Subject: EMA draft Submission on PSD2 to European Commission Payment Systems Market Expert Group (PSMEG)

Date: 6 May 2022

PSD2 Review;

A Payments Systems Market Services Expert Group (PSMEG) was established by the European Commission some years ago, and the membership refreshed again in 2021. The first two meetings of the newly formed PSMEG have focused mainly on seeking input from industry practitioners on PSD2, as the Commission undergo their review process with a view to drafting amending/new legislation.

The Commission are inviting input from PSMEG members by 29 April on the topics set out below.

Separately the Commission are also expected to publish a set of consultations in mid-April:

1. General consultation on PSD2 and on Open Finance
2. Targeted consultation for industry stakeholders on PSD2
3. Targeted consultation on industry stakeholders on Open Finance

Stakeholders will have 12 weeks to respond to the consultations.

The external economic study by VVA will continue to run its course, with an interim report to the Commission due by 29 April, and a final report before the summer 2022. The EMA are preparing a separate submission for VVA for submission on 22 April.

European Commission questions and draft EMA position

Topic	Question	EMA response

Scope of PSD2	1. To what extent do you consider the scope of the PSD2 framework (and its exclusions) still fit for purpose in view of recent developments in the payment market? Do you see a need for regulatory changes and if so which ones?	1. PSD2 provides a common basis for different types of payment service providers ("PSPs") to offer payment services with common expectations for service levels and liability etc. It also sets out similar expectations for service levels and liability for different types of payment products. 2. This leaves provisions that relate to the attributes of different products to the legislative frameworks that define such products. The capital requirements and related directives deal with deposits, consumer rights in relation to deposits and banking obligations. Similarly, the second Electronic Money Directive ("EMD2") deals with the attributes of e-money, redemption obligation, distribution etc. The consumer credit directive addresses consumer rights and disclosure obligations in relation to the offering of credit products. 3. This approach has been effective and continues to be so. We do not believe there is merit in combining for example the e-money regime with that of payment services; one relates to the payment services while the other to the product. We strongly urge the European Commission not to pursue this approach as the consequences could be disruptive and unpredictable, and this is a mature industry that has been applying this regime for some 20 years. We set out below further issues in this regard. 4. The electronic money Directive seeks to regulate e-money as a product, it sets out issuance and redemption requirements, and defines e-money as a prepaid instrument. E- money is not a deposit or debt instrument, and consequently attracts its own legal treatment. It can be purchased and sold, and it is pegged against national currencies at par, with a right for redemption also at par. 5. It is modelled on cash, in that it is a claim against the issuer, and is intended to function in many instances where an electronic equivalent of cash is required. 6. As a prepaid instrument, the prudential risks associated with e-money go beyond those of settlement, which is that of immediate payment services, as funds are held by the issuer on an ongoing basis; pending a payment instruction. This is an important distinction that separates immediate payments from those that are prepaid and contemplated to be held on an ongoing basis. 7. Use of the e-money product to undertake payment services on the other hand is shared with all other payment instruments, and these are captured in PSD2. Risks associated with payment service provision are shared and EMIs comply with these, as do PIs and banks. 8. It is the prudential risks and controls associated with the issuance and redemption of e-money that are distinct, the legal nature of the instrument, and consequently the prudential obligations that mitigate these risks that merit a distinct framework.

		9. The e-money industry has put in place a detailed contractual structure that utilises the legal attributes of e-money, enables its distribution and creates business models that rely on these attributes. These have been effective for some 20 years. The utility of the instrument and its distinction from bank funds should therefore not be underestimated or degraded. 10. As described above, electronic money is an instrument, in the way that cash is an instrument or in the way that a deposit is a loan instrument. Payment is the process of transferring and accepting different instruments in fulfilment of payment obligations, or as a gift. 11. It is appropriate therefore to regulate banks under a consolidated banking directive, to regulate credit under a consumer credit directive and to regulate e-money under an e- money directive. Making payments with any of these three different types of products: debit, credit or a prepaid e-money instrument would however all be subject to common payments regulation under PSD2. 12. The main differences between payment institutions and e-money institutions concern the e-money instrument itself, and that it involves the holding of users' funds on an ongoing basis; whereas other payment products offered by PIs do not involve holding of balances on an ongoing basis. 13. There may however be benefit in cross referencing a recast PSD2 and EMD2 in a manner that enables providers of payment services to be able to vary their permissions to obtain an e-money issuing permission without having to apply for a new license entirely. 14. There are discussions in relation to the manner in which crypto asset products that are used exclusively for payment services such as those that could be backed by an EU fiat currency would be addressed by a revised PSD. We believe that whilst a level playing field is desirable; the Directive must take account of the distributed nature of such systems, the degree of oversight that an issuer or crypto asset service provider may have and the distinct attributes associated with crypto asset systems. The issuer for example is unlikely to have sight of transactions and cannot be responsible for consequent service levels. 15. Similarly, crypto asset service providers ("CASPs") that may execute transactions or hold 'accounts' for users may have distinct obligations in this regard. 16. The applications of a recast PSD2 to crypto assets will require careful assessment. 17. We have a number of comments in relation to Article 3 negative scope/exemptions: ● **Commercial agent exemption Article 3(b):** There is benefit in maintaining the commercial agent exemption, as it allows for bill payments and similar arrangements to

		be offered, where the merchant can manage the risk in a similar way to other commercial risks. ● **Technical service provider exemption Article 3(j) ("TSP")**: is of paramount importance. The exclusion as currently drafted is required and should form a key part of a redrafted PSD3, otherwise competent authorities will find their resources stretched to breaking point when attempting to supervise businesses that only have a tangential relationship to payment services. Additionally, overregulation would be detrimental to innovation and, ultimately, harm consumers as well as the economy. TSPs should be allowed to operate under an exclusion considering that they work with already regulated entities that are subject to payments regulation, which ensures protection of the customer and the payment system. ● **Limited network exemption Article 3(k):** there are divergences between the competent authority approaches towards notification; some NCAs have introduced notification processes that are comparable to an authorisation application; this of course undermines the benefit and intended objective of the exemption. The EBA Guidelines on the Limited Network Exemption have provided some clarity and harmonisation. However we consider that a more effective approach, and one that would encourage the single market in the EU, would be to provide the ability to passport an exemption to other EU member states, or simply to recognise the home member state's assessment as having authority across the EU. This is in line with approach in the E-commerce Directive (2000/31/EC), where the only competent authority ("CA") that can object to the use of the exclusion is the CA in the MS in which a service provider relying upon an exclusion is in incorporated (or otherwise established); host CAs would then accept this determination, although they would be free to report their concerns about the service provider's conduct so as to assist the host CA. At the moment service providers must notify each MS if they wish to operate under the limited network exclusion. In practice this has proven far too burdensome and unnecessary, particularly in light of the fact that MSs have adopted the same payments directive. Having to notify in this way and not being able to "passport" an exclusion will prevent innovative products - that could be beneficial for the economy and users - to get

Topic	Question	EMA response
		off the ground for the fear of regulation in some of the MSs due to the absence of a uniform approach by MS CAs. We also consider that PSD2 should be revised to address the dilemma faced by firms not knowing whether a product will be regarded as exempt once it reaches the notification threshold, and therefore refraining from offering services at all at the outset. It would be better for a simplified notification procedure to be made available at the outset, enabling clarity and regulatory certainty for business. ● **Article 37(2) relates to notification under Article 3(k)**: following from our comments above, and in relation to the home member state competent authority, the CA should be required to respond with any objections it may have within 2 months of notification, and if a CA does not respond within this period, it should be deemed to have agreed with the service provider's application of the LNE. The threshold trigger for the notification to the home CA should also be increased (from EUR 1 million) to when the total value of payment transactions executed over the preceding 12 months exceeds the amount of EUR 3 million in any MS to reflect the increased use of non-cash means of payment in the EU and the impact of inflation. Once a notification has been made, no further notifications should be required unless there are changes to the service that could impact the application of the LNE. ● **Electronic communication network exemption 3(l)**: we do not object to this exemption, and are supportive of the values being increased in line with inflation to enable users to continue to benefit from the convenience that it offers.

Topic	Question	EMA response
	2. Do you think that PSD2 ensures a level-playing field between payment service providers under the “same business, same risks, same rules” principle? If not, what would you consider should be changed?	As set out in our responses above, PSD2 places common obligations that different types of payment products must meet, and similarly that different types of PSs must implement. There are however distinctions that reflect a legacy payments infrastructure and which merit review, as well as poor practices that discriminate against non banking PSPs including those set out below. ● PIs and EMIs still have difficulty opening accounts with CIs, and most are subject to increasing de-risking practices. This is particularly acute in relation to safeguarding accounts, the conditions for which are set out in the PSD2. PSD2 does not do enough to stop CIs from using their position to place barriers to entry for PIs and EMIs. This issue has become acute and distorts the competitive landscape in favour of legacy credit institutions. ● Access to designated payment systems are restricted to non credit institutions and this should be resolved. ● The market for safeguarding by insurance appears limited with very little uptake so it would be helpful to get EC/regulator assistance with this. ● The Directive distinguishes the process for EMIs and PIs seeking to offer AIS and PIS services from that for credit institutions. The process, whether it amounts to notification or variation of permission should be identical. ● PSD2 introduced SCA related provisions that are overly prescriptive and reflect legacy technologies. These have furthermore been interpreted in divergent ways by different member states. New PSPs are able to deploy innovative means of addressing authentication and security and it would be more appropriate to set out security objectives than to define a technical solution in any legislation. In summary, PSD2 has made important strides in creating a single level playing field for different types of PSPs. There remain however important asymmetries: namely access to payment systems, access to bank accounts, the ability to introduce innovative means of authentication and in deploying services across the EU without onerous host member state requirements.

Topic	Question	EMA response
	3. Should specific services or market players (e.g. technical service providers) that are currently not in the scope of the Directive be included and made subject to supervision? Please specify which ones and why?	We concur with the approach of distinguishing technical services from payment services and propose that this continues.
SCA and payment fraud	4. Which recent new types of fraud have you observed in the payment market?	Instant payments have created opportunities for fraudsters deploying 'authorised push payment fraud' scenarios. These are payments correctly authorised by a user but relating to an underlying fraud; for example the fraudster may have substituted a bank account IBAN over which they have control, for a legitimate merchant's or it may be a payment solicited on a dating site etc. The ability of the fraudster to perpetrate the fraud and then move their funds across a number of accounts has made this attractive to criminals and the rate of fraud has risen significantly.Frauds include romance scams, money mules, goods not sent, Dear CEO fraud, sextortion, crypto fraud, investment fraud etc. This needs to be dealt with in a connected manner and it is not appropriate to place the responsibility for combating or compensating such frauds on the PSP, as the typology usually related to the underlying transaction and circumstances that are not visible to the PSP. The pSP may nevertheless play a part in a joint-up strategy for comparing such crime.

Topic	Question	EMA response
	5. Do you think that additional measures should be considered to tackle new types of payment fraud?	A confirmation of payee type service could be deployed for those participating in the SEPA schemes. Also a joint-up multi industry approach to dealing with fraud would be very welcome.

	6. Have any practices emerged in the payment market to avoid or to circumvent rules on strong customer authentication? If so, which ones?	In the absence of a questions on the merits of SCA provisions as a whole, we have taken the opportunity to address this below. We have provided commentary or the deployment of exemptions -(see paragraphs 4-9) that are provided in the RTS, and on trends in payment that seek to avoid channels that require SCA to avoid user friction (see paragraph 14). 1. PSD2 SCA rules limit the number of options/technologies available to payment market participants, meaning that most forms of SCA combine passwords (knowledge) with some sort of form of device-based authentication factor as possession (e.g., OTP, app-based notifications). The narrow interpretation of inherence-based SCA elements to include only a limited range of behavioural biometrics set out in the EBA Opinion (EBA-Op-2019-06) does not take into account the extensive experience of the payment sector in data-driven authentication, thus limiting the options available to firms. This has added further friction to PSU everyday interactions with payment accounts. The introduction of SCA has also impeded the ability of PSPs to deliver their services to PSUs with lower levels of digital literacy (or access to digital devices) or to vulnerable customers. We hope that a revision of PSD2 would largely focus on payment account security objectives rather than specify acceptable authentication elements. 2. EMA members have commented that the detailed SCA requirements and SCA exemption requirements prescribed in the regulatory technical standards have imposed costs on PSPs significantly beyond those originally envisaged. PSPs have expended time, effort and costs in understanding, preparing for and implementing solutions compliant with regulatory technical standards that became outdated as soon as they were published, hindering innovation and competitiveness in the market. Further changes to SCA should be focused on the outcomes, with industry determining the most appropriate measures to address fraud risk. 3. It is generally accepted that the initiation of payment transactions where SCA is applied involves more friction on the PSU side. Current SCA rules emphasise active authentication techniques, with explicit customer intervention; this approach limits choice and distorts the customer experience, when frictionless solutions might also be available. 4. Payment ecosystem participants (Acquirers, Issuers) have been trying to limit such friction through the balanced use of SCA Exemptions (Low Value, Trusted Beneficiary,

		Acquirer TRA, Issuer TRA). There has also been growing use of Merchant-Initiated Transactions (MITs) that are excluded from SCA requirements. 5. The requirement to apply SCA (and Dynamic Linking) has severely impacted the use of remote payments in certain Use Cases (Travel, Entertainment) that involve the use of service delivery intermediaries and aggregators. Many of these Use Cases continue to operate on the back of sector-specific SCA exemptions/waivers granted by local NCAs. 6. There are also good arguments to distinguish the application of SCA for payments involving corporate entities from those for purely retail payments; the former face more limited fraud risks. A risk-based application of dynamic linking for remote payments may reduce friction in use cases where the payer (or payee) is a corporate entity. 7. Small/medium size retailers are facing integration difficulties (and increased costs) to deploying SCA compliant solutions that allow the use of payment cards for remote/e-commerce payment transactions. These retailers are dependent on the support of Acquirers and Payment Gateways to deploy SCA-compliant payment solutions; acquirers and gateways have prioritised onboarding the larger e-commerce merchants and that has created a backlog of SME e-retailers that have limited access to such solutions. Total Merchant Service Charges (MSCs) incurred by e-retailers for SCA-compliant payment card solutions (e.g. 3DS v2.x) are higher than for previous, non-SCA compliant solutions. Increased Acquirer, Gateway, technology vendor (ACS) and Card Scheme fees contribute to the increased MSCs incurred by retailers. 8. Finally, whilst device manufacturers can provide compliant and seamless payment experiences, competing PSPs are blocked from accessing the more diverse OS/device-level controls because of Data Protection limitations. This has led to a distortion in competition in the market, as the level of friction has a direct impact on customer experience, and therefore on customer choice. 9. As stated earlier, SCA requirements have added friction to the everyday interactions of PSUs with payment accounts. The introduction of SCA has also impeded the ability of PSPs to deliver their services to PSUs with lower levels of digital literacy (or access to digital devices) or to vulnerable customers. PSPs are increasingly relying on less secure fallback channels (e.g. SMS, email) to complete PSU authentication for these customers.

		One possible solution would be to expand the scope of acceptable SCA elements to consider offline Use Cases or to service PSUs with lower levels of digital literacy. 10. Any future iterations of PSD2 should adopt a risk-based SCA application approach whereby Strong Customer Authentication is only applied where necessary (i.e. for high-risk payment account interactions). Such an approach would reduce the likelihood of legitimate transactions being declined and lower transaction abandonment rates. Allowing PSPs to deploy holistic user authentication frameworks that leverage "adaptive authentication" approaches to reflect the varying risks of attempted payment account interactions can preserve current SCA PSU security benefits while minimising friction in the customer experience. 11. The current treatment of all payment account interactions listed in Art.97(1) of PSD2 as a trigger for SCA appears to ignore the different risk profiles of such interactions (balance/history look up, payment transaction initiation/execution, account profile lookup/revision). This monolithic treatment of account interaction types has resulted in **multiple SCAs being performed by payment ecosystem participants to complete a single payment transaction**. Common examples include (i) The use of digital wallets to initiate a payment when both the wallet funding and the outward payment transaction require the execution of SCA or (ii) Combined AIS/PIS payment account accesses where a user first reviews account information before subsequently initiating a payment transaction. Payment industry participants have attempted to reduce the impact of this blanket regulatory treatment of different payment account interactions for SCA purposes by re-engineering payment flows and making use of SCA exemption or exclusions (e.g. increasing use of MITs). However, there is growing industry concern that this may not be a viable, long-term approach. The revision of Art. 97 (1) of PSD2 to afford greater PSP flexibility to apply SCA only in higher-risk transactions would offer a more viable alternative. Under the proposed revised treatment of account interactions, PSPs could still be required to apply appropriate customer authentication techniques (e.g. leveraging a single authentication element type) for lower-risk interactions. 12. Therefore, it would be useful to define more tightly the payer activities that must trigger SCA in Art.97 (1) of PSD2. Specifically, condition (c) should be revised to identify the actions - carried out over a remote channel - that must trigger SCA. The specification of

Topic	Question	EMA response
		SCA exemptions should continue to be included in Level 2/3 legal text that can be revised more frequently to address evolving fraud threats. 13. Additionally, the adoption of a prescriptive approach to implementing SCA in Level 1 text - rather than **setting out a set of security objectives to be attained** through the use of SCA implementation approaches- is likely to give rise to greater systemic payment ecosystem security risks. Attacks that target the specific SCA implementation can impact the entire payment ecosystem in the Union. The adoption of a prescriptive SCA implementation approach in Legal text that changes slowly can also limit innovation and the use of novel technologies that are showing potential to address payment security risks (AI, machine learning, behavioural biometrics). In this context, future revisions of PSD2 could consider allowing the use of alternative authentication mechanisms that can demonstrate equivalent strength to the current definition of SCA (e.g. one or multiple authentication elements of the same type coupled with additional PSP layered data) to attain the stated security objectives. 14. It is worth highlighting that Retailers and Acquirers are making increasing use of Merchant Initiated Transactions (MITs) including Direct Debits, Standing Orders to receive payment using transaction types that are excluded from the SCA requirements in PSD2. If MITs were moved within the perimeter of SCA requirements, the payment industry would suffer significant additional disruption. MOTO transactions are also currently out of scope of the SCA requirements in PSD2 unless a remote electronic channel is used to initiate such transactions. Our view is that MOTO transactions should remain out of scope SCA requirements since they experience low levels of fraud. 15. PSPs have commented that changes to SCA for e-commerce card payments have only recently been fully implemented (end of December 2020) and they will need some time to operate before meaningful conclusions can be reached as to their efficacy.

Topic	Question	EMA response
	7. Have you identified any fraud related security risks that are not addressed by the strong customer authentication requirements?	Authorised push payment fraud have been increasing and are not impacted by SCA; these utilise instant payment as a means of extracting funds quickly, and can vary from romance scams, to money mules, goods not sent, Dear CEO fraud, sextortion, crypto fraud, investment fraud. Please refer to our response to question 4 above.
	8. Are you already observing a reduction in fraud rates since the introduction of SCA?	EMA members report that they are seeing a reduction in fraud rates since the introduction of SCA, but there has been a sharp drop in successful completion of transactions, and also widespread use of exemptions in order to counteract the negative impact on user experience.
	9. Are merchants still observing a drop of their conversion rates?	There is some industry evidence[1] pointing to increased numbers of dropped/abandoned remote electronic payment transactions after the requirement for full SCA compliance started to apply to credit transfers (14th September 2019) and to payment cards (30th December 2020). Data on failed/abandoned transactions will be available at EU Retailers and Acquirers. There is also anecdotal evidence of similar rates of user abandonment at the point of failure in the application of SCA in other channels. [1] Card Scheme (MCI) data from Q1/Q2' 2021 indicates c.22% of all browser-initiated card transactions and to 53% of in-app card transactions failed to complete Issuer Step Up (Soft Declines).

Access to Payment Accounts	10. Have you identified a need for clarification or amendment to certain provisions of PSD2 (at Level 1) on the application of the requirements for access to payment accounts? Which Articles should be changed and why?	<u>Definition of 'payment account':</u> 1. Member State transposition of the definition of a 'payment account' into national legislation has led to differences in interpretation which presents complications for TPPs that are active in multiple countries. For instance, the assessment of whether a 'credit card account' falls within the scope of the PSD2 definition of 'payment account' varies by Member State. Consequently, TPPs providing services in multiple EEA countries may access credit card account data in one country, whereas banks in another country do not make this data accessible. 2. We have addressed the definition of payment accounts more fully in our <u>response to question 25 on definitions below.</u> <u>Providing access to 'payment accounts':</u> 3. As PSD2 implementation has demonstrated, ASPSPs have faced significant costs in developing compliant access interfaces to payment accounts. This has had particular impact on smaller ASPSPs who, as yet, have not seen significant demand for access by TPPs. Indeed, some of our Members have implemented, and now maintain, PSD2 compliant interfaces to payment accounts, and report no demand at all for access from TPPs. The requirement to provide an interface for data access by TPPs where there is no market demand, is a barrier to entry for small and niche innovative financial solutions. 4. If PSD2 rules on access to payment accounts are to be further developed, consideration must be given to the potential impact on smaller financial institutions, and whether the cost borne will result in the anticipated benefits to consumers and businesses. 5. There is an opportunity to introduce thresholds (volume of payment accounts, volume of transactions, etc.) below which ASPSPs could launch and operate payment services without having to provide TPP access to payment accounts data. This could also be

Topic	Question	EMA response
		coupled with an exemption process for those ASPSPs whose payment services and accounts see no demand from TPPs for access. <u>TPPs' access to data:</u> 6. TPPs' product propositions, and ultimate value, will only be fully realised by combining multiple financial data sets. The key barriers to developing and scaling TPP propositions is the data provider's willingness to share data, and a standardised mechanism for accessing data (such as APIs). Some of the challenges experienced by TPPs accessing data are: ● The mixture of different types of interfaces (APIs and MCIs) to access data and the operational complexity and cost this introduces for TPPs in maintaining multiple connections across all data providers, ● Poor stability and performance of PSD2 APIs, in some cases, ● Data parity between customer interfaces and dedicated interfaces: for example, some APIs don't contain FX pricing information, though they contain all other prices (to allow customers to compare products), ● 90-day re-authentication requirement: AISPs should be able to operate their services on a continuous unattended basis without the need for the PSU to re-authenticate with the ASPSP every 90 days (or every 180 days, as per changes currently proposed by the EBA in its CP 2021/32), ● Regulatory perimeter – PISPs should be able to access AIS data in order to manage their payment risk even if they don't intend to offer AIS products. ● Definition of 'payment account' - see also our response above regarding the differing interpretations of what constitutes a payment account and the subsequent fragmented approach to data access this can result in.

Topic	Question	EMA response
	11. Should the access to payment accounts be further standardised? Do you think that further mandatory elements should be defined at Level 2?	Further alignment of industry standards will help drive migration to PSD2 APIs because implementation complexity and cost will reduce, and ultimately encourage pan-European solutions to emerge. In particular, when considering payment initiation APIs, there are a number of areas where further standardisation would assist PSPs to develop the market for innovative PIS solutions. However, further layers of *legislation* at the API standards level could risk the technical neutrality of the regulatory framework and limit the opportunity for market innovation based on PSD2 APIs. There is also the risk that maximum harmonisation principles applied at the API standards level may result in a narrowing in scope of PSD2 API functionality, diminishing their usefulness and driving more functionality to the commercial API space. We therefore do not consider it necessary for a legislative solution in this respect.

	12. As regards the access to payment account provisions, do you see a need to further align PSD2 with other pieces of EU legislation, e.g. the General Data Protection Regulation (GDPR) and/or to further clarify the guiding material, e.g. the EDPB Guidelines? Please provide concrete examples, if any.	Article 94(2) of PSD2 provides: *Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.* This article merits amendment to either: 1. remove the term "explicit"; or 2. clarify that "explicit consent" in this context <u>does not necessarily</u> mean contractual consent. The EDPB Guidelines on the interplay between PSD2 and the GDPR interpret "explicit consent" in article 94(2) to mean contractual consent. Paragraph 36 provides: *"Explicit consent" referred to in Article 94 (2) PSD2 is a contractual consent. This implies that Article 94 (2) PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under the PSD2, data subjects must be made fully aware of the specific categories of personal data that will be processed. Further, they have to be made aware of the specific (payment service) purpose for which their personal data will be processed and have to explicitly agree to these clauses. Such clauses should be clearly distinguishable from the other matters dealt with in the contract and would need to be explicitly accepted by the data subject.* In the context of a PISP providing a payment initiation service ("PIS") to a merchant, which is the payee and not the payer in a payment transaction for the purchase of goods or services, the interpretation that "explicit consent" means "contractual consent" means that the relevant payment service user for the purposes of PSD2 94(2) is the merchant (i.e. the payee) and not the consumer or another type of purchaser (i.e. the payer). Such a PISP (that is one providing a PIS to a merchant) does not routinely enter into a contract with the payer because it provides its payment service to the merchant not the payer. A PISP enters into a contract with the payee and is, therefore, able to obtain the payee's "explicit consent" i.e. on the basis of the payee agreeing to certain clauses legislating for such consent in the framework contract. PSD2 article 94(2) must be clarified to ensure the Guidelines are not misconstrued as requiring a PISP that provides PIS to merchants to enter into contracts with a payer in order to obtain the payer's explicit consent. <u>This is not required under PSD2 94(2) nor practically feasible.</u> The payer

Topic	Question	EMA response
		does not enter into a contract with such a PISP. The payer has limited interaction with this type of PISP. Such an interpretation would be incorrect and restrict the PISP's ability to comply with PSD2 94(2).

Authorisation of PIs and Supervision of PSPs	13. Do you consider that the provisions on authorisation (licensing) of providers of payments services in the PSD2 are adequate? Which provisions, if any, should be revised? Do you see potential for simplifications?	**Authorisation in general**: 1. Authorisation requirements introduced by PSD2 amounted to an increase in the obligations that firms were expected to comply with. Since that time, additional obligations have been introduced or elaborated, such as those in level 2 text issued by the EBA and by NCAs, as well as general expectations relating to issues such as outsourcing, operational resilience, wind down planning, consumer protection including vulnerable customer policies etc. We strongly urge the Commission to refrain from further regulatory intervention in the prudential, conduct of business and supervisory framework. 2. If there is a perceived need for greater scrutiny, we suggest this is addressed by way of supervisory oversight rather than further regulatory obligations. Similarly, greater harmonisation of supervisory practices would be helpful, together with NCA cooperation to reduce the need for host member state intervention. 3. Any additional authorisation proposals should be supported by a robust cost/benefit analysis. 4. There is currently a discrepancy between the manner in which a credit institution can seek to take on the permissions of AIS and PIS and that PIs and EMIs. We suggest a more uniform approach where all three types of institutions are treated in a similar manner; either requiring simple notification to add such a permission, or requiring a variation of permission. There should not be a discrepancy as this could translate into a competitive or time advantage for one type of institution over another. **Safeguarding requirements** 5. The PSD2 requires outstanding funds for both PIs and indirectly for EMIs to be safeguarded when the safeguarding conditions are met. The main means of safeguarding is to place the funds in a separate account with a credit institution. PSD2 then delegates the criteria for determining the permissible credit institutions to home member states. This is often interpreted as being restricted to EEA authorised credit institutions. 6. This restriction is inflexible and does not take into account the needs of diverse business models that PSPs have, particularly those with a global presence, and that operate on a 24-hour basis. EMI and PI transactions take place in real time, but often the CIs holding safeguarding accounts only operate during banking hours. It would assist business

Topic	Question	EMA response
		enormously if eligible credit institutions for the purpose of safeguarding are set out more broadly in the legislation, including credit institutions authorised outside of the EEA, and that this is harmonised in level 1 text. **Additional issues** 7. Firms need greater clarity regarding the type of secure, liquid and low risk asset that safeguarded funds can be invested in. There is a need for diversification and limited flexibility to enable a limited revenue to be generated in order to contribute to the cost of safeguarding. 8. EMIs and PIs should additionally be permitted to safeguard customer funds at central banks, removing investment risk altogether, and assisting in the resolution of part of the de-risking challenges that are faced by the industry.
	14. Has the use of the waiver (Article 32) facilitated the market entry for small payment institutions? In particular, do you think the level of the threshold set in Article 32 is appropriate?	The PSD2 waiver and notification requirement has operated effectively, and allowed smaller institutions to operate, scale up, and then apply for a full licence. It is a useful tool to allow market entry for new players.
	15. Do you see a need for changing the prudential requirements (in particular Article 7- 9)? If so, which one(s), why, and how?	We do not see a need to amend capital requirement provisions; the manner of calculating own funds however varies considerably by member state, and there could be better alignment in this regard. There is a tendency to err on the side of caution, resulting in onerous obligations that may deprive a business of working capital without contributing significantly to risk mitigation. Operational risk is particularly hard to measure, and it may not necessarily be addressed by increasingly onerous own funds requirements.

Topic	Question	EMA response
	15. Are there elements in the supervisory framework that applies to credit institutions (CRD/CRR) which should be extended to payment institutions, such as group supervision?	We are not aware of any shortcomings in relation to the current supervisory framework. We are not aware of any systemic failings or risks that have led to failings at an industry-wide level. The EMA has branches in 6 EU member states, and has observed national supervisory oversight of the e-money and payments sectors increasing significantly over recent years. NCAs are increasing their supervisory engagement with the industry, their understanding of the market is greater than before, and the degree of scrutiny of firms is higher. In this context, we do not see which aspects of the supervisory framework applicable to credit institutions would be suitable or appropriate for the PI/EMI sector. EMIs and PIs do not take deposits and do not utilise user funds for any purpose including lending. The nature of the risks associated with the banking sector is significantly different. Both EMD2 and PSD2 have been calibrated to the risks associated with the respective activities. In addition, the new PISA framework introduced by the ECB will add a layer of oversight that will capture the more significant institutions.

Topic	Question	EMA response
	16. Does the EU-passport regime work adequately? Has it fostered the offering of pan-European payment solutions? Have you identified any obstacles, e.g. regarding the interaction with the competent authorities?	Although PSD2 is a maximum harmonisation directive, member states can adopt different policies when applying the supervisory regime. One particularly important choice relates to that of calculating own funds. The three methods of calculation can give rise to significantly differing outcomes. The choice between using turnover (method B) and income (method C) as own fund indicators is particularly important and is subject to variations in business model and business practices. Some NCAs adopt a non-flexible approach and result in discrepancies in the capital charged from one member state to another. **Passporting** We also note the variation in supervisory practices and reliance by host member states on engagement with passporting firms rather than on cooperation with home member state supervisors. This means that passporting on the basis of freedom to offer services is often interpreted as one through right of establishment; often by requiring a local contact points to be appointed through PSD2 or AML legislation, or regarding distributors as establishments, or regarding outsourced services in a similar way etc. This then results in member states applying local reporting and engagement obligations, and ultimately leads to a compromise of the value of the single market. The single market fragments and service offerings are restricted to the biggest member state markets by size. We encourage the European Commission and other European policymakers to address harmonisation in a more inclusive manner, addressing soft factors such as cooperation and data sharing in a more robust manner, removing the need for host member states to seek to impose obligations, to seek a finding of establishment, and to regulate at a host member state level.

Topic	Question	EMA response
Transparency of conditions and Information Requirements	17. To which extent have transparency and information requirements improved user convenience and contributed to an informed user choice among different payment products?	Overall information disclosure obligations are helpful; we have however set out in our response to question 18 below a number issues that merit review and amendment.

	18. Do you see a need for legislative changes in Title III? Which provisions and why?	1. The MS derogation regarding the treatment of microenterprises as set out in Art. 38(2) PSD2 merits review with a view to removal. Microenterprises are not consumers and need not be treated as such. Furthermore, this derogation and the matching one in Title IV create inconsistent COB treatments across the EU as not all MSs apply the derogation (and some apply it in one PSD2 title but not the other). This will also ensure consistency with the approach to businesses in EMD2 with respect to holding e-money and consistency with the general commercial approach of the freedom to contract. 2. Article 42(1) regarding a reduced information requirement for low-value payment instruments and e-money: the values in this article should be increased to reflect at least inflation if not increased to an individual transaction limit of EUR100, and spending/storage limits of EUR500. 3. Article 42(2): For national payment transactions, we have not found any significant argument for MS to reduce the limits set out at Article 42(1). There are however good reasons to double this value, and this should continue to be available. We similarly propose that the e-money storage limit should be increased to EUR1,000 to reflect the passage of time and inflation. 4. Regarding Article 51(1) and any other reference to providing information or providing information on a durable medium: providing information through an app or a dedicated online interface (e.g. online account) should be treated as providing information on a durable medium. Consumer practices have changed and it is beneficial to amend provisions to keep up with consumer behavior. For example, consumers today will use their app notifications the way letters, or even emails, used to be used a few years ago. Consumers have access to their online interface with all the information about the transactions in one place and use the interface to keep informed. Notifications sent to these online interfaces/accounts merit treatment as a durable medium. 5. Article 54(1) sets out the means by which unilateral changes to a framework contract are permitted. Thi is an important feature and must be kept, and furthermore, MS consumer protection law should not be permitted to override this important tool used to manage contractual relationships with PSUs. The PSD2 already provides the necessary safeguards and the intervention of MS laws would create inconsistent (and differing) treatment across

Topic	Question	EMA response
		the EU. Some MSs attempt to implement (or are already implementing) separate rules to take away the unilateral change right (when agreed in the contract) and replace it with a requirement to always obtain an agreement from the PSU when introducing changes to the framework contract. This requirement is disruptive and is not beneficial to consumers, who may forget to accept the changes and then find themselves in a position where their cards/accounts are cancelled, DDs do not work and similar, when this is not something they wanted. PSD2 provisions already protect the consumer by making sure they are notified fully of any changes in advance. Introducing an obligation for consumers to actively accept proposed changes in order to continue using the service is unnecessary and burdensome. Making sure they are notified correctly protects them and then they should have a choice to exit the contract or continue without doing anything (i.e. unilateral change). 6. If the change is beneficial to the consumer, the notice period should be less (e.g. two weeks (general consumer protection law notice period)). This ensures any beneficial changes will be introduced swiftly for the benefit of the consumer.
	19. Should any additional information be provided to payment service users before initiating a payment other than mentioned in the current provisions, i.e. Article 45 and 52?	We are not aware of any further information that has been lacking or that is requested by PSUs.

Topic	Question	EMA response
	20. With regard to one-leg transactions, should there be an obligation to disclose currency conversion costs before and after a payment transaction?	We do not provide comments on this issue.
Rights and obligations of customers	21. Do you see a need for changing the derogation for low value payment instruments and electronic money in PSD2 (Article 63)?	• **Article 63(1):** reduced obligation requirements for low-value payment instruments and e-money - the values in this article should be increased to reflect at least inflation if not increased to an individual transaction limit of EUR100, and spending/storage limits of EUR500. • **Article 63(2)**: we make similar comments to those made above under Title III. For national payment transactions, MSs should not be permitted to reduce the limits, but only to double the amounts in Article 63(1). Same comments as above for Title III. The e-money storage limit should be increased to EUR1,000 to reflect the passage of time and at least the inflation.
	22. Do you see merit in introducing maximum limits for the amounts to be blocked on the payer's payment account when the exact transaction amount is not known in advance (Article 75)?	We do not see merit in setting a limit, the amount will vary depending on the use case, and the impact will depend on the funds available and the needs of the user. It is better to leave this for the parties to agree.

Topic	Question	EMA response
	23. Is it appropriate to apply a limit to the maximum execution time in 'one-leg' transactions, taking into account developments such as the implementation of SWIFT gpi and the targets established in the G20 Roadmap on cross-border payments?	We consider that the scope of article 82 should not be increased to include one-leg-out transactions. PSD2 legislates for payment services within the European Union. There may however be initiatives that seek to standardise practices on a global basis, and the Commission should seek to adopt these where they are consistent with the objectives of the PSD. These include FSB developments in this regard.

Topic	Question	EMA response
Other issues	24. Derogations and consumer liability	1. **Article 61(1):** this derogation is better removed, and non-consumer PSUs and PSP should be free to contractually agree to disapply the provisions of the domestic implementation of Article 102 (ADR procedures). This would give the businesses the same freedom to agree their own bespoke ADR mechanisms as in other commercial arrangements without the PSP being caught in a government-mandated system that is consumer focused and not business focused, and that operates without the benefit of the court systems' legal expertise and the intermediation of lawyers. 2. **Article 61(2):** the MS derogation regarding the treatment of microenterprises is better removed. Microenterprises are not consumers and should not be treated as such. Furthermore, this derogation and the equivalent provision in Title III create inconsistent COB treatments across the EU as not all MSs apply the derogation. This will also ensure consistency with the approach to businesses in EMD2 with respect to holding e-money. 3. **Article 74(1):** the maximum liability for a payer resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument should be increased to reflect inflation and also to discourage careless or reckless behaviour on the part of the consumer - we suggest a new limit of EUR150. Furthermore, MS should not have a derogation permitting them to reduce the maximum liability as this creates differing treatment across the EU for different consumers.

Topic	Question	EMA response
	25. Definition of Payment Account	The case of *Bundeskammer für Arbeiter und Angestellte (Austria) v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG* has produced an unusual outcome, in that the PSD2 definition of a payment account is being interpreted under the Payment Account Directive Directive 2014/92/EU ("PAD"), rather than within PSD2 itself. It would be helpful for the definition of payment accounts to be clarified within PSD itself. The CJEU case suggests that accounts that are intended to be captured in PSD2 under access obligations set out at Articles 65-67 are informed by the definition at Article 1(6) of the PAD which require payment accounts to have a certain number of functionalities, which are: (a) placing funds in a payment account; (b) withdrawing cash from a payment account; (c) executing and receiving payment transactions, including credit transfers, to and from a third party. This relevant functionality that was utilised in the case related to the third limb (c) which provided for transfers to be possible to third parties. It is however possible to suggest that other functionalities must also be present. The scope of accounts that are captured is interpreted differently in different member states, with resulting uncertainty over which accounts are available to PIS and AIS providers. It would be helpful to clarify scope, and for this to be set out in a pragmatic manner. Please also see our further response to Question 31. Whilst this response relates to PSD2, we would also bring the Commission's attention to the varying interpretation of accounts falling within the PAD, where countries such as Germany, Poland and Lithuania have taken an inclusive approach that has brought e-money accounts within scope of PAD obligations, requiring for example the provision of Fee Information Documents and Statements of Fees, even though there is no basis for comparison with current account products.

Topic	Question	EMA response
	26. Categories of payment services	There appears to be some inconsistency in how member state NCAs interpret the different payment categories; the following are some examples: - Some require permissions 1 or 2 or 3 if payment accounts are used in relation to permissions 4 or 5, as these permissions make mention of payment accounts; we believe this is an overly restrictive interpretation and that permissions 4 and 5 both allow for payment accounts to be operated implicitly. - Acquiring of payment transactions is sometimes associated with card payment transaction acquiring only, although acquiring of transactions may utilise other payment instruments including bank transfers or mobile wallet payments; clarity on the generality of this provision would be helpful. - Account information service is defined as relating to the provision of consolidated information on accounts held in a number of places. This reflects the nature of AIS services at the time of drafting of PSD2, but today only reflects a small part of such services. It would be better to define this term more generally, for example as services that involve access to payment account information held by an ASPSP. The current definition is currently resulting in restrictions on innovation and AIS service offerings in member states. - The definition of 'account information services' also refers to the provision of information on account(s) held with another PSP or more than one PSP. Some PSPs offer accounts that can only be accessed (for example, to view balance and/or transactions) by PSUs via an interface (such as an app) developed and maintained by a third party. It would be helpful to clarify that such third parties are not engaging in account information services when providing account information on behalf of a PSP, on an account held with that PSP.

Topic	Question	EMA response
	27. TPPs' access to data	TPPs' product propositions, and ultimate value, will only be fully realszed by combining multiple financial data sets. The key barriers to developing and scaling TPP propositions is the data provider's willingness to share data, and a standardised mechanism for accessing data (such as APIs). Some of the challenges experienced by TPPs accessing data are: ● The mixture of different types of interfaces (APIs and MCIs) to access data and the operational complexity and cost this introduces for TPPs in maintaining multiple connections across all data providers, ● Poor stability and performance of PSD2 APIs, in some cases, ● Data parity between customer interfaces and dedicated interfaces: for example, some APIs don't contain FX pricing information, though they contain all other prices (to allow customers to compare products), ● 90-day re-authentication requirement: AISPs should be able to operate their services on a continuous unattended basis without the need for the PSU to re- authenticate with the ASPSP every 90 days (or every 180 days, as per changes currently proposed by the EBA in its CP 2021/32), ● Regulatory perimeter – PISPs should be able to access AIS data in order to manage their payment risk even if they don't intend to offer AIS products. ● Definition of 'payment account' - see also our response to Question 25 above regarding the differing interpretations of what constitutes a payment account and the subsequent fragmented approach to data access this can result in.

Topic	Question	EMA response
	28. Operational and security risks	1. **Operational and security risks** are only referenced at a high level in Art.95 of PSD2. The risks are detailed in Level 1 text (the EBA Guidelines on ICT and Security Risk Management). These Guidelines cover an appropriate range of operational and security risks; they are next scheduled for review in 2022. There is some uncertainty on the treatment of Operational Resilience risks due to the publication of the EC DORA Draft Regulation. An area where additional regulatory guidance is required is the exchange of risk information from NCAs and the ECB to regulated entities. It is not clear at present whether the operational risk monitoring and incident reporting requirements that the DORA regulation introduces are to be treated as part of the operational and security risk frameworks that regulated entities have already deployed to comply with the relevant requirements in PSD2. 2. **We are in favour of IT security related provisions being set out at a high level, as objectives rather than specific solutions**. In the event that this is not achieved we suggest that: ● Level 2 RTS/GLs etc are impacted by product and market developments on a continuous basis; the EBA should therefore be given a mandate to implement changes on a regular basis to keep pace with market changes, without the need for Level 1 PSD2 text changes. ● Similarly, the process of producing RTS and GLs, then clarifying via Q&As, often over several years, is out of step with business and market needs, and requires revision to enable speedy responses, that are informed by business and market needs, and which provide an explanation of how market issues have been addressed.

Topic	Question	EMA response
	29. Reporting obligations	**Reporting obligations draw considerably on firms' resources**, with little visible impact on supervisory effectiveness or on policy. ● We request increased coordination and alignment between NCAs, the ECB and EBA regarding reporting requirements, and some means of providing feedback on the outcomes of data collection exercises. ● There have also been recent changes to the data elements that are reported and this has given rise to considerable additional resource requirements. Although the burden has been reduced somewhat by combining the two reports at national level, it would be helpful if EU policymakers could guarantee that the data collection would remain static for some years to come, in order to reduce the cost and resources needed for the recent substantive changes that were introduced twice in the course of 2 years.