems that the refusal would be based on an automated decision within the meaning of Art. 22 para. 1 GDPR, which is generally prohibited. In this case, the question arises, which exception under Art. 22 para. 2 GDPR should be used as the basis for automated decision-making, in particular whether an exception within the meaning of Art. 22 para. 2 letter b GDPR should be made here. However, this would then require "appropriate measures to safeguard the rights and freedoms as well as the legitimate interests of the data subjects". • We were under the impression that the commission would consult its GDPR-unit in order to assess compliance of the proposed Art. 65(1a) with GDPR. Has such assessment taken place? If so, it would be very important for us to see such assessment before deciding out such provision. Having a clear and legally sound provision here should be in our common interest. CZ (MS reply): On 51(2) - We are flexible. On 65(1a, 2) - we think it should be clarified what is a fraudulent transaction. In PSD2 we only know the term fraudulent behaviour etc. How and when are PSPs to assess whether a transaction is fraudulent? Is it some kind of manipulation of the payer or just an Article

PUBLIC

Question	MS reply
	59 fraudulent transaction? Or just unauthorised transactions? The clear definition is crucial in this respect. We think a broader formulation is better; former version: “fraud against the PSU”. The new wording seems to be limited to fraudulent transactions, then the PSP won't be able to block it in some cases where the payer is manipulated by the fraudster but the transaction itself is not fraudulent. On 65(1a) - we would like to point out to the same problem with the meaning of fraudulent transaction? We are concerned that this could lead to a large number of rejected payment transactions. Also in this para we propose to delete this sentence: ~~For the purpose of this Regulation, the fact that a payment order is unusual shall not by itself constitute reasonable grounds to suspect fraud .~~ The sentence is very confusing Also in 65(2), first sub-paragraph, we do not agree with the new wording: "correction of the decision to refuse to execute the transaction" - if the user insists on executing the transaction, then the transaction must be executed, the PSP can inform the PSU about the risks, but if the user insists, the PSP must execute the transaction - the consequence is gross negligence of the PSU. Therefore, the PSP cannot correct the decision. In the second subparagraph of paragraph 65(2), it should not be stated: "provide or make available", but only "provide". Make available is used,

PUBLIC

Question	MS reply
	for example, for price lists and terms and conditions. It is not an appropriate wording for this type of information. CY (MS reply): We have no comments. BE (MS reply): BE: In general, we can support the PCY's proposal. However, we have some formal remarks and questions. Regarding Article 51 (blocking of payment instrument): We have a question regarding the scope of Article 51 (4). In accordance with this provision, the PSP shall unblock the payment instrument transaction or replace it once the reasons for blocking no longer exist. The words "unless the payment service user confirms his / her consent in a safely manner" are now deleted. Does this mean that the PSU cannot, in any case, object the unblocking of the payment instrument? Does this also apply when the PSU has notify the PSP of an incident with its payment instrument in accordance with Article 52? In this case, Article 53 (1)(e) oblige the PSP to prevent all use of the payment instrument. How does Article 51 (4) interact with Article 53 (1)(e)? We believe

PUBLIC

Question	MS reply
	that, where the PSU notify an incident with its payment instrument, the PSP should block it and should not unblock it without the consent of the PSU. Regarding the PSP's liability where blocking does not take place despite reasonable grounds for suspecting fraud: in general we believe that the PSP should bear a liability where they fail to have robust fraud prevention mechanisms in place. In our view, any element that enable the PSP to escape the liability in case of fraudulent transaction could constitute an incentive for PSPs not to have robust fraud prevention mechanism in place. We should therefore be cautious in this respect. On the other hand, we understand that the PSP's liability where blocking does not take place could be an incentive for PSPs to block automatically any payment instrument or transaction in case of mere grounds for suspecting a fraud only to escape the liability. This could lead to the unwanted blocking of legitimate transactions and undermine the efficiency of the payment system. Moreover, we assume that it would be complicated, if not impossible, to prove that the PSP had sufficient reasonable doubts to justify blocking a payment instrument or refusing a payment order. In this sense, we can accept the removal of the last sentence of Article 51 (2). But PSPs should still be incentive to have robust fraud prevention mechanisms in place. Regarding Article 65 (refusal to execute a payment order):

PUBLIC

Question	MS reply
	We notice that in Article 65 (1a), the decision to block a payment instrument should be based on transaction monitoring and any relevant information available to the PSP. We believe that the decision should be based on transaction monitoring or any relevant information available to the PSP (alignment with the wording of Article 69 (2a) regarding freezing funds). Regarding the notion of "unusual transaction": it should be clear in PSR that an unusual transaction does not constitute by itself reasonable grounds to suspect fraud. However, any unusual transaction could constitute a first indication of fraud, which should alert the PSP and should be further investigated. PSPs should bear a certain liability in this respect and should always take appropriate and reasonable actions to block potential fraudulent transactions. Finally, we are concerned about last sentence of Article 65 (2): *The framework contract may include a condition that the payment service provider may charge a reasonable fee for such a refusal if the refusal is objectively justified, but not in the case of a refusal due to a suspected fraudulent transaction*. What is the scope of this rule, i.e. which cases are covered by the right of the PSP to charge a fee? Moreover, what should be mean by "reasonable fee"? AT (MS reply): Yes. We particularly welcome the latest amendments to Art. 65 para 1a and the deletion of the last sentence of Art 51 para 2.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
Q6. Could Member States accept the wording of Article 83(1a) and (2) PSR?	MT (MS reply): Malta agrees with the wording outlined in Articles 83(1a) and (2) on the obligation of the payee's PSP to conduct transaction monitoring. SI (MS reply): New draft provision of Article 83 para 1a PSR might prove difficult to use in practice. We consider that the assessment of the scope of fault of each party might be difficult. SE (MS reply): We would have preferred less detailed provisions on TMM and an open-ended list of information to be monitored, but can accept the proposal for the sake of compromise. RO (MS reply): We agree that where such monitoring does not take place in a specific transaction, the payer shall not bear any financial consequences from that specific transaction, except where the payer has acted fraudulently. However, in case the payer has acted with gross negligence we agree that

PUBLIC

Question	MS reply
	the liability for the damage incurred shall be shared between the payer and the payer's PSP. Additionally, in our opinion the PSP should not be in any way encouraged to refuse the development or usage of efficient monitoring tools, in this case by having the payer (victim) bear part of the loss. While we agree with the idea that the payer and payer's PSP might share liability in some cases of gross negligence, we believe that this should not apply when the PSP has not applied efficient transaction-monitoring mechanisms. Proper monitoring should be a prerequisite of the PSP, before any shared liability is applied. PT (MS reply): PT would deem it worthwhile to further specify the sentence "*The exact share of liability shall depend on the scope of the fault of each party"*, as it appears to be rather complex and subjective to ascertain the degree of fault attributed to PSP and PSU. Alternatively, and given these challenges, we would favour removing this sentence from the Article's text. Moreover, on the 2nd paragraph of Article 83(2), we suggest removing the reference to the name of the beneficiary in point (c), as that detail appears to be already encompassed in the information of the payee envisioned in point (a).

PUBLIC

Question	MS reply
	Please consider the following adjustment: *" 2. (...)* *Processing by the payment service provider of the payee shall be limited to the following data required for the purpose referred to in paragraph 1, as applicable:* *(a) information on the payee;* *(b) information on the payment account of the payee, including the payment transaction history;* *(c) transaction information, including the transaction amount~~,~~ **and** the name of the payer ~~**and of the beneficiary**~~.* *(...)"* NL (MS reply): • Not all paragraphs of Article 83 are not included in the current text. For our comments to the other paragraphs, we refer to our previous input. We reiterate our request to the Presidency to provide for integral provisions, in order to allow Member States to review proposed changes in the context of the provision as a whole. • As for paragraph 83(1a), we cannot agree with the proposed changes. If the PSP has not performed its transaction monitoring,

PUBLIC

Question	MS reply
	the PSU should not bear any financial consequences (safe for fraud by the PSU). Only when the PSP has in fact performed monitoring, the PSU's gross negligence will constitute a ground for a shared liability. Furthermore, we suggest to rephrase the last sentence as follows: "The burden to prove that the payment service user has acted grossly negligent shall be on the payment service provider". We find this wording to be more clear, as the provision covers quite a lot and the wording "breach of this Article" thus seems quite vague. • We can agree to paragraph 83(2) but the formulation of point (a) is still rather vague. Which "environmental and behavioural characteristics" are referred to here? What is "a normal use"? Is it possible to make the provisions here, and possibly also provisions for other elements of the transaction monitoring mechanism, more specific? LV (MS reply): We support the additional parts, which we have already supported without further comments. LT (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	Regarding Article 83(1a) - a proposal for shared liability where the payer has acted with gross negligence as well, seems quite a balanced one at a glance. However, the notion that '*The exact share of liability shall depend on the scope of the fault of each party.*' might bring more confusion to the liability scheme proposed that potential benefits: PSPs will have discretionary power to decide on the share of liability for each party and this might be disadvantageous to PSUs (consumers), i.e. result in PSUs having to bear the lion's share of the losses. Especially, since there is no criteria that could be the basis for making an objective decision on the share of liability. Therefore, to avoid the negative consequences of the proposal, it is advisable in such cases to split damages between PSP and PSU in equal parts. IT (MS reply): On par. (1a): we broadly agree with the introduction of a rule on "shared liability" in cases where both parties are "at fault". In our view, such a rule is useful in addressing the issues arising from the liability shift introduced by the second sub-paragraph of Art. 83(1a). However, we would have preferred a more general provision on "contributory negligence" (see our comments in Q2 of the Presidency Note on fraud, discussed in the WP of February 25). In any case, we think that the exclusion of the payer from any liability should not apply in the case of "intentional" breach of its obligation by the PSU (see Art. 60(1), last subparagraph). We therefore propose the following amendments to art. 83(1a):

PUBLIC

Question	MS reply
	1a. The payment service provider of the payer shall carry out the transaction monitoring referred to in paragraph 1 prior to the execution of a payment transaction. Without prejudice to Article 69(2), the payment service provider of the payee shall also carry out transaction monitoring of received payment transactions. *Where such monitoring does not take place in a specific transaction, the payer shall not bear any financial consequences from that specific transaction, except where the payer has acted fraudulently or intentionally failed to fulfil its obligations under Article 52.* *Where the payer has ~~acted~~ failed to fulfil its obligations under Article 52 with gross negligence, the liability for the damage incurred shall be shared between the payer and the payer's payment service provider. The exact share of liability shall depend on the scope of the fault of each party.* *The burden to prove that there was no breach of this Article shall be on the payment service provider.* Moreover, we note that art. 83(1)(c), in defining the TM, refers to "fraudulent" transactions. As pointed out before (see Q5) "fraudulent" is not a notion defined in the PSR and does not necessarily coincide with "unauthorized", as it could be interpreted to include, e.g., fraud related to the "underlying reasons" of a transaction. The proposed par. (1a) provides that, where the TM does not take place in a "specific transaction", then the PSP shall be liable (with the exceptions and limitations provided therein). Therefore, when the TM is not performed, then

PUBLIC

Question	MS reply
	the PSP may be held liable, for example, even in case of APP fraud, expanding the liability beyond (what will probably be) the scope of Art. 56 (and Art. 59, if retained). In addition, the liability shift seems to apply if the TM is not performed, regardless of whether the transaction should reasonably have been or not be intercepted by the TM. We are not necessarily opposed to such an extension, provided that it applies *only* to cases where the PSP *entirely* fails to conduct the TM. However, we are worried – as expressed in our comments to Q2 in the Presidency note on fraud-related issues discussed in the WP of February 21st – 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. Such an interpretation could extend significantly the scope of the liability. To avoid such an extension, we should clarify that the special liability rule only applies where the transaction monitoring does not take place at all. For example, a recital could expressly clarify that when the TM was performed, but its correct execution is debatable, the special liability rule does not apply; instead, only the "ordinary" liability regime under Title II, Chapter 4, is applicable. Also, for maximum consistency with art. 51(2) [blocking of a payment instrument], Art. (83)(1)(c) [definition of TM] could refer to both “unauthorized” and “fraudulent” transaction.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	On par. (2): we have some doubts about the exhaustive nature of the list of information that PSPs may use for the TM (even though the listed items are very broad in their scope). At the very least, we do not understand why this list is exhaustive, whereas the list in Art. 83a (on data sharing) is not, especially considering that sharing information with other PSPs poses a greater privacy risk. We therefore propose aligning the wording of Art. 83 to that of Art. 83a. For example: "*Processing by the PSP of the payer/payee may include, but is not limited to, the following data, to the extent necessary to comply with its obligation in paragraph (1)…*"]. IE (MS reply): We welcome the clarification on the interplay with Regulation (EU) 2024/1624 (AMLR) in order to ensure legal certainty and consistency in application across member states. We can support a shift in liability if the payer's PSP fails to fulfil its obligations, such as transaction monitoring, however we would note that any data monitored must respect the general principles of GDPR. It is not clear to us what the proposal under Article 83(1a) is trying to achieve. HU (MS reply): We largely agree.

PUBLIC

Question	MS reply
	In our opinion in case of gross negligence, the liability shall be shared between the payer, the payer's payment service provider and the payee's payment service provider in Article 83(1a). We agree with the extension in Article 83(2) as we believe strengthened transaction monitoring is the key to prevention. HR (MS reply): We accept the proposed wording of Article 83(1a). We acknowledge the amendments made to Article 83(2), but it is unclear why is there a limit to the data for the purpose of transaction monitoring mechanism. In our opinion, the data included in the transaction monitoring mechanism should not be limited to the proposed list of data. The PSPs should be allowed to decide on the data to be included in the transaction monitoring mechanism. FI (MS reply): FI: Firstly, we agree on the principle that TMM should take place and that there could be consequences for the PSP in case of breach of that obligation. However, creating a separate framework for shared liability and its division depending on "the scope of the fault" as proposed under the second and third sentence of Article 83(1a), second subparagraph,

PUBLIC

Question	MS reply
	would make the provision unnecessarily complicated, given that the provisions of Chapter 4 would be also applicable. The suggestion would also create major problems for dispute resolution bodies because evaluating PSU's possible negligence together with PSP's failure to use TMM would be extremely difficult. EL (MS reply): **EL:** We accept the proposed wording of article 83(1a) and (2). DK (MS reply): In general, we support the changes proposed. However, we remain of the firm opinion, that the list of datapoints to be included in the transaction monitoring should be non-exhaustive to make it more future proof. DE (MS reply): With regard to Art. 83(1a) and (1b) PSR: • The wording still 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. • Further, it is very important for us to 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).

PUBLIC

Question	MS reply
	• We suggest a new provision – similar to Art. 57 PSR – regulating the liability regime that dependents upon the PSP carrying out the duties in Art. 83(1a), instead of adding a sentence to Art. 83(1a) PSR. In particular, this would be preferable to adding an Art. 83 (1b) PSR only referring to the provisions of chapter 4. With regard to Art. 83(2) PSR: • We suppose that the monitoring mechanism means an additional, separate procession of said personal data. We therefore kindly ask COM for explanation, which data protection regimes applies to the data processed within the monitoring mechanism, esp. which regulations about the collection. transmission, storage and deletion do apply and which safeguards have to be taken? CZ (MS reply): We would like to thank you for improving the text in Article 83(1a). We would just like to be sure that the PSP's liability is only in the event that the monitoring mechanism is not in place. This could be clarified in a recital. We don't understand why Chapter 4 is mentioned in Article 83(1b). We would welcome some clarification why the reference is included. On Article 83(2) - we think that the limitation is not necessary, the data is not shared, so we would like to ask why there is the limitation there, both

PUBLIC

Question	MS reply
	for the PSP of the payer and the PSP of the payee. The limitation could weaken the monitoring mechanism and its effectiveness. CY (MS reply): We have no comments. BE (MS reply): BE: We have some concerns regarding the shared liability introduced in Article. 83(1a) where the PSU acted with gross negligence. Firstly, as we mentioned above, PSPs should have robust fraud prevention mechanisms in place. In this sense, PSPs should carry out robust transaction monitoring, in accordance with Article 83. If such adequate monitoring does not take place, it is in our view the sole liability of the PSP as defined in Article 83(1a). Moreover, the question of the behaviour of the PSU in the event of a fraudulent transaction is already covered by the provisions in Chapter 4 of PSR, in particular in Article 60. If the PSU has been grossly negligent, they could bear some financial losses, in accordance with Article 60. We do not see the need for having this in Article 83. It is also not appropriate to have a reference to gross negligence in Article 83. PSPs tend to use gross negligence systematically to escape from their liability. We fear that PSPs will now be encouraged to use gross negligence to escape from the obligation to carry out an adequate and robust transaction monitoring.

PUBLIC

Question	MS reply
	Ultimately, this would undermine the effectiveness of the transaction monitoring. We are also concerned about the level of robustness of the monitoring mechanisms expected of PSPs. In our opinion, PSPs should not only have transaction monitoring mechanisms in place, they should also ensure that their transaction monitoring mechanisms are sufficiently robust and efficient. However, Article 83 does not contain any sanction where the transaction monitoring mechanism of the PSP is not sufficiently robust and efficient. We wonder how we could reinforce the obligation for PSPs to have robust and efficient transaction monitoring mechanisms in place? Member States should be able to ensure supervision and control regarding transaction monitoring mechanisms and their hight level of effectiveness. It could also be beneficial to have some criteria for assessing the robustness of the monitoring mechanisms in EBA RTS. Furthermore, the assessment of the monitoring system could also be incorporated in the report on the application and impact of this Regulation and Review Clause. AT (MS reply): Yes, the proposed way forward seems acceptable to us. However, it should be closely monitored whether the decentralized information sharing arrangements according to Art. 83 para 3 create duplicative structures and should rather be replaced by a central information platform.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
Q7. Could Member States accept the proposed wording of Recital 103a and Article 83a para. (1), (1a), (2) and (6) PSR?	MT (MS reply): Malta agrees with the wording outlined in Recital 103a and Article 83a(1), (1a), (2) and (6) on anti-fraud information sharing. SI (MS reply): We could accept the proposed drafting. SE (MS reply): To us, it is central that the list of information to be exchanged is inexhaustive. Making the exchange mandatory is of less importance. We welcome the latest amendments, including the clarification that the list of data is inexhaustive and refers to the *PSU* instead of the *payee*, and that the maximum limit for data storage has been extended to 5 years. These are small but important changes that ensures that PSPs can share all relevant information with each other in an efficient way to combat fraud. RO (MS reply): We agree with the proposals set out in Article 83a para (1), (1a), (2) and (6) but we believe that the proposal regarding Recital 103a might be

PUBLIC

Question	MS reply
	somewhat redundant. Therefore, for Recital 103a we propose the following wording: *"Timely sharing of relevant fraud data amongst payment service providers and also with ~~payment service providers and~~ relevant national authorities to enhance their transaction monitoring mechanisms plays an important role in achieving the objective of timely detection and prevention of fraudulent payment transactions. In some cases, different data sharing frameworks under other relevant Union legislation may apply to the data being shared. To ensure legal certainty regarding the conditions under which payment service providers shall ~~can~~ share fraud-related information for the purpose of fraud prevention, including ~~also~~ with the relevant national authorities, the conditions under which such data sharing is allowed under this Regulation should be specified. Information sharing should be subject to robust safeguards, in conformity with Regulation (EU) 2016/679 in relation ~~relating~~ to confidentiality, data protection and the use of information. This should be without prejudice to the requirements under the AMLR not to disclose that a suspicious transaction has been reported to the FIU or that an internal analysis into ML and TF is being carried out, and should not lead to jeopardizing an AML/CFT investigation."*

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	PT (MS reply): PT agrees with the suggested wording and does not currently wish to provide additional relevant remarks. NL (MS reply): • We can accept the proposed wording of recital 103a if ECSPs are also added to this provision. • Art. 83a(1): data sharing should not only be possible to comply with Article 83(1)(c), but also to exchange data with national authorities and with supervisory authorities. This is a very important topic for us. We proposed the following subparagraphs for Article 83(1): (d) enable payment service providers to inform competent national authorities for the purpose of a possible criminal investigation. (e) enabling payment service providers to establish accountability towards supervisory authorities. • Furthermore, with respect to Article 83a(q) we always were in favor of a limited set of data. We can thus not agree to a non-exhaustive list. We agree with making data sharing mandatory. • We can agree to Article 83a(1a).

PUBLIC

Question	MS reply
	• We can agree to Article 83a(2). • We cannot agree to paragraph 6. It is very important for us that the PSR provides a legal basis for PSPs to share data with national authorities. While the newly proposed paragraph 6 is a step in the right direction, it is not sufficiently prescriptive, which means that it could not serve as a legal basis. For this reason, we propose the following wording: • Payment service providers shall share the data as referred to in paragraph 1 with the relevant competent national authorities to the extent strictly necessary to comply with their obligations in Article 83(1), point (d). LV (MS reply): We support the proposal. LT (MS reply): We accept. IT (MS reply): We welcome the addition in para. 6. However, we do not support the mandatory nature of participation in fraud data sharing mechanisms,

PUBLIC

Question	MS reply
	which we infer from the replacement of "may" by "shall". If the provision means that sharing is mandatory once the PSPs had decided to be part of such agreements, this should be made clear in the wording. We have no objections to the proposed wording. In particular, we agree with the deletion of the second sentence of Art. 83a(1a). However, we are not entirely sure about the use of "shall" instead of "may" in par. (1) and (1a) of Art. 83a. Participation in an "information sharing arrangement" does not appear to be mandatory and, in any case, is subject to confirmation by the other participants under par. (4). Therefore, as currently worded, we understand that Art. 83a requires a PSP to exchange data *only if* it is a member of such an arrangement. Also, we understand that data can be shared exclusively with the other members of the same arrangement. If this interpretation is correct, Art. 83a (or at least R103a) should explicitly clarify the point. In any case, if "shall" is retained in the first sentence of par. (1a), the second sentence should be amended as follows: "*The catalogue of data ~~that may~~ **to** be shared shall include, but not be limited to* […]" IE (MS reply):

PUBLIC

Question	MS reply
	We support the drafting in general but would prefer a non-exhaustive list – GDPR is very strong in IE. We note that the 5-year retention period needs to align with any obligations under AML/CFT legislation. HU (MS reply): Yes, we strongly agree with the changes in Article 83a, in particular the transformation in an open catalogue and the longer retention periods. Information sharing is key in prevention of fraud and if the co-legislators want to curb fraud this can only pass by enhancing transaction monitoring and cooperation among PSPs. HR (MS reply): We agree with the proposed wording. FI (MS reply): FI: Firstly, we find the expression "*...to the extent strictly necessary to comply with their obligations...*" extremely important, especially now that the data to be shared would not be exhaustively listed in the Article. Secondly, we would call for clarity on the relationship between Article 83(1) and 83(1a). The provisions appear to have the same content, except

Question	MS reply
	that paragraph 1a imposes an additional requirement for the PSP having to have reasonable and objective grounds to suspect fraudulent behaviour by a PSU. We do not understand the added value of including paragraph 1a in addition to paragraph 1. In case the provisions are overlapping, paragraph 1a could be deleted. EL (MS reply): **EL:** We can accept the proposal; however, we recommend conducting a GDPR impact assessment regarding the data-sharing requirements DK (MS reply): We can support the wording of Article 83(1a) and (2) PSR. We generally support the proposed amendments. We support that the list in paragraph (1) is clearly made non-exhaustive. We support the more neutral reference to "payment service user" instead of "payee". In paragraph (1a): We are happy to see the new wording as we believe it is quite far reaching to assign full responsibility to the provider if they have not shared data. Data sharing does not always prevent fraud - and sharing data is not that simple, considering GDPR and other regulations. We are also supportive of the extension of the timeframe for storing of data in paragraph (2). And also support the amendment in (6). DE

PUBLIC

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	(MS reply): We have **two** main remarks: • **First**, fraud data sharing should remain voluntary. The idea behind Art. 83a PSR is to set a legal basis for PSPs to voluntarily exchange fraud data based on information sharing agreements. In contrast, Art. 83a PSR was never meant to specify another obligation for PSPs. Changing this fundamental underlying principle of Art. 83a PSR by making fraud data sharing compulsory would raise significant legal and practical questions. • In particular, the approach of Art. 83a PSR is based on PSPs voluntarily entering information sharing agreements with other PSPs. Within those agreements the PSPs would set out terms and conditions under which a data sharing takes place – based on a thorough data protection impact assessment. In our understanding, the changes proposed would lead to a situation in which the participation in information sharing agreements with other PSPs would continue to be voluntary. However, within such agreements, data sharing would be compulsory. Hence, the changes proposed would disallow PSPs to determine well-defined, data sensible terms and conditions of data sharing within their data sharing agreements contradicting the whole set-up of Art. 83a PSR. Further, making data sharing within the agreements compulsory provides a clear disincentive against entering data sharing agreements in the first place and hence, has the potential

PUBLIC

Question	MS reply
	to decrease the level of data sharing altogether, against the aim of this proposal. Hence, fraud data sharing should remain voluntarily. • **Second**, like said in the last working party already, we still have serious GDPR-related problems with the set up of Art. 83a: ○ For GDPR-reasons we still consider an exhaustive list of data points in Art. 83a PSR as necessary. If such exhaustive list is not deemed to be future-proof, we would support the FR approach to exhaustively define additional data points on level 2. ○ Further, again for GDPR-reasons, it is in our assessment imperative that the data lists in Art. 83 and 83a PSR match. The purpose of Art. 83a PSR is to set a legal basis for data sharing between PSPs (w.r.t. Art. 6 par. 1 lit. c, par. 3 GDPR) in order for PSPs to better comply with their obligations with respect to Art. 83 par. 1 lit. c. In this logic, there is no room for additional data points in Art. 83a PSR that go beyond the exhaustive list of data points in Art. 83 PSR. We were under the impression that the COM would assess these problems with its GDPR-unit. Has such assessment taken place? If so, it would be very important for us to see such assessment before deciding on such provision. Having a clear and legally sound provision here should be in our common interest. Further, we have a set of additional comments:

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	Art. 83a para 2: • Even if, according to the PCY, several MS have spoken out in favour of a longer storage period, there should be objective reasons for this. Five years is a considerable period of time. Therefor we would ask for some more detailed reasons for the necessity to extent the storage period from three to five years. Could it be a way forward to keep the three year period in general and to allow an extension another two years in individual cases where necessary? Art. 83a para 3: • It seems likely that different payment service providers participating in an information sharing arrangement would be considered joint controllers when processing shared data. • Has this assessment already been considered? Which supervisory authority would consequently be considered lead supervisory authority in the case of transnational information sharing arrangements? Art. 83a para 6: • It remains unclear, o for which purpose the data exchange is to take place (clarification of individual cases, i.e. ultimately criminal prosecution, avoidance of future fraud data in the sense of prevention, identification of systematic risks, etc.), o accordingly, which authorities may be “relevant” here and

PUBLIC

Question	MS reply
	○ whether it is a case-by-case or systematic data exchange. ▪ This should be clarified where possible. The principle of purpose limitation laid down in Art. 5 para. 1 lit. b GDPR refers to "specified" and "explicit" purposes. From a data protection perspective, the envisaged data exchange between service providers and national authorities should be limited to specific occasions and individual cases. For example: "*For the purpose of investigation and prosecution of suspected fraudulent activities, Member States shall ensure ... so that SP are able to share data referred to in paragraph 1 to the extend necessary with the competent national authorities where they have reasonably grounds to believe that fraudulent acts have been committed.*" CZ (MS reply): We have scrutiny reservation, preliminary we are flexible, we will send detailed position in written comments if needed. CY (MS reply): We have no comments. BE (MS reply): BE: We understand the need for an effective cooperation and communication between PSPs in the fight against frauds. In general, we are not opposed to the

PUBLIC

Question	MS reply
	principle of fraud data sharing. However, we still have concern regarding the GDPR. The risk for the data protection is quite important: the list of data that can be shared is non-exhaustive and PSPs can exchange these data even in case of mere doubt regarding a payment transaction. PSPs could therefore exchange information at their sole discretion. We see that the information sharing should be subject to robust safeguards in accordance with GDPR. We are concerned that some PSPs overstate the need to share information and understate the GDPR risks related to the data sharing and the safeguards that should be required. We should be more cautious in preventing any abuse in the information sharing. AT (MS reply): Yes.
Presidency Discussion Note on services where cash is provided in retail stores without a purchase (cash-in-shops) (WK 3366/25)	
Q1. Do Member States agree with the proposed way forward and drafting suggestions?	MT (MS reply): Malta agrees with the proposed way forward that the withdrawal limit should be regulated in level 1 text. However, with regards to the drafting suggestion about the amount of the said limit per se, Malta is of the view that a lower limit would be more appropriate. In particular, taking into consideration the Commission's initial proposal for a limit of €50 and the Presidency's proposal for a limit of €150,

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	Malta proposes that a withdrawal limit of €100 would be an adequate compromise. Nevertheless, this should be complemented by the option for Member States to set the limit. SI (MS reply): We agree. SE (MS reply): We support the proposal. RO (MS reply): Having in mind that we expressed a preference for setting a limit for these transactions, from the perspective of addressing a possible AML risk, we can support PRES proposal. PT (MS reply): PT would prefer maintaining Article 37(3) to mandate EBA to fully clarify how limits should be enforced, believing it is a viable way to avoid abuses and non-compliance. Notwithstanding, and given the apparent lack of support for this approach, we are willing to go forward with the suggested deletion.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	NL (MS reply): Making sure that the access to and acceptance of cash is preserved is very important. Therefore, we support the introduction of the possibility to withdraw cash in retail stores without doing a purchase. We do think that withdrawing cash through an ATM should remain the main channel to withdraw cash. Cash-in shops should be a nice addition and not a replacement of the infrastructure and responsibility of banks to make cash accessible. In general, we can agree with the proposed way forward, but we do have some concerns how this would work in practice. How can a daily limit be monitored? It should not lead to an administrative burden for merchants or lead to an extensive supervisory framework leading to additional costs for the consumer. These practical questions should first be answered before setting a limit. Given these difficulties we prefer to have one limit (a limit per transaction) of 50 euros, in line with the commission proposal. However, we could also agree with a higher limit of 150 euros per transaction if this is more suitable given the different national situations. LV (MS reply): We support the proposal. We would also support regulation at national level, in which case limits should be set where possible.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	LT (MS reply): We agree with the drafting proposing higher transaction limit. It is important that there is a possibility for additional way to withdraw cash, i.e. in shops, it helps with a cash availability. IT (MS reply): While we agree on the importance of ensuring access to cash, we see the need of having more legal clarity related to cash-in-shop services, considering the AML risks and also the need to maintain high level of trust in cash distribution and protection against counterfeiting. In particular, our first best remains not exempting such services from the PSD3 scope, and qualifying the cash-in shop as cash withdrawal payment service (see comments to the Consolidated table PSD3 of 24 March 2025). However, in the light of the compromise, we can be open to accept an exemption regime as second best, provided that the following conditions are met: • About exemption limits, introducing two thresholds (one per single transaction, that we notice has been increased up to three times the initial proposal of 50 euro; one limiting the overall value

PUBLIC

Question	MS reply
	of transactions that may be carried out on a daily/weekly/monthly basis) in order to reduce the overall amount of withdrawn cash with such service and, thereby, the related ML/TF risks (about the proposed value of the global daily limit, please see Q.2). • We strongly advocate for a clarification on how the compliance with the obligations set in this article will be monitored on a continuous basis, also in the course of the next CWPs. We suggest to explicitly recall in art. 37, par. 2 the PSP acquirer's transaction monitoring duties towards the merchant as his customer (to detect any anomalies in withdrawal operations and verify that operations thresholds are met). Furthermore, as far as notes distribution to the public matters are concerned, in line with ECB opinion (paragraph 5), we believe that the need to ensure compliance with the cash recirculation legislation should be explained, to ensure the necessary quality of euro banknotes distributed within the euro area. In this regard, we suggest inserting the red engraving in paragraph 2: "*This Article shall be without prejudice to Directive (EU) 2015/849 or any other relevant Union or national anti-money laundering/terrorist financing laws as well as the legal framework regarding authenticity and fitness checking of euro banknotes distributed to the public.*"

PUBLIC

Question	MS reply
	• From the same perspective, we do not agree with deleting art. 37, par. 3, pursuant to which EBA is entrusted with a specific regulatory mandate: in our view, such mandate is necessary since the text of Directive in Level 1 does not specify how limits set by art. 37 would be enforced and who would assess that enforcement. On this topic, we reiterate our previous comment to recommend that the AMLA is involved in the drafting process in order to ensure that ML/FT risks are properly taken into account. Moreover, we suggest to modify Recital 62 deleting "independent" before ATM deployers, to align the wording to the one agreed in the February WP. IE (MS reply): As per below we support a lower withdrawal limit of 50 euro. HU (MS reply): Yes, we agree. HR (MS reply): We agree with the proposal. FI

PUBLIC

Question	MS reply
	(MS reply): FI: We support the proposal partly. Namely, we support the increase of the withdrawal transaction limit to EUR 150 as well as the deletion of the EBA mandate. We do not support the introduction of the daily limit, at least not in its current form, please see Q2. EL (MS reply): **EL:** Specific rules must be implemented to address not only daily and global limits but also other aspects, such as the framework for applying and monitoring these limits, measures to prevent counterfeit banknotes, and the liability regime. Our opinion is to implement the cash-in-shop regime within the PSD *agency* framework. DK (MS reply): We agree with the proposed way forward and drafting suggestions except from. We support the deletion of the EBA mandate, and we support the reference to other kinds of currencies than the euro. DE (MS reply): • As argued before, we do not support Article 37 PSD 3 exempting cash-in-shop services without a purchase from the scope of PSR / PSD 3.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	• In our view, the current approach to exempt cash-in-shop activities from the scope of PSR / PSD 3 only if they were part of a payment transaction for the purchase of goods and services was striking the right balance between supporting the access to cash on the one hand and AML / counterfeiting arguments on the other hand. • Additionally, the foreseen exemption with a spending limit of 200 € per day would raise serious question regarding the level playing field between cash-in-shop services and the services provided by ATM deployers (independent or not). CZ (MS reply): We do not understand why, if there is no limit for services where cash is provided by the payee to the payer as part of a payment transaction for the purchase of goods and services under 2(2) d) PSR, there is such a different approach for similar services, just without the purchase of goods or services. From CZ perspective exemption under 2(2) d) PSR works well and we prefer cash-in-shops without a purchase is given similar flexibility. CY (MS reply): We are supportive of the proposed way forward and drafting suggestions. AT

PUBLIC

Question	MS reply
	(MS reply): Yes.
Q2. Do Member States agree with the global daily limit and a proposed value? If not, please provide an alternative.	MT (MS reply): Malta agrees with a global daily limit rather than a weekly or monthly limit. In relation to the proposed global daily limit value, Malta considers that this should be €150. Nevertheless, this should be complemented by the option for Member States to set the limit. SI (MS reply): We agree. SE (MS reply): Yes. We assume that it is the ASPSPs' obligation to enforce these limits. This would however presume that the shop registers the amount correctly as *cash withdrawal* and not as a purchase. RO (MS reply): - PT (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	PT agrees with the possibility of having both daily and global limits. However, we strongly support the specific thresholds should be established by each Member States, rather than in the L1 text, as a way to take into account the specific circumstances of each national reality. NL (MS reply): See also the answer to question 1. We prefer a limit of 50 euros per transaction. LV (MS reply): We support the proposal. LT (MS reply): It would be best if any cumulative limits, if any, would be decided by the market, issuing PSPs depending on relevant circumstances. Daily global limit could be accepted only if its monitoring is done by issuing PSPs. No obligations in this regard should be put onto merchants. If concrete limit is put in the PSR – we would favor the same limit as transaction limit – 150 EUR. That would mean that consumer can withdraw the same amount in one or several transations. IT (MS reply):

PUBLIC

Question	MS reply
	We agree with introducing a global daily limit, but we consider too high the proposed value of 200 euro. We suggest to set the same threshold for both single transaction and global daily limit (150 euro), also taking into account that in the current drafting the two thresholds are very close. If it is not possible to find an agreement on the threshold values, considering the different level of cash availability in MS and specific national AML risks, we suggest to set in article 37 two maximum threshold and to leave to MS the option to set their own withdrawal limit below to that maximum threshold (this approach mirrors the one already adopted in the AML Package for cash payments threshold). IE (MS reply): IE supports a lower limit. Our view is that the proposed limit of €150 per withdrawal is too high. In the short term, this high limit could depress demand for ATM services and make them less economically viable, while over the long term, retailers will likely carry less cash or opt to not provide the service, and thereby not meet demand, which will subsequently then be underserved as ATMs were removed due to retailers' high limit for cash. It is our view that it not feasible to put mechanisms in place to require retailers to provide cash or require them to stock it.

PUBLIC

Question	MS reply
	Ireland's preference is for a limit of €50, so that the cash services from retailers complement the cash infrastructure rather than undermine it. We consider that the €50 amount should remain in the level one text. The proposals here also raise the question of how the Commission envisages gathering, analysing, reporting and acting on information on cash services by retailers, when retailers come and go, can opt in and out of providing the service, and NCAs have no information gathering powers? HU (MS reply): Yes, we agree. HR (MS reply): We agree with the proposal. FI (MS reply): FI: We strongly object to the introduction of additional burden on merchants, as any such burden would be detrimental to their willingness to provide cash-withdrawal services and thereby undermine the objective of adding to cash-supply. The proposal leaves it open who would be the obliged entity to establish and monitor the daily limit. It would be a matter of interpretation whether the obliged entity would be the account servicing payment service provider (ASPSP)

PUBLIC

Question	MS reply
	or the merchant, leading to substantial legal uncertainty and to unlevel playing field owing to different national interpretations. In addition, as the limit is proposed to be set at the account level, it would be very difficult, if even technically possible, for the merchant to set up such a limit and to monitor it. It would require merchants either to have online access to banks' accounting systems so that the merchants would be able deny cash-withdrawal breaching the daily limit or to create accounting systems by themselves where they record the customers' bank account and follow its usage. Such accounting systems of the merchants should be set up at EU-level in order to avoid the situation where the limit is circumvented by withdrawing cash from different merchants. Thus, the impact of requiring merchants to set up such a daily limit would clearly lead to a situation where they no longer provide cash-withdrawal services. Based on the above we would propose 3 alternatives: i) provide explicitly in the text that the obliged entity for establishing the daily limit would be the ASPSPs; ii) make the introduction of the daily limit a MS-option; or iii) delete the daily-limit requirement. EL (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	EL: Our primary concern is ensuring the effective application of any daily limit when these transactions are processed as card payments at points-of-sale, just like any other card transaction. How will the PSP be able to distinguish a card transaction intended for cash-in-shop purposes from a standard purchase transaction to accurately enforce the daily limit? DK (MS reply): Regarding the limits. We understood that the Presidency would come up with a new draft which would allow for more national flexibility. We could support this option and look forward to see the Presidency's drafting suggestion. DE (MS reply): • Setting the daily withdrawal limit of cash in shop services without a purchase to 200 € would essentially jeopardize the well-established cash back with a purchase practice, given that the limit for those services is set at 200 € per transaction. • Further, we still do not understand who the obliged entity to monitor the global daily limit would be? The accounting servicing payment service provider? How would the monitoring work in practice? **As long as there is no clarity about these practicalities we should not agree on daily spending limits.**

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	• Finally, we have understood that a potential line of compromise could be to leave the decision about the size and type (e.g. per transaction, daily) of the limit of transaction to the discretion of MS. We could see merits in such line of compromise. CZ (MS reply): We **disagree** with the introduction of a daily limit. This is too restrictive. We also doubt that this is technically feasible as it leads to new requirements for the whole card ecosystem. CY (MS reply): We have no comments. AT (MS reply): Yes.
Presidency Discussion Note on interplay with the FIDA Regulation (WK 3395/25)	
Q1. Do Member States agree with the proposed drafting suggestions for Articles 3 and 36 PSD3? If not, please provide an alternative.	MT (MS reply): While Malta supports in part the latest proposed drafting suggestions, Malta does not support the removal of the following provision from Article 3 which was carried out as a result of 28 January Council Working Party meeting held, stating

PUBLIC

Question	MS reply
	"For the purposes of point (c), a payment institution's own funds or initial capital shall not be excluded from what a comparable guarantee is." Moreover, Malta also considers that the requirement of monitoring the coverage of the insurance or comparable guarantee on an ongoing basis should not be removed. SI (MS reply): / RO (MS reply): - PT (MS reply): PT does not agree with the deletion of Article 3(5), second paragraph, which clearly depicted that an entity's own funds or initial capital shall not be excluded from the concept of comparable guarantee, meaning the usage of these to comply with the obligation foreseen in Articles 3(4) and 36(4) will remain dependent on certain conditions to be set in RTS.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	As previously stated, experience from the implementation of PSD2, has highlighted certain jurisdictions, such as PT, face a considerable lack of offering of products that would allow interested entities seeking authorisation to obtain the demanded PII. This consequently tends to undermine entry of new market operators and the penetration of new and innovative services in those countries. It is therefore essential that the scope of alternative comparable guarantees encompasses a range of possibilities to satisfy the mandated requirement. This includes the usage of additional initial capital or own funds to deduct the minimum monetary amount of the PII or, considering its nature of comparable guarantee, to completely replace the obligation to hold the PII. In this regard, please see the EC's answer to our Q&A 2023-6675, where Portugal raised a question about the possibility to consider own funds requirements as a possible comparable guarantee, which seems to accept the possibility of own funds being considered as an equivalent guarantee (provided certain requirements are met). From our view, we cannot impose the insurance/comparable guarantee approach on the grounds that it is the least burdensome, since, when, compared to own funds requirements or a minimum amount of initial share capital, it ends up preventing the entry of new market operators.

PUBLIC

Question	MS reply
	It is also worth noting the current rather unclear characteristics of what constitutes a comparable guarantee, whose specification was also granted in an EBA mandate under PSD2. From the information we were able to gather, the omissive precision in this regard has prevented interested entities on trying to seek authorisation from pursuing this concept. Consequently, these entities are faced with few reliable alternatives to the PII, an absence that can either deter them from providing their services or leave them no choice but to seek authorisation in other MS that does not hold the same offering constraints. On a final note, let it also be highlighted that the deletion of Article 3(5), second paragraph, is not aligned with the approach followed by the Council in the FIDA proposal negotiations, as that exact sentence is previewed in its Article 12(4), on the authorisation of FISPs. In summary, and recognising that facilitating initial capital or own funds from being regarded as comparable guarantee directly in the text of PSD3, as intended by the PRES HU, might not be achievable given the strong opposition of other MS, PT would suggest going back to the approach previously envisioned by the PRES BE in leaving to national discretion what constitutes a comparable guarantee, removing that part of the mandates to be given to EBA, depicted in Articles 3(5) and 36(4a). In our view, this would allow each MS to accommodate that definition to their

PUBLIC

Question	MS reply
	respective market reality, making it perhaps the only possible solution to accommodate the distinct opinions in this regard. NL (MS reply): Yes. LV (MS reply): We support the drafting proposal. IT (MS reply): We agree with the proposed drafting suggestions for Articles 3.4 and in article 36(4) and article (36(4a)) PSD3 first paragraph but considering that – as summarized in the Discussion Note - it is not appropriate to consider a direct and linear substitution of capital requirements by the professional indemnity insurance, we suggest deleting the last paragraph in the article 3.5 and in the article 36(4a). We do not support the deletion - in article 3.4. and 36(4) - of: - the references to excesses, deductibles or thresholds, as we consider as appropriate and prudent to allow AISPs to cover any excess, threshold or deductible contained in the insurance or comparable guarantee and taking into account that these references are present in the FiDAR proposal. In this sense, we believe it is appropriate to request the EBA to

PUBLIC

Question	MS reply
	include indications on how AISPs can cover for excess/thresholds/deductibles in the EBA RTS; - the paragraph related to the monitoring of the coverage, as we believe it is appropriate and prudent to require AISPs to regularly monitor the coverage of the PII or comparable guarantee. As a second best, we deem important that the deleted references will be at least contained in the EBA RTS provided for at either art. 3.5 or art. 36(4a). IE (MS reply): We retain concerns that Article 36(4a) still refers to *'initial capital or own funds'* in the context of a firm that has no requirements for either. To count as a CET1 instrument/share premium, explicit NSA permission is required on first issuance (per CRR Article 26(3)) and thereafter explicit notification of subsequent issuances. As such we would prefer the term to be replaced by *"items that might otherwise count towards initial capital or own funds"*. HU (MS reply): We can agree with the direction of travel. HR (MS reply):

PUBLIC

Question	MS reply
	We agree with the proposed drafting suggestions. However, we propose to insert following clarifications in the proposed drafting in Article 3(5) and Article 36(4a): 3(5) For the purposes of point d), where ~~a payment institution~~ an undertaking that applies for authorisation to provide payment services as referred to in Annex I, point (6) holds additional initial capital ~~or own funds~~ beyond the level required pursuant to this Directive or own funds, the respective funds may be deducted from the minimum monetary amount of the professional indemnity insurance or comparable guarantee as referred in paragraph 4, or replace them, subject to the conditions to be set in the regulatory technical standards referred to above. 36(4a) For the purposes of point d), an undertaking that applies for registration as an account information service provider holds ~~any~~ initial capital or own funds ~~held by an account information service provider~~, the respective funds may be deducted from the minimum monetary amount of the professional indemnity insurance or comparable guarantee as referred to in paragraph 4, or replace them, subject to the conditions to be set in the regulatory technical standards referred to above. EL (MS reply): **EL:** We agree

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	DK (MS reply): We agree with the proposed drafting suggestions for Articles 3 and 36. DE (MS reply): • As we have argued in the past multiple times we do not agree with the proposal to hold initial capital / own funds as an alternative to a PII since initial capital does not cover risks in the same way as an insurance does, especially in case of insolvency of the payment institutions. In case of insolvency, initial capital/own funds might be depleted and are typically not excluded from the insolvency estate/assets. Hence in case of insolvency initial capital or own funds might not be available anymore to cover any risk. An insurance or comparable guarantee issued by a third party is usually not affected by the insolvency of the PI and the obligation of the insurer in case the insured events occur is independent of an insolvency of the PII. • However, in case we navigate towards a compromise that allows to hold initial capital / own funds as an alternative to a PII it is important for us, that the results of the EBA mandate to determine the interplay between PII and other forms of security will be applied consistently throughout the process to decide on the interplay between PII and comparable guarantees. In order to allow for consistent application, we propose the following drafting (changes in green):

PUBLIC

Question	MS reply
	Art. 3(5) PSD 3: "For the purposes of point d), where an undertaking that applies for authorisation to provide payment services as referred to in Annex I, point (6) holds additional initial capital beyond the level required pursuant to this Directive or own funds, the respective funds may be ~~deducted from~~ taken into account for the purpose of reducing the minimum monetary amount of the professional indemnity insurance or comparable guarantee as referred in paragraph 4, subject to the conditions to be set in the regulatory technical standards referred to above." Art. 36(4a) PSD 3: "For the purposes of point d), an undertaking that applies for registration as an account information service provider holds initial capital or own funds, the respective funds may be ~~deducted from~~ taken into account for the purpose of reducing the minimum monetary amount of the professional indemnity insurance or comparable guarantee as referred to in paragraph 4, subject to the conditions to be set in the regulatory technical standards referred to above." CZ (MS reply): In general we strongly prefer the approach previously envisioned by the PRES BE in removing the EBA mandate and **leaving to national discretion what constitutes a comparable guarantee**. In our view, this would allow each MS to accommodate that definition to their respective market reality, making it perhaps the only possible solution to accommodate the distinct opinions in this regard.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	In Article 3 we recall that under Article 6 there are own funds requirements therefore the wording should clearly refer to "own funds beyond the level required pursuant do PSD3". CY (MS reply): We have no comments regarding the proposed drafting suggestions to Article 36 and Article 3. BE (MS reply): BE: we continue to be in favour of accepting initial capital as an alternative to indemnity insurance and would urge the PCY to take this into account. AT (MS reply): Yes. However, for full alignment with FiDA, we still ask for a clarification that initial capital is not excluded from what a comparable guarantee is.
Q2. Do Member States agree with the proposed drafting suggestions on recital 65 and Article 43 PSR? If not, please provide an alternative or further suggestions.	MT (MS reply): Malta agrees with the drafting suggestions proposed in recital 65 and Article 43 of the PSR. SI

PUBLIC

Question	MS reply
	(MS reply): We agree with proposed change that there should be a single dashboard for FIDA and PSR covering all cases, not only when the PSU asks for it (proposed change to Article 43(2)(e) PSR). We also agree that withdrawing data access for a given account information service or payment initiation service provider should be free of charge for the payment service user (proposed change to Article 43(2)(b) PSR). With respect to aligning expressions related to time (proposed change to Article 43(2)(5) PSR), we would suggest double checking whether the wording is aligned with draft FIDA, where it seems that the availability of information is required in real-time. SE (MS reply): We welcome the adjustments made in article 43, especially in aligning it with the technical set-up of APIs. RO (MS reply): - PT

PUBLIC

Question	MS reply
	(MS reply): Despite further alignment to be introduced in subsequent stages of the negotiation of this file, as to approximate the drafting of Article 43 PSR with the one envisioned in Article 8 of the FIDA proposal, also liable to newer adjustments in trilogues, PT strongly supports the establishment of a single dashboard that would allow management of all data permissions pursuant to FIDA and PSR. NL (MS reply): We do not agree with the deletion of paragraph 2, point b and c and suggest the following text: *(b) withdraw the data; and* *(c) without undue delay, erase all data received as a result of the data access permission granted by the payment service user.* *2b. The payment initiation service provider or account information service provider concerned are not obliged to fulfil to the obligation under paragraph 2, point b and c, if this is not best interest of the payment service user, and they are able to demonstrate why that it is the case.*in the LV (MS reply): We do not have any additional comments; we support the drafting proposal.

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	IT (MS reply): In general, we agree with the proposed drafting suggestions, but we reiterate the necessity to guarantee the alignment with FIDAR, especially regarding the deletion of the sentence "upon the request of the payment service user" in Article 43(2). In general, we agree with the proposed drafting suggestions on recital 65 and Article 43 PSR which take into account our previous comments. However, we suggest: • to specify in Article 43(6) that the exclusion of liability of the ASPSP for the actions envisaged in paragraph 2 points (b) and (c), undertaken by the payment service user, does not imply that any other operators involved in the provision of the service (i.e. TPPs) could not be liable for such actions (see our proposal below); • to ensure a full alignment between FIDAR and PSR in relation to the use of "*in real- time*" and "*without undue delay*". **Article 43(6).** ***Without prejudice to the liability of third part providers, ~~T~~****t****he account servicing payment service provider shall bear no liability for the actions envisaged in paragraph 2 points (b) and (c) undertaken by the payment service user.*** IE (MS reply):

PUBLIC

Question	MS reply
	We are in favour of ensuring that the provisions of Article 43 PSR and those of the FIDA Regulation are aligned as far as possible; the drafting appears reasonable as it relates to PSR. HU (MS reply): We can agree with the direction of travel. HR (MS reply): We have no comments. EL (MS reply): **EL:** In the context of the deletion of points (b) and (c) of paragraph 2a of Art. 43 PSR and the corresponding explanation on page 4 of the presidency note, we suggest that a new point is added in paragraph 2a that foresees the explicit customer consultation on whether they want already collected data to be retained or not as a follow up action to the data access withdrawal i.e. *(b) explicitly consult the payment service user on whether the payment initiation service provider or account information service provider should retain already collected data and until when. The provider may retain the*

PUBLIC

Question	MS reply
	already collected data for the period indicated by the payment service user, if any, and erase them without undue delay aftewards. DK (MS reply): We generally support the intention to align the requirements for the permission dashboards between PSD3 and FIDA and if changes are made in PSR the FIDA team should be made aware. <u>Article 43(5)(a)</u> We are strongly supporting the proposed amendment to article 43(5)(a) and agree with the Presidency's reasoning as to why this is necessary. This provision is a key concern of ours. During these negotiations we have heard many say that PSR should be an evolution – not a revolution. However, the requirements currently being proposed fundamentally contradicts how the APIs functions as it would entail that the APIs should be able to push information. The PSD2-API solve the fundamental issue of secure communication between TPPs and ASPSPs. In all the myriad ways these APIs work, a session always entails 1) a TPP "calling" the API - which initiates a "session" – and 2) the API giving a highly specific and automatic response based on the specific call - hence ending the session. In no cases has a PSD2-API ever initiated a session. All sessions start with the TPP calling the API. Hence what is being proposed in the PSR, with ASPSPs informing a concrete TPP about consent withdrawal, is entirely outside the scope of what a PSD2-API can actually do.

PUBLIC

Question	MS reply
	In fact, in order for such communication to happen securely, the TPPs would have to build their own APIs on which the ASPSP must then be onboarded. Only in that way would an ASPSP be able to "provide" this information to the TPP. No such requirement for TPPs to develop APIs exists in the PSR – and it would also be very expensive to develop so we would not suggest this. Earlier we have heard an argument, that if the ASPSP does not provide the TPP with the information of a withdrawn consent, then the TPP has no way of knowing whether the consent has been withdrawn or if its just a malfunction of the API. However, we have been in dialogue with the sector in Denmark, and as we understand, they use several different labels for different reasons to deny a TPP access to specific PSUs data, and it would be possible to make the information of a withdrawn consent available to the TPP when calling the API. <u>Solution for article 43(5)(a)</u> We support requiring the ASPSP to "make available" information concerning a withdrawn consent, so that the TPP, when it attempts to access the particular PSU payment account, is informed of the consent withdrawal. <u>Article 43(2)(c)</u>

PUBLIC

Question	MS reply
	We do not agree to the introduction of the requirement that it should be possible to reestablish data access through the dashboard after a consent has been withdrawn. Here, we have a few concerns: • Even though it is technically feasible to reopen the access for TPPs, it would not be possible for the ASPSP to communicate to the TPP that data access has been reopened so the TPP would only know this if they try to gain access e.g. if the PSU actively uses their service. And if the PSU has to actively use the TPPs service anyway they could also reestablish their consent through the TPP flow instead. • What happens if the TPP has changed its terms and conditions within those 48 hours? Would the PSU then be covered by the old or new terms and conditions. • How does this requirement of allowing reestablishment of consent within 48 hours work together with the requirement for the TPP to delete all data on the PSU if the consent is withdrawn in the new 43(2)(e)(second subparagraph)(c)? <u>Solution for article 43(2)(c)</u> We would delete the possibility for reestablishment of consent through the dashboard within 48 hours. Reestablishment of consent would then happen by the PSU again going through the TPP flow. DE (MS reply): • We welcome the changes in Art. 43 PSR in order to clarify dashboard and data access provisions and in order to harmonise these provisions

PUBLIC

Question	MS reply
	with Art. 8 FIDA Councils mandate. Nevertheless, regarding the proposed drafting we have **three important remarks**: ○ The PCY suggests to delete Art. 43(2a)(c). The reasoning is that in case a PSU withdraws the permission the PSU may want the AISP to still make use of the already accessed data in the future. We see some merits in this proposal, however, it would create an inconsistency with FIDA. In fact, Art. 6(2)(b) and Art. 8(2a)(c) FIDA Councils mandate obliges data holders to delete accessed customer data when the permission has been withdrawn. From a data protection perspective the data should be deleted, at least after a defined storage period. Instead of deleting Art. 43 (2a) (c), the provision could be amended in a way, that it defines a limited period for the retention of the data after the PSU has withdrawn his permission. Accordingly, Art. 8(2a)(c) and Art. 6(2)(b) FIDA Councils mandate must be adjusted to avoid inconsistency with FIDA. ○ **In order to ensure that the FIDA / PSR dashboards align as closely as possible**, we request that the application of the guidelines for FIDA-Permission Dashboards through the JC ESAs, as provided by

PUBLIC

Question	MS reply
	Art. 8(5) FIDA Council mandate, should be included in Art. 43 PSR as well. We propose to introduce the following new paragraph 43(7): "7. The common guidelines develop by the ESAs, through Joint Committee, according to Art. 8 paragraph 5 FIDA should apply for the Dashboards developed under the provision of paragraph 1 as well." ○ We request a **deletion of Article 43(2)(c)**. In fact, there are multiple problems with this provision, e.g. what happens if the TPP has changed its terms and conditions within those 48 hours? Would the PSU then be covered by the old or new terms and conditions? Accordingly, Art. 8(2)(c) FIDA Councils mandate must be deleted and Art. 6(2)(b) FIDA Councils mandate must be adjusted. ○ We suggest to insert the negotiated changes of Art. 43 PSR of the Councils Working Group into the FIDA-trilogue in order to initiate necessary adjustments in Art. 8 FIDA to harmonise the dashboard and permission provisions within PSR and FIDA. CZ (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	The text is still under scrutiny. If needed we will provided drafting suggestions in the written comments. CY (MS reply): We have no comments for the proposed drafting suggestions of Article 43 and recital 65. BE (MS reply): BE: we agree AT (MS reply): Yes.
Presidency Discussion Note on use of ECB reference rates in PSR and CBPR2 (WK 3367/25)	
Q1. Could Member States accept the proposed amendments to Recital 50 and Articles: 3(56), 5(4), 13(1)(f), 20(c)(v) PSR and Articles 4(1) and 5(1) CBPR?	MT (MS reply): Malta believes that, given the absence of an obligation for the issuer's PSP to express currency conversion charges in monetary terms, imposing such a requirement on the acquirer's PSP offers limited value. As the payment services user (PSU) at the point of sale (POS) cannot compare two monetary amounts under these conditions, hence, this obligation would

PUBLIC

Question	MS reply
	likely result in minimal benefit. Additionally, the associated compliance costs for the acquirer's PSP should be considered, given the low added value of this requirement. SI (MS reply): We could accept the proposed amendments. SE (MS reply): We accept the proposal but would have preferred to use ECB rates as reference rates, as this information is more straightforward and comprehensible to customers. RO (MS reply): We agree with the proposal. PT (MS reply): PT can support the drafting of the Recital and Articles under appreciation, as those preview option 2a, which previously deserved our preference. Moreover, we also do not oppose both the newly used term for the applicable rates, to avoid the labelling of a benchmark administrator under

PUBLIC

Question	MS reply
	the BMR's scope, as well as the refined disclosure priorities prior to transaction initiation. NL (MS reply): Yes. LV (MS reply): We could accept the proposed amendments. LT (MS reply): We still believe that this topic should be analysed within CBPR review. The change from one reference rate to another might be costly for the market to implement, and the benefits of that for PSPs and PSUs are not proven. It raises the administrative burden. There are several administrators, therefore it is unclear how the comparability of currency exchange costs will be ensured, if different administrators are used as source of data. E.g. in case PSU compares mark-up by his bank and mark-up proposed by a merchant. IT (MS reply): Yes, we agree. IE

PUBLIC

Question	MS reply
	(MS reply): We support the removal of references to ECBRRs. HU (MS reply): Yes, we can agree. Yet at the same time it is necessary to clarify who produces the aggregated mid-market exchange rate and in what manner, as well as what the relationship of this indicator will be to the Benchmark Regulation. HR (MS reply): We have no comments. FI (MS reply): FI: We would prefer the use of the ECB rates, but as a compromise we can accept the PCY's proposal. DK (MS reply): In general, we find these options to be very complicated for some-thing which, to our mind, provides only limited benefits for the PSU. We do however agree that reference should not be made to ECB reference rates as

PUBLIC

Question	MS reply
	there are also currencies other than the euro. We would prefer simply a reference to the relevant central bank. DE (MS reply): We support the proposal and generally agree with the amended wording. The IOSCO principles are well-established on a global level, were e.g. endorsed as global standards also by the Financial Stability Board. Thus, we see benefits in referring to these established criteria instead of needing to set out criteria through new RTS, bringing additional administrative burden. CZ (MS reply): We strongly disagree with the new wording of Articles 5(4), 13(1) f) PSR and 20 c) (v) PSR. We are concerned that the whole system would be very costly for PSPs, especially smaller PSPs – several sources of real time information are required [new definition – Article 3(56)]. We think that some analysis of the possible costs should be done before this rule is introduced. **The reference to ECB rates under cross-border payments regulation works well and is easily understandable for users.**

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	In Article 5(4) PSR we are not in favour of compulsory adherence to IOSCO principles and we do not understand the limit of 10 minutes. In Article 13(1)(f) and in Article 20(4)(v) we do not understand how this will work in reality because Articles 13 and 20 have the nature of general information provided by PSP to PSU, which is more static in nature and often available on PSP's website. But this currency markup will always change due to market changes. So we would like to ask how it will work in practice. Regarding Articles 4 and 5 of the CBPR2 as it seems that these provisions are not interpreted consistently, we would appreciate clarification in the text that the exchange rate mark-up is part of the 'currency conversion charges'. CY (MS reply): We are supportive of the proposed drafting suggestions to Articles 13(1)(f), 20(c)(v) PSR and Articles 4(1) and 5(1) CBPR. AT (MS reply):

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	Yes.
End	MT (MS reply): ***End*** SI (MS reply): ***End*** SE (MS reply): ***End*** RO (MS reply): ***End*** PT (MS reply): ***End*** NL (MS reply): ***End*** LV (MS reply): ***End***

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	LT (MS reply): ***End*** IT (MS reply): ***End*** IE (MS reply): ***End*** HU (MS reply): ***End*** HR (MS reply): ***End*** FI (MS reply): ***End*** EL (MS reply): ***End*** DK

Presidency questionnaire following the WP meeting on 19 March 2025

From: MT, SI, SE, RO, PT, NL, LV, LT, IT, IE, HU, HR, FI, EL, DK, DE, CZ, CY, BE, AT **Updated: 02/04/2025 15:19**

PUBLIC

Question	MS reply
	(MS reply): ***End*** DE (MS reply): ***End*** CZ (MS reply): ***End*** CY (MS reply): **End** BE (MS reply): ***End*** AT (MS reply): ***End***