Electronic Money Association
68 Square Marie-Louise
Brussels 1000
Belgium
www.e-ma.org

Eric Ducoulombier
Head of Unit,
Retail Financial Services European Commission,
DG FISMA B.3 Rue de Spa 2
Brussels,
Belgium

1 November 2023

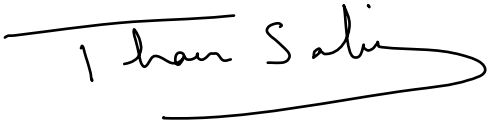
Dear Eric

Re: EMA response to European Commission proposal for a draft Regulation on payment services in the internal market and amending Regulation (EU) No 1093/2010 and proposal for a Directive on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. Most members operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

I would be grateful for your consideration of our comments and proposals.

Yours sincerely,



Dr Thaer Sabri
Chief Executive Officer
Electronic Money Association

EMA response

The Electronic Money Association (EMA), established in 2001, is the trade body for European and UK Crypto Assets Providers (CASPs), Payment Institutions (PIs), E-Money Institutions (EMIs), and Credit Institutions (CIs) providing innovative payments.

The EMA supports the European Commission's revised Payment Services Directive ("PSD3") and Payment Services Regulations ("PSR"), as representing a step towards improving the experience of payment service users across the EU, as well as ensuring the objectives of PSD2 can continue to be met.

We welcome the European Commission's draft proposed Regulation, and acknowledge the efforts made by the Commission to address a number of areas under the existing Payment Services Directive that have not met the original objectives.

In particular, we welcome the Commission's proposals to improve the access of EMIs and PIs to bank accounts, including holding safeguarding accounts at Central banks. We also welcome the provisions opening up access by EMIs and PIs to the payment and settlement systems in order to create a level playing field for payment services in the EU, encourage more competition, resulting in improved products for customers, both individual consumers and businesses.

We also welcome a number of changes that have been introduced to the open banking provisions, allowing for the application of a more proportionate regime, as well as removing existing barriers for TPPs.

Please find below an overview of the issues of most impact on the e-money, payments, and crypto asset sectors, and on which we would very much welcome your support throughout the policymaking process:

1. Re-authorisation requirements/transition provisions
2. Safeguarding
3. E-money services in scope
4. Definitions and use of agents and distributors, passporting
5. Negative scope (commercial agent exemption, Limited Network Exemption, Technical Service Provider exemption)
6. Access to payment accounts for EMIs and PIs
7. Access to payment schemes
8. Fraud, Confirmation of Payee service and data sharing
9. Fraud and PSP liability attached to impersonation scams
10. Administrative sanctions
11. Open banking
12. Conduct of business (Title III) issues, including:
    a. PSP liability for unauthorised payments
    b. MS option on refund rights
    c. pre-authorised payments
13. Strong Customer Authentication provisions

EMA response

1. **Re-Authorisation requirement/transitional provisions**:

Article reference: PSD3 Articles 44, 45

EMA comment: Transitional measures will require firms authorised under PSD2/EMD2 to submit an application for a licence under PSD3 at the latest 24 months after the PSD3 entry into force.

Taking into account the PSD2 experience, we are concerned that a full re-authorisation process for existing PIs and EMIs will be lengthy, resource-demanding for both firms and the Member State national competent authorities ("NCAs"), and disproportionately burdensome to any benefits achieved.

Article 44(2) provides Member States with an option to authorise PIs automatically if the NCAs *"have evidence that those payment institutions already comply with Articles 3 [which sets out the requirements for authorisation applications] and 13 [which deals with conditions for granting an authorisation]"*. A similar allowance is provided for automatic re-authorisation of EMIs, under Article 45(3), where NCAs *"have evidence that the [EMIs] concerned comply with this Directive"*. Automatic re-authorisation should be a requirement, rather than a Member State option, with NCAs required to assess compliance with the new PSD3 authorisation requirements only. This will facilitate harmonisation of the requirements across the EU and will reduce the burden on the NCAs and PIs without compromising the new standards set out in PSD3.

In addition the evidence that EMIs may be required to provide for re-authorisation purposes should be (as for PIs) limited to compliance with PSD3 Articles 3 and 13, not the entire Directive. Considering the harmonised authorisation standards for both PIs and EMIs under PSD3, we see no reason why EMIs should be subject to a higher evidentiary burden in obtaining re-authorisation.

Finally, we are reminded of the importance of Member States being adequately resourced to process re-authorisations in an expedient manner. For example, in some Member States the authorisation process has taken, for some applicants, as long as 26 months, i.e. more than the entire length of the transitional period envisaged for PSD3 authorisations; the influx of re-authorisation applications to meet the transitional deadlines will undoubtedly add to the the time it already takes to process the business-as-usual applications and would likely cause significant disruption to the NCA's activities, including potential detriment to their supervisory work.

Recommendation: automatic reauthorisation should be a requirement for all Member States rather than an option, recognising existing licences and addressing only new provisions in legislation.

2. Safeguarding

Article reference: PSD3 Article 9

EMA comments:

(a) Article 9(2) provides for a new obligation on PIs to *"avoid concentration risk on safeguarded funds by ensuring that the same safeguarding method is not used for the totality of their safeguarded funds".*

More clarity is needed on what is intended for varying the "safeguarding methods" to be used by PIs.

(i) For example, if the expectation is that PIs must use a combination of the segregation and insurance/comparable guarantee methods, this will not be feasible given that the insurance/comparable guarantee method has had limited uptake due to insufficient market offering of suitable insurance policies to meet the requirements.

(ii) On the other hand, combining safeguarding at a bank account with safeguarding by investing in secure, liquid, low-risk assets could also pose problems, especially where the criteria for the assets to be considered to be sufficiently secure, liquid and low-risk is too restrictive, or where the size of the business does not support such treasury practices.

(iii) The impact of credit institution **derisking** practices**,** and difficulties for PSPs in obtaining safeguarding bank accounts in the first place are growing more and more acute over time. This makes the draft PSD3 Article 9(2), which requires PIs to *"endeavour not to safeguard all consumer funds with one credit institution"* almost impossible to comply with.

Additionally, permissible investments, the type of secure, liquid and low risk asset that safeguarded funds can be invested in, would benefit from diversification and some flexibility to enable a limited revenue to be generated in order to contribute to the cost of safeguarding (which can be significant given the minimum fees levied by credit institutions for providing a safeguarding bank account, which are required under both safeguarding methods). See also paragraph (c) below in relation to UCITS and MMFs.

The costs of maintaining several safeguarding bank accounts and/or the insurance /comparable guarantee policy (in addition to safeguarding accounts) will be significant, particularly for smaller PIs. Furthermore, managing the various safeguarding arrangements is time consuming and costly, with the risk of error increasing significantly. Firms who use the insurance method to safeguard report that the annual premium is not insignificant, and the process to renew the policy is time consuming and lengthy.

Recommendation: We therefore suggest making such diversification, based on the use of both safeguarding methods to reduce concentration risks, or of multiple bank accounts, an advisory provision rather than a requirement, and qualifying this with ”where appropriate” to only capture instances where the size of safeguarded funds would logically justify this approach. As an advisory provision, the responsibility to reduce concentration risks would form part of the firms' risk management arrangements and would be assessed alongside controls such as the initial and ongoing due diligence performed on credit institutions by firms as part of their selection process.

Similarly, the wording to “endeavour” not to safeguard all consumer funds with one credit institution should be maintained or strengthened to allow firms to make a decision based on their risk management processes and balance operational complexity, and associated additional risks of error, where multiple safeguarding bank accounts are maintained.

Finally, we consider that this requirement should only be adopted where PIs are also given the opportunity to safeguard at the central bank, as set out below.

(b) Safeguarding at a central bank

EMA comment: We strongly support the option for PIs to safeguard customer funds in accounts at central banks. (Article 9(1) PSD3).. We believe that access to central bank accounts is essential and will bring many benefits: reducing systemic and investment risks associated with safeguarding with third party banks, increasing competitiveness in the payment services industry, and increasing customer confidence in the services offered by PIs. It could finally provide real alternatives to having to rely on commercial banks for safeguarding, alleviating de-risking issues, but also more importantly, reducing the unlevel playing field in the ability to use central bank services. For these same reasons we urge to also review and align Article 54 (a) of MiCA to properly reflect the broadening of permissible safeguarding to accounts with central banks. Article 54 (a) of MiCA requires issuers of EMTs to deposit at least 30% of funds received in exchange of issued EMTs in separate accounts in credit institutions. The broadened scope for safeguarding of customer funds must be read across to this MiCA provision. Not doing so would cause an unjustified regulatory discrepancy between traditional e-money and EMTs, thus, run counter the principle of technology neutrality effectively at the expense of holders of EMTs not benefitting from the additional mitigation of safeguarding-related risks. Beyond the alignment of Article 54 (a) MiCA it should also be made clear that any exposures to central banks are to be disregarded for any limitations of concentration risks.

However, central banks' exercise of discretion in deciding whether to offer safeguarding accounts in each Member State could undermine the harmonisation objectives of the Directive.

Recommendation: We propose that safeguarding accounts at central banks should be made available to PIs across all Member States, **as a right**, with appropriate safeguards to ensure that the account opening criteria is objective, proportionate and non-discriminatory as regards PIs whilst appropriately managing the risks to the central banks. As with existing access for Credit Institutions, this would not prevent central banks from being able to apply application criteria to manage any risks they deem necessary.

(c) Secure low risk assets: The provisions of Article 9(1) PSD3 refer to investment of safeguarded funds in 'secure and low-risk' assets "as determined by the competent authority of the home Member State". This wording is consistent with that in previous legislation. This approach to safeguarding is becoming more common in industry particularly as firms seek to diversify away from bank deposits. It has however suffered a significant setback due to the manner in which it is expressed in the Second Electronic Money Directive.

Implementation by Member States has limited investment of users' funds to (i) securities that have a particular capital treatment (defined in accordance with particular legislative provisions) and (ii) to UCITS which are comprised "solely" of such securities.

The use of the term "solely", as it relates to potential investments in UCITS, has proven to be problematic. This is because UCITS will always need to hold some form of cash or cash equivalents, for example in order to manage liquidity and to settle redemption requests from investors, or to pay fees and expenses, and accordingly cannot meet the "solely" criterion, investing only in the relevant securities. This has also posed issues for proposed investments in money-market funds ("MMFs"), which are some of the most secure, liquid and low-risk investments in practice but which, by requirements set down in other EU laws (namely the MMF Regulation), are legally required to hold certain assets other than securities but which would be regarded as 'secure and low-risk' (such as cash, and certain other derivatives).

Industry believes that a practical and purposive reading of the E-Money Directive could, in principle, permit investments in MMFs, but at least one central bank has not accepted this position on the basis that MMFs do not, in its view, invest "solely" in the relevant securities. This has the effect of excluding MMFs from possible means of safeguarding, which could not have been the intention.

The European Banking Authority ("EBA"), in its own review of PSD2 recognised this issue, stating that "one of the specific issues identified by the EBA was the lack of clarity in relation to what is a secure liquid low-risk asset under Article 10(1)(a) of PSD2" and "Clarity on this point is further needed since many PIs and EMIs seem to be exploring options to safeguard funds in such secure liquid low-risk assets because of the current negative interest environment having an impact on the cost of holding funds on accounts."

Article 9(5) of the proposed text of PSD3, retains the reference to UCITS investing "solely" in the relevant securities, and it would be helpful if this was amended to recognise the liquidity requirement, and allow for such products to be adopted in practice.

We suggest the following addition to the second paragraph of Article 9(5) as a possible solution: *"...specified in the first paragraph, without prejudice to assets held for liquidity or risk-management purposes."* It may also be helpful to state definitively in the text that certain types of MMFs should be automatically accepted as secure, low-risk assets by competent authorities.

In this way, for UCITs which are required to hold other assets for liquidity and risk-management purposes, the use of broader language could clarify the position and put beyond doubt the possibility that firms authorised to provide payment services under PSD3 can in fact safeguard users' funds through investments in UCITS which are simply secure, low-risk and liquid.

In our view, without such a clarification, it is likely that national law transposition of PSD3 risks continuing to exclude UCITS funds (and MMFs in particular) as part of their safeguarding processes.

Recommendation: clarify that UCITS can comprise assets held for liquidity management, without compromising their status as secure low risk assets for the purposes of safeguarding. This is also applicable to MMFs.

3. Scope: Electronic money services

Article reference: PSD3 Article 2(37), PSD3 Annex II; PSR Article 3(52), PSR Annex II (Definition of electronic money services)

EMA comment: The scope of the e-money regulated activities under the existing regime covers the *issuance of electronic money.* However, the proposed definition of the "electronic money services" in the PSR broadens their scope to include:

(i) the issuance of electronic money,

(ii) the *maintenance of payment accounts storing electronic money units, and*

(iii) transfer of electronic money units.

The rationale for adding these specific activities to the scope of regulated e-money services remains unclear and creates uncertainty in the regulatory perimeter of the e-money service permissions. The operations linked to payment accounts and the transfers of funds are already covered under the regulated payment services (Annex I of PSD3 / PSR), where e-money is just another type of payment product (alongside, for example, commercial bank money and future central bank issued digital currency) which can be transferred or held in a payment account within the scope of payment services activities.

The singling out of activities concerning maintenance of payment accounts storing e-money, or the transfer of e-money, as a regulated activity creates dual regulation for the same activity. Transfer of e-money would for example be a regulated activity under e-money permission, and again under Annex 1 payment services. Storage on the other hand is part of the definition of e-money and is part of the activity of an issuer. Where DLT structures are employed and storage can be undertaken by third party custodians, this will fall under the scope of MiCA, and be regulated under that framework. It would not be appropriate to make custody of EMTs for example subject to authorisation for e-money services. Issuance and holding of safeguarded funds etc. however continues to merit such authorisation.

The sale of e-money by distributors, such as supermarkets, could for example be regarded as a regulated service, when in fact it is merely a commercial activity having no regulated component.

Recommendation: The definition of e-money services should continue to relate to the issuance or creation of the e-money product, while its storage or transfer can be regulated under payment services provisions that govern all payment products - as set out at Annex I payment services.

Own funds/ongoing capital requirement

Article reference: PSD3 Articles 7, 8

EMA Comment: Currently, the own funds requirement for EMIs is calculated in accordance with Method D in relation to the issuance of e-money. Additional capital requirements (calculated in accordance with one of the Methods A, B or C) only apply with respect to

payment services provided by EMIs that are not linked to the issuance of e-money (Article 5(2) EMD2).

Under the new Article 8 of PSD3, the Method D own funds calculation appears to be reserved for PIs only offering e-money services (Art 8(2)); for PIs that offer both e-money and payment services, the own funds for their payment services activity is to be calculated in accordance with the rules that apply to payment services (Art 8(1)). Art 8(5) - which still refers to payment services not linked to the e-money services - is not sufficiently clear on the own funds calculation for the payment services that are linked to the e-money services. Hence a regulatory interpretation could emerge that where a PI engages in an activity that is both an e-money service (e.g. a transfer of e-money) and at the same time involves a payment service under Annex I, the own funds are to be accumulated under separate calculations for the same activity. The use of e-money, by definition, involves making payment transactions; hence would result in much higher own funds requirements for PIs that provide e-money services. This was probably not intended.

The concept of payment services linked to the issuance of e-money for the purposes of own funds calculation was clarified in the ECJ Paysera decision (C-389/17). A clarification in PSD3 text reflecting this decision may be helpful.

Recommendation: we propose revising Article 8(1) to clarify that the additional own funds requirement under Article 7 only applies to payment services activities that are not linked to the electronic money services.

Authorisation: Payment services

Article reference: PSD3 Article 13(1)

EMA comment: PIs are to be authorised "for the payment services and electronic money services that they intend to provide" (Article 13(1) PSD3). With the EMD2 and PSD2 merger, this creates an uncertainty on what, if any payment services permissions e-money issuing PIs would need in order to provide their services.

Currently, in addition to issuing e-money, EMIs are entitled to carry out the payment services listed in PSD2 (Article 6(1)(a) EMD2). No additional authorisation is required for payment services, subject to additional capital requirements that apply to payment services that are not related to e-money. This position is practical, since e-money instruments are intended to be used for payment transactions, which would typically involve one or more payment services. However, there is no equivalent provision in PSD3. This may prove problematic,

particularly with the expanded e-money services definition, where transfers of e-money, for example, could be covered under both the Annex II e-money and Annex I payment services. It creates uncertainty on whether EMIs, including on PSD3 reauthorisation, should require e-money services permissions only, or will they also need specific payment service permission for activities linked to e-money. This could disrupt and/or impose restrictions on the EMI's existing services, even where the underlying activity covered by the EMI's authorisation hasn't changed.

Recommendation: It should be clarified that PIs that provide e-money services are also entitled to provide payment services that are linked to the e-money services.

Ancillary credit services/activities

Article reference: PSD3 10(4)

EMA comment: PSD2 Article 18(4) provided for a possibility for PIs to grant credit relating to both payment services (4) and (5) of PSD2 (i.e. execution of payment transactions covered by a credit line and issuing/acquiring services). The equivalent PSD3 Article 10(4) now appears to restrict the granting of credit in relation to payment service (2) of Annex I only - the execution of payment transactions. This is at odds with other provisions in PSD3 (ref. Article 10(4)(b) and Recital (23)) which reference the granting of credit by way of a credit line and credit cards. The change from PSD2 position was probably not intended. PIs currently grant credit not only in relation to execution of payment transactions, but also issuing and acquiring services, in line with PSD2 conditions. Any change would disrupt their business models, which we submit is unwarranted.

Recommendation: the conditions allowing for PIs to grant credit should remain the same as in PSD2, including credit relating to payment services (2), (3) and (4) in PSD3.

1. Agents, distributors, passporting and competent authorities

Definition: Agents

Article reference: PSD3 Article 2(28) , PSR Article 3(44)

EMA comment: The PSR definition (Article 3(44)) refers to agents as persons acting on behalf of PIs to provide payment services, but *"with the exclusion of electronic money services". T*his approach was taken in PSD2 when e-money services were restricted to issuance of e-money. The new extended definition of e-money services makes transfer and storage by agents also impossible. This is probably not intended.

Recommendation:

(i) If our comments at section 3 above in relation to restricting the definition of e-money to issuance only are accepted, then Article 3(44) can stand as it is.

(ii) If however the expanded definition of e-money is adopted, then Article 3(44) needs to be amended to remove the exception for e-money services. There is no reason why an agent (on behalf of its appointing principal) should be precluded from transferring electronic money units, unlike any other type of funds. The PSD3 definition does not contain this restriction and should be used instead.

Definition: Distributors

Article reference: PSD3 Article 2(36), Article 20

EMA Comment: In line with the position established under EMD2, a distributor can *distribute* or *redeem* e-money on behalf of a payment institution (see PSD3 Article 2(36) and Article 20(1)). Currently, the scope of the permitted distribution activity (distribution and redemption of e-money) does not extend to the provision of payment services (which can be provided by agents instead), nor to issuance of electronic money (which can only be undertaken by EMIs). Whilst the definition of the distribution activity has not changed, the PSD3 and PSR text makes references to distributors engaging in payment services and/or electronic money services, for example:

Recital (45) PSD3: *"To expand the reach of their services, payment institutions may need to use entities providing payment services on their behalf, including agents or, in the case of electronic money services, distributors."*

Article 20(2) PSD3: "... payment institutions that intend to provide electronic money services through a distributor…"

Article 31(2) PSD3: *"...as far as the agents, distributors or branches provide payment services or electronic money services."*

The scope of the permitted distribution activities therefore remains unclear, i.e. is it:

- distribution and/or redemption of e-money; or
- includes provision of payment services on behalf of a PI; and/or
- includes provision of the e-money services on behalf of a PI?

To the extent it is the distribution or redemption only, clarification is needed to ensure that these do not clash with the scope of the payment services and/or the e-money services, hence requiring a licence.

Recommendation: the scope of distribution should continue to be 'the sale or redemption of e-money'. These do not amount to payment services, and therefore this can be clarified in corresponding text. Where payment services are desired, then a PSD agent relationship can be put in place.

Use of agents & distributors & passporting

Article reference: PSD3 Articles 19, 20 and 21

EMA comment:

(i) These articles explicitly recognise commercial practices that were previously inferred under PSD2 and PSD1, where a PI can provide payment services in a second Member State by engaging an agent, or by establishing a branch, located in a third Member State.

(ii) Article 20 however, applies registration obligations that are intended for agents that undertake payment services, when distributors that sell and redeem e-money do not perform payment or other regulated services. It is disproportionate to apply Article 19, albeit mutatis mutandis, to the activity of distribution, as this comprises the sale or purchase of e-money value, and not the performance of payment services. The extension of the definition of e-money services to transfer and storage is strongly opposed again, given that it could have the effect of regulating distributors as PIs. Any distributor registration requirement (which could include, for example, registration of individual shops that sell e-money products) would result in a disproportionate administrative burden in processing and managing registrations for both the NCAs and the PIs alike, without any clear benefit to be achieved from a supervisory perspective.

Where distribution is undertaken for EMT's, the activity will be regulated under MiCA (as CASPs) and will be addressed under that regime.

(iii) Separately, a replacement of the RTS on passporting (Regulation (EU) 2017/2055) should be provided prior to the implementation of the PSD3 in order to provide clarity on the use of agents and distributors.

Recommendation: The EMA perceives that the new distributor registration requirement introduces an unnecessary and disproportionate burden, without any clear benefit to be achieved, and fails to acknowledge that e-money distribution does not involve payment or other regulated activities. The EMA proposes that the registration requirement is removed.

Replacement RTS on Passporting should be published before PSD3 implementation, to provide clarity on the use of agents and distributors.

Competent authorities and investigative powers

Article reference: PSR Article 91, 93

EMA comment: Article 91(3) grants competent authorities broad investigative powers, in respect of not only PSPs, but also including technical service providers, outsourced service providers, agents and distributors.

The jurisdiction of the competent authorities and the manner in which investigatory powers would be exercised in respect of each of the outsourced entities would benefit from further clarification. For example, Article 93(1) PSR sets out the general principle for supervisory oversight; that in the event of suspected infringements of Titles II and III PSR, the competent authorities are those of the home Member State of the PSP, except in the case of agents and branches falling under the right of establishment, where the competent authority is the one of the host Member State.

However, Article 91(3) refers to investigatory powers over various entities (including PSPs, their agents, or distributors) that are "*established or located in the Member State of the competent authority or providing services therein*". This means that a single PSP that engages agents or distributors, could be subject to investigations by at least 3 NCAs (where it is established, located and where the service is provided). We note that from a practical perspective preparing for and responding to supervisory requests and visits takes up valuable resources. Furthermore, responding to several competent authorities over the same service or issue will result in duplication of effort and of regulatory compliance costs.

This issue is likely to be particularly acute for agents, distributors, technical service providers or other outsourced service providers whose services are used to support multiple PSPs in various jurisdictions.

Separately, harmonisation would be helpful with expectations under other initiatives or legislative provisions such as the Central Electronic System of Payment Information (CESOP) and host Member State reporting expectations for fraud and other data, that are made to passporting firms (under both establishment or services provisions). It would be helpful to set out a regime for data sharing between home and host Member State NCAs rather than seeking direct information from firms in an unharmonised manner; clarifying at the same time the scope of such reporting obligations for services and establishment passporting.

Recommendation: The scope of competent authority jurisdiction and investigative powers should be the same as that for supervisory competence. It should be that of the home Member State or where there is an establishment, then also the host Member State of that establishment.

Secondly, clarification of the scope of reporting obligations to host Member States and finding a means for data sharing between NCAs to harmonise supervision and minimise bilateral obligations.

2. Negative scope: Exclusions (Commercial Agency, Limited Network, Technical Service Provider)

Commercial agency exclusion

Article reference: PSR Recital (11), Article 2(2)(b))

EMA comment: The commercial agency exclusion now refers to the definition of a commercial agent, as set out in Article 1(2) of Directive 86/653/EEC ("Self-Employed Commercial Agent Directive", or "Agent Directive"), presumably with the implication that in order to be considered a commercial agent under PSD3/PSR, the commercial agent must also meet the definition in the Agent Directive. This approach raises significant negative consequences:

- Agent Directive is a minimum harmonisation directive. It is limited in scope to agents active in the sale or purchase of **goods**, whereby only some Member States have extended its application to agents active in the sale or purchase of services. Depending on the Member State, PSD2-exempt commercial agents that are authorised to negotiate /conclude the sale or purchase of **services** could hence automatically cease to be able to benefit from the PSD2 commercial agency exclusion.
- The Agent Directive definition carries a body of existing case law and legal consequences that is influenced by its purpose - the protection of commercial agents vis-à-vis their principals - including rules on indemnity or compensation due to agents in case of contract termination. Such protection and rules are not appropriate or necessary in the context of businesses that seek to benefit from the PSD2 exclusion.

The PSD commercial agent definition also adds a requirement that the agreement between the principal and the commercial agent should give the payer or the payee "*a real margin to negotiate with the commercial agent or conclude the sale or purchase of goods and services*". It is unclear what a real margin to negotiate, and even less so, what a real margin to conclude the sale, might include. The requirement for a "real margin" may be difficult to reconcile with the online sales environment, and is subject to further divergent interpretations across Member States as to its meaning.

Recommendation: The EMA considers the PSD commercial agent exclusion to offer significant value, and its scope should not be unduly restricted. The exclusion allows for bill payments and similar payment arrangements to be offered, where the merchant can manage the risk in a similar way to other commercial risks. It can be particularly useful for merchants entering new markets where commercial agents already have the infrastructure to help merchants to offer their services/products.

Limited Network Exclusion (LNE)

Article reference: PSR Recitals (12), (13), Article 2 (2)(j)); PSD3 Article 39

EMA comment: The EMA welcomes the fact that the LNE has been maintained.

However, we would also like to see the following ongoing concerns being addressed:

- Divergences between Member State national competent authority ("NCA") approaches towards notification: some NCAs have introduced notification processes that are comparable to an authorisation application; this increases compliance costs and undermines the benefit and intended objective of the exemption;
- Diverging interpretations between Member State NCAs on the scope of services that qualify for LNE, together with notification requirements in each MS for where the service is provided means LNE providers have to go through multiple LNE notification processes, with uncertain and sometimes conflicting outcomes depending on the Member State. The EBA Guidelines on the LNE have provided some clarity and harmonisation and further harmonisation is expected from the new EBA RTS on LNE conditions. A helpful extension to this 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.

LNE duty of notification (PSD3 Article 39) remains substantially the same, and subject to the same issues:

- 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. A simplified notification procedure should be made available at the outset, enabling clarity and regulatory certainty for business.
- No timeline for LNE notification assessment: following an LNE notification, the NCA should be required to respond with any objections it may have within 2 months of notification, and if an NCA does not respond within this period, it should be deemed to have agreed with the service provider's application of the LNE.
- 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. (We note that although EBA Guidelines provide for this, some Member States continue to require periodic re-notifications).

The restricted use and utility of LNE instruments acts to limit the risk to users. Reference to payment volumes or the number of customers (Recital (12)) is overly restrictive and does not recognise the original purpose of such exemptions, ensuring that payments regulation did not extend to products and services that could be significant in size, but which did not give rise to payment related risks. We propose that reference to volume- or customer-based criteria for LNE should be avoided.

PSD3 Article 39 referencing appears to involve drafting errors, which should be rectified:

- Article 39(1) PSD3 reference to the LNE should be to Article 2(2)(j) PSR (not 2(1)).
- Article 39(2) PSD3 (requirement for an annual audit opinion) should reference the Electronic Communications Exclusion (ECE) (as it did in PSD2 equivalent), not LNE; hence the reference should be to Article 2(2)(k) (not 2(2)(j)).

  The EMA opposes the introduction of an annual audit opinion for LNE (if this is the intention) - the need for it has not been explained and we believe is not justified.

Recommendation: Harmonisation of notification obligations would be helpful, coupled with a passporting provision enabling service providers to offer services in multiple Member States without having to undertake the notification process multiple times, especially if it is harmonised.

Furthermore, we propose removal of transaction volume and user numbers as criteria for the application of LNE provisions.

Technical Service Provider (TSP) exclusion

Article reference: PSD3 Article 2(24); PSR Article 3(36), 58, 87 and 91(3)

EMA comment: EMA welcomes the fact TSP services remain largely out of scope of the regulatory perimeter, noting however the new obligations placed as regards TSP service providers.

(i) The TSP definitions in PSD3 and PSR are subject to subtle differences. For clarity and consistency, the definitions could be aligned. The EMA supports the PSD3 definition (Article 2(24)), encompassing technical services that are *necessary to support* the provision of payment services.

(ii) From the perspective of a number of our members, the provisions of Article 58 PSR are considered excessive and disproportionate. Given that TSPs will be contractually obliged to deliver requisite services to regulated entities, it is not necessary to introduce provisions that describe the nature and scope of liability that will flow from this contract. Similarly it would not be appropriate to provide for liability that is outside of the scope of a contract. The regulatory

regime makes provisions, obligations and levies liabilities on PSPs as the regulated entities, and this should be sufficient.

Further clarity as to when an outsourcing agreement will be required is desirable to ensure a consistent approach, given the audit and security provisions may well be resisted by some TSPs.

Similarly, clarity on the scope and extent of activities that give rise to: 'providing and verifying the elements of SCA' would be helpful. This could also ensure a consistent approach is taken across all Member States.

(iii) It is our view that it is disproportionate to introduce powers enabling the competent authority to investigate a TSP directly (Article 91(3)(b)) including the examination of records and the interviewing of personnel. A right of audit can be provided under contract, as a means of providing certainty and accountability. Given that TSPs are not subject to regulatory oversight, such a power could be excessive.

Recommendations: Alignment of the definitions of TSPs in the Regulation and the Directive would be helpful. Provisions for liability of TSP that are not subject to regulation themselves are not needed, and similarly direct investigatory powers for NCAs in relation to such TSPs is excessive.

6. Access to Payment Accounts:

Article reference: PSR Article 32

EMA comment: The significant impact of de-risking is also reflected in the difficulties PSPs experience when trying to obtain bank accounts in the first place; the issue has grown more acute over recent years. This is exacerbated by the draft PSD3 Article 9(2), which requires PIs to "*endeavour not to safeguard all consumer funds with one credit institution*". The EMA therefore welcomes the EC's initiative to address the issue of de-risking in the draft PSRs by broadening the scope of entities that can benefit from the provisions in this Article, and by providing specific reasons for the refusal to open/for closing a bank account.

(i) We suggest at the outset that access to bank accounts by regulated PSPs, and in fact access to a choice of bank accounts must become a right of every PSP upon authorisation. This must be the case if PSPs are to be expected to play their role in the payment system and to act as an effective competitor to existing banks. It is no longer acceptable to tolerate a situation where PSPs can get authorised and find they cannot participate in the payment system because banks' risk appetites differ from their own, or because banks refuse to offer

services to this sector. The only reasonable solution is to make access to bank accounts a RIGHT of every authorised PSP, and in the event of failure to find a bank account, for the NCA to nominate one or more banks to offer such a service. This is not unlike the arrangements in France and we strongly propose this approach be adopted across the EU.

We will nevertheless also consider the proposed language as part of our response:

(ii) Some of the reasons offered for valid de-risking are very broad, in particular: insufficient information, an excessive risk profile and disproportionately high compliance costs. These terms are vague, and give banks broad scope for justifying a derisking decision. They appear unlikely to deter banks from de-risking a PSP or an applicant e.g. [PSR 32(1)(c)-(e)].

(iii) De-risking will no longer be notified to the national competent authority ("NCA") but to the PSP who may then appeal to the NCA : this will unfortunately reduce transparency, as there is no longer a central point for the collection of data. Given the limited list of reasons for which banks can derisk a PSP, NCAs should be in a position to gather and publish statistical data. We therefore propose that notification should be addressed to both the PSP ***and*** to the NCA, alongside an obligation on the NCA (and potentially the bank) to publish aggregate data. This role in addressing derisking, a potentially anti-competitive exercise, should be more formally defined, with NCAs having clear objectives and timeline in this regard.

(iv) Art. 32(3) states that a *credit institution shall notify… any decision … and duly motivate any such decision*: We suggest a minimum notice period of at least six months for banks wishing to de-risk PSPs, in order to allow PSPs to find alternative banking providers.

Recommendation: access to bank accounts should become a RIGHT enforced by NCAs if Payment Institutions are to be able to play a role in the payments infrastructure, and if competition between PSPs is to be achieved.

The role of NCAs should be formally defined with clear competition related obligations to ensure unhindered access to bank accounts.

7. Access to Payment Systems:

Article reference: PSR Article 31; PSD3 Articles 46, 49

EMA comment: The EMA strongly supports open, non-discriminatory access to multilateral payment systems, by all market participants, and welcomes amendments to the Settlement Finality Directive (SFD) to include PIs as eligible participants. Non-bank PSP participation in

SFD-designated systems will depend on implementation of non-discriminatory and transparent payment system access rules by system operators (PSR Article 31), as soon as possible. The payment system access provisions in Article 31 should therefore also be subject to a shorter transposition and application timeframe, aligning with the transposition timeframe of the Settlement Finality Directive amendments (PSD3 Articles 46 and 49), i.e. no more than 6 months.

Recommendation: amendment of the SFD to include non credit institution PSPs is strongly supported. Payment system access rule changes should be implemented as soon as possible, to enable participation by non-bank PSPs.

8. Fraud & IBAN Verification service and Data sharing

IBAN Verification:

Article reference: PSR Article 50 and 57

EMA comment: The EMA strongly supports an alignment of the matching service envisaged under the Instant Payments Regulation and that under the Payment Services Regulation, and in particular that the PSD2 definition of “unique identifier” is used rather than a reference to IBANs. A common EMI and PI operating model uses one IBAN (often the IBAN of the PSP) to route funds to multiple customer accounts. When received by the PSP, the funds are allocated to the correct customer/account using “secondary reference data” that has been sent in the payment instruction. This means that any text that limits the use of the matching service to IBAN only will automatically exclude this type of PSP from participating and meeting their obligations under the PSR. Instead, reference to “unique identifiers” as defined by PSD2 (as opposed to prescribing the exclusive use of IBANs as identifiers) will facilitate consistency, including in terms of the necessary IT developments needed to implement the matching service, as well as ease consumer understanding.

Recommendation: ensure legislation refers to a “unique identifier” rather than restricting the reference to an IBAN, and ensure a broad definition of such identifier.

Data sharing:

Article reference: PSR Article 83

EMA comment: The EMA supports the possibility for PSPs to share unique identifiers in order to combat fraud. This is one of the most effective tools to prevent fraudsters from taking advantage of the industry and or payment service users.

We note that data sharing is limited to sharing of unique identifiers, which appears rather limiting. There are many different types of fraud which may not be detectable solely through unique identifier sharing. In order to enable improved fraud prevention, we believe there are merits to extending the scope to allow for data sharing beyond unique identifiers.

The text states that unique identifiers can be shared only when "*at least two different payment services users who are customers of the same payment service provider have informed that a unique identifier of a payee was used to make a fraudulent credit transfe*r". This definition appears to be very restrictive, and not risk-based. It may also disproportionately impact smaller PSPs, as they have fewer users and therefore are less likely to reach the 'two users' thresholds and thus be able to share a unique identifier with other PSPs. This definition also reduces the ability of firms to prevent certain scam typologies, where there are fewer victims but for very high amounts of money (e.g. some investment scams). We believe the Level 1 text should not define "sufficient evidence"; it should be defined on a case-by-case by the PSP, based on the evolving fraud typologies observed.

Recital 104 restricts the definition of a unique identifier: under this article, a unique identifier is limited to an 'IBAN' as defined in Article 2 point 15 of Regulation (EU) 260/2012. This definition directly contradicts the definition of a unique identifier in Article 3(39) of the PSR. This restriction would result in a large number of PSPs being unable to share data to combat fraud. These PSPs do not attach unique IBANs to each PSU accounts, but instead have one IBAN for several (sometimes hundreds) of accounts, and use other unique identifiers for the individual PSU account.

This would also lead to confusion and inefficiency as some IBANs that are not attached to PSU individual accounts could be reported. If there is no possibility to share a unique identifier (in addition to the IBAN), these PSPs would be unable to share data on the fraudulent payment account.

Therefore, the EMA supports a consistent approach to the definition of 'unique identifier' in the PSR, and suggests the removal of recital 104. This would maintain the current definition of unique identifier, avoid excluding a growing section of the payments industry, and allow all PSPs to more efficiently make use of use data-sharing to prevent and mitigate fraud.

The text also appears to extend the data sharing ability to PSPs only. This data sharing possibility should be extended to other actors that participate in the combat against fraud, including but not limited to public entities, social media platforms and ECSPs, as well as industry consortia, non-profit organisations and security solution providers, for example, in order to include groups which are already collaborating in this space. As long as an entity can demonstrate a legitimate interest in accessing and sharing such information in order to combat fraud, they should be able to benefit from this article.

Recommendation:

The EMA proposes to remove the definition of 'sufficient evidence' in article 83(3) as this would limit the efficiency of data sharing for certain typologies of fraud as well as for smaller PSPs. The EMA also supports an extension of the scope of entity that can share data to combat fraud to include other actors in addition to PSPs. Finally the EMA supports the deletion of recital 104 to allow all PSPs to benefit from data sharing in order to fight fraud. The scope of the data to be shared also merits revision, to enable sharing beyond unique identifier data, in order to improve fraud prevention.

9. Fraud & liability of PSPs in case of impersonation scams

Article reference: PSR Article 59

EMA comment: The requirement for mandatory reimbursement for fraud cases involving spoofing of the PSP will have a significant economic impact on PSPs. At the same time, the mitigating measures for this type of fraud are frequently outside the control of the PSP. It will more commonly lie with electronic communications services providers, social media hosts, and other communication service providers. It may be difficult in particular for smaller PSPs to detect all such instances of spoofing, and may then be equally difficult to have rogue web sites or communication channels closed or removed.

It remains unclear why PSPs should be liable for this type of impersonation scam, as the fact that the fraudster is impersonating employees of the PSP does not provide the PSP with specific clues or indicators that would allow it to mitigate or prevent this type of fraud during the payment process. For other forms of spoofing, for example fraudsters impersonating the police or a delivery company, there would never be an expectation that the spoofed party should be liable for the losses incurred by the customer. The same logic should apply here; the PSP has no power to control or prevent a fraudster from impersonating its employees.

Therefore, making best efforts to detect and mitigate such risks should provide a defence against reimbursement obligations. Furthermore, a means of including the broader network ecosystem in the obligations to address this risk, as well as creating legal tools to deter criminals would be more effective in reducing the volume of fraud incidents in the EU.

Recommendation: PSPs should be liable for impersonation scams, only if and when (1) the PSP had controls over the specific impersonation scam that took place and (2) except in cases where PSP has made reasonable efforts to detect and mitigate the risk. The liability should only lie with the PSP if it has failed to meet reasonable expectations for the detection

of such incidents and/or where it has not made best efforts to address/mitigate the specific risks that have been detected.

Instead, a cross-industry approach should be taken, whereby liability should be borne by specific telecommunication providers, internet platforms and media providers who can also be expected to make reasonable efforts to mitigate such risks, and where they fail to do so.

Such intermediaries could usefully also be obliged to cooperate with PSPs for the prevention, deterrence and mitigation of such scams and frauds. This is more likely to give rise to an effective approach to combating financial crime.

We also propose that the payer should bear all the losses if the payer acts fraudulently, with gross negligence or if the payer failed to fulfil some of their obligations, which would then constitute gross negligence or intent.

PSPs' liability for unauthorised transactions and suspicions of fraud

Article reference: PSR Article 56,60

EMA comment: Article 56 provides the PSP with a period of 10 business days from the time of notification by a user of an unauthorised transaction, to investigate any suspicions of first party fraud, and therefore whether or not to reimburse.

It is the EMA's view that this period should start from the day the payment service user has provided all the necessary information for the case to be reviewed, rather than from notification. Otherwise it is likely that the 10 days could elapse simply from delays on the side of the consumer. Additionally, it is in the interest of combating financial crime for firms to investigate cases of unauthorised transactions, in order to avoid reimbursing fraudsters, and therefore encouraging the perpetuation of the fraud. We would suggest that unless it is obvious from the facts that the user is at no fault, some investigations should always be undertaken as a norm. *Immediate* reimbursement should be an obligation only once investigation has been undertaken. This would provide firms with the ability to pursue and address fraud that impacts legitimate customers.

Ten days is a short time period within which firms must conduct their investigation; we suggest this period is extendable where there is evidence of fraud and further time is required. 20 business days may be appropriate for more complex investigations.

Separately, corporate payments exhibit a different set of characteristics to consumer payments and merit a different approach to fraud risk management.

Recommendation:

We suggest allowing investigation of fraud as a rule, and for an extended period of investigations where this is required. Immediate reimbursement can then take place. The obligations are also less appropriate in the corporate payment context.

10. Administrative sanctions

Article reference: PSR Article 97

EMA comment: Article 97 introduces new administrative sanctions that competent authorities can impose regarding breaches *or circumvention* of:

- the rules on access to accounts maintained with a CI laid down in Article 32
- the secure data access rules by either [ASPSP] or by [AISPs and PISPs] laid down in Title III, Chapter 3 ...
- ... strong customer authentication as set out in Articles 85 [SCA], 86 [SCA for PIS and AIS] and 87 [Outsourcing agreements with TSPs for application of SCA]
- ... transparency on fees by ATM operators or other cash distributors, in accordance with Article 20(c) point (ii)
- failure of PSPs to respect the period for compensation of PSUs as set out in Article 56(2) [unauthorised transactions], Article 57(2) [authorised credit transfers - incorrect application of matching service] and Article 59(2) [liability for impersonation fraud].

The most notable of sanctions is that a competent authority can impose on a legal person (e.g. a company) a fine of up to 10% of the legal person's annual turnover or where such a legal person is part of a corporate group 10% of the group's annual turnover. We note that Article 96(1) requires "*administrative sanctions and administrative measures shall be effective, proportionate and dissuasive*". It is not clear how this would apply when comparing the case of two payment institutions with equal turnover that commit a breach subject to the power in Article 97 but where one payment institution is not a member of a corporate group ("**PI A**") while the other is a member of a corporate group with a very large turnover ("**PI B**"). Potentially, PI B would be subject to a much larger fine than PI A for committing the same breach under Article 97 just because it is part of a large corporate group.

This does not appear to be proportionate. A proportionate approach would be that the turnover of the corporate group would only be considered when determining a fine where other members of the corporate group contributed or facilitated the breach.

There is an ambiguity in the current text on whether the prescribed amounts of fines are intended as the maximum measure of fines that could be imposed, or whether it leaves it open to the NCAs to impose higher fines. The ambiguity stems from conflicting references in Art 97 to 'maximum' fines that are 'at least' of a specified size (Article 97(2)). Any provisions allowing the NCAs to impose yet higher fines would be disproportionate and undermine the harmonisation objective sof the Regulation. Other EU legislation (e.g. the GDPR, the Digital Markets Act, the Digital Services Act) provide for the maximum amount of fines which can be imposed, and the PSR text should be amended to follow a similar wording.

It is proposed in Art 97(1) that sanctions could apply not only for breaches of PSR requirements, but also for their circumvention. Legal certainty demands that sanctions can only apply to breaches of clearly defined legal obligations or prohibitions. What is a legitimate business strategy for some might be interpreted as a circumvention to others. It should not be possible to impose fines for something as vague, uncertain and subject to subjective interpretation as acts described as circumvention. The reference to 'circumvention' in Art 97(1) should be deleted.

Recommendation: we propose amending the group sanction to only apply where the group entities are at fault. A more precise drafting is needed to clarify the prescribed amounts of fines apply as a maximum measure, in line with other EU legislation, and that sanctions can apply to specified breaches, and not to acts described as 'circumvention'.

11. Open Banking

Definitions

(i) Payment Account

Article reference: PSD3 Article 2(13); PSR, Article 3(15)–

EMA comment: the definition has been amended to encompass the interpretation of the European Court of Justice in the case of ING-DiBa Direktbank (Case C-191/17) as well as the EBA's response to PSD2 questions (EBA Q&A 4272 and 4856), which indicate that only an account that can both send and receive funds to / from third parties is a 'payment account'.

In the context of TPP access to payment accounts, the EMA welcomes the clarifications in the updated definition of payment account as it will better support a uniform approach for identifying those accounts which should be reachable by authorised third parties through an access interface across Member States. However, we note that the new definition may

exclude some ‘savings accounts’ which some jurisdictions may have previously granted access to under PSD2.

(ii) **Account Information Service (AIS)**

Article reference: PSD3 Article 2(18); PSR Article 3(21)

EMA comment:, the definition has been updated to better reflect the market for AIS which has developed.

We note that Recital 26 clarified that “..*the information aggregated by the authorised account information service provider may be transmitted to a third party to enable that third party to provide another service to the end-user*”, but the proposed AIS definition does not contemplate onward sharing of data to third parties as being within the scope of AIS. We suggest the definition should include this point to ensure a clear regulatory perimeter for AIS.

Furthermore, there continues to be a reference to consolidation of information as a characteristic. This reflects initial use cases for AIS services, but many new use cases do not involve aggregation or consolidation but simply access and analysis of data and provision of added value.

Recommendation: the definition of AIS should make consolidation an optional characteristic and it should also refer to use of the data by a third party service provider.

Professional Indemnity Insurance (PII):

Article reference: PSD3 Recital (23); PSD3 Article 36

EMA comment: the Commission states (in Recital (23)) the intention to allow both PISPs and AISPs the flexibility to delay the holding of PII until after authorisation or registration.

Art 36(5) PSD3 provides for this delay in obtaining PII for AISPs but we note that the possibility for PISPs to delay obtaining PII under PSD3 does not seem to have been included in the proposed text. We recommend that PISPs are afforded the same flexibility on PII that was intended under Recital (23) to ensure a level playing field.

We also suggest that the final text should clarify the ambiguities in Art 36 as to whether an AISP must obtain PII when they have opted for initial capital alternative (..*which can be replaced*..) and by when (.. *without undue delay.*.) to ensure a consistent application by Member States.

Recommendation: PISPs should be extended the same allowance for the timing of obtaining PII as AISPs. Additionally, clarity as to whether initial capital serves as an alternative to PII for AISPs.

Data Parity (PIS):

Article reference: PSR Article 37(3)

EMA comment: recognising the issues that PISPs have encountered with access to payment account data to provide their services the proposed regulation seeks to ensure that transaction data provided to PISPs is on par with the data customers receive directly via their ASPSP.

Art 37(3) obliges the ASPSP to provide real-time information until the transaction is 'final'. The EMA welcomes the inclusion of the requirement to provide PISPs with information on the initiation and execution of the payment transaction on an ongoing basis. However, we note the definition of 'final' is not clear – it could mean when the transaction is settled with the receiving PSP, or when the execution of the payment is confirmed by the sending ASPSPs. The EMA would welcome further clarity in this provision so that the impact can be properly assessed.

Furthermore, we consider that without a common approach to describing payment status and error messages (or reasons for rejection or failure of a payment) there will be added complexity and fragmentation between ASPSPs and Member States. Thus hampering PSPs ability to investigate and resolve issues in a consistent and efficient manner. As a result some level of standardisation should be considered.

Recommendation: clarity on the definition of finality would be helpful. We also suggest some standardisation around the reasons for transaction failure in EBA RTS or Guidelines, as discussed under our comments on Art 35.

Dedicated interfaces

Article reference: PSR Article 35

EMA Comment: except in exceptional circumstances, ASPSPs will be required to provide a dedicated interface for open banking access to payment accounts. The Commission has not proposed that dedicated interfaces are fully harmonised to a single API standard.

The EMA are encouraged by the Commission's intention to improve the operation of account access interfaces while minimising the impact on the burgeoning market that has emerged since PSD2's introduction. We support the approach where no single payment account access API standard is mandated; this would cause significant disruption to the market. We note that ASPSPs who have provided TPPs access to their payment accounts using a 'modified customer interface' (MCI) under PSD2 may need to create a dedicated interface under these proposals.

The EMA also welcomes the requirement (Art 35 (7)) to provide clear API messages to TPPs to explain the reasons for unexpected events or errors. PISPs experience numerous instances where transactions are rejected or fail without sufficient information as to the reason. This is not only essential for PISPs to be able to deliver good experiences for their customers, but also to enable PISPs to diagnose issues and improve levels of payment success. Furthermore, this can create a credit risk for the payee's payment service provider (PSP). We note that unless a common standardised framework for communicating the reason for transaction error or failure is developed the provision of error messages alone may not enable PSPs to investigate and resolve any issues in a consistent manner.

Recommendation: mandating a single API standard will cause disruption and is not regarded as necessary, the Commission position is supported. However we acknowledge that some level of standardisation is needed to improve the functioning of the Open Banking market, and recommend that the EBA RTS or Guidelines developed for dedicated interfaces address the need for:

- consistent use and relaying of error messages for payment or permission rejection or failure; and
- Provision of accurate information to PISPs on the status of a transaction, including confirmation of payment execution.

Exemption from provision of a dedicated interface

Article reference: **PSR** Article 39

EMA comment: recognising the disproportionate burden that providing an interface can place on some ASPSPs, competent authorities will be able to exempt them from providing a dedicated interface, or from having an interface at all.

The EMA welcomes this proposal as some Members have reported little demand for payment account access using their interface developed for PSD2 given their particular service proposition.

We note that the EBA will be responsible for determining the exemption criteria that will apply for this provision. It will also be helpful for the Commission to provide the EBA with a policy steer on the exemption criteria to ensure a more consistent outcome.

Experience from PSD2's fallback interface exemption process has revealed that interpretation and application by NCAs of the exemption criteria can lead to inconsistencies across jurisdictions. The mandate to the EBA for developing the relevant RTS under the PSRs should require them to provide NCAs with a clear tool for consistent decision making. We also see merit in setting out criteria based on, for example, limited use or value of payment account products, which would be automatically exempt under Article 39 (or enabling the EBA to do so in its RTS), without having to seek exemptions individually with NCAs. This may contribute towards a harmonised approach while alleviating the administrative burden.

Recommendation: policy direction to the EBA on the development of clear exemption criteria would be helpful and ensure a more predictable and consistent outcome. ASPSPs that see little or no demand for access to user data should be able to benefit from exemption to the provision of a dedicated interface.

Contingency Measures

Article reference: PSR Article 38

EMA comment: Whilst the PSD2 provision to provide a fallback interface (when the dedicated interface is unavailable) has been removed in the proposed regulation (Art 35 (2)), in some circumstances, ASPSPs will have to provide an alternative access point for when a dedicated interface is unavailable.

The EMA considers that the proposed provisions for an '*alternative solution*' to be used by TPPs are as yet not clearly defined. The proposed process to provide access when an alternative solution is not provided by an ASPSP is somewhat cumbersome and involves undue delay, requiring for example that (i) only if the ASPSP has failed to provide a '*rapid and effective*' alternative access interface can TPPs request that NCA's allow them to temporarily use the customer interface, and then (ii) if the NCA has failed to make a decision '*without undue delay',* only then can they use the customer interface by default.

It would be more helpful to provide specific timelines for alternative interface availability, or for the NCA to make a decision on a request to use the customer interface. The proposals as currently envisaged are likely to introduce complexity for NCA's and the industry.

Recommendation: for contingency measures, further clarity on the definition of when an dedicated interface is 'unavailable', on what constitutes suitable 'alternative solutions', and specific timelines for NCA interventions on the use of customer interfaces should be provided.

Performance and functionality of dedicated interfaces

Article reference: **PSR** Article 36

EMA comment: provisions from the PSD2 RTS on SCA and CSC have been incorporated alongside new requirements for dedicated interfaces in order to improve API functioning, and ultimately improve user experience of Open Banking services. Of note, the proposals clarify the payment types that are in scope of PIS, require that dedicated interface response times must be on par with customer interfaces, and introduce requirements that interfaces must support confirmation of the name of the account holder before initiation of the transaction, and the ability to initiate a payment with only one SCA.

The setting of minimum standards for the availability and performance of account access interfaces should improve the current fragmentation and inconsistency between ASPSPs that has evolved under PSD2, and enable TPPs to provide consistent services to their customers, although its ultimate success will depend on the implementation, regulatory technical standards, and the enforcement activities of NCAs. For instance, Art 36. 1 (c) regarding the response times of the dedicated interface (and requiring parity with direct customer interfaces), will only generate improvements if direct customer interfaces operate to a level which improves current dedicated interface performance. Otherwise, this provision could result in a downgrading of dedicated interface performance.

Art 36(2) PSR requires functionality that will enable both AISP and PISPs to interact with dedicated interfaces, but Art 36 (2)(d) only provides for PISPs to be provided with the unique identifier and account holder's name prior to initiating a payment. We note inconsistent provision of this data to AISPs in some Member States, and suggest this could be remedied by broadening this provision to both AISPs and PISPs.

Recommendation: we support the additional clarity. In particular we support the introduction of Article 36 (4h), which allows the initiation of a payment with only one SCA.

We suggest that Art 36(2) PSR should allow both PISPs and AISPs to retrieve Account Holder Name and account unique identifier.

Permission dashboards

Article reference: PSR Article 43

EMA comment: introduction of a requirement for ASPSPs to offer customers a permission "dashboard" allowing the withdrawal or re-connection of access from any given AIS/PIS provider, and a historic view of permissions granted.

The EMA agrees with the Commission's assessment that a permission dashboard will likely help end-users understand and manage payment account access by AIS and PIS service providers. We also appreciate the proposal in Art 43(3) that ensures that ASPSPs have to consider the positioning and ease of use of the dashboard. Experience in markets where permission dashboards are already in use suggest this is important for customer experience and trust in Open Banking services.

However, the proposed provisions of Article 43 require a real-time exchange of information between ASPSP and TPP on the status of permissions granted by the customer, and must include the ability for the customer to withdraw or re-establish access granted to an AISP or PISP. We also question the practicality of being able to re-establish a connection with a TPP after a permission has been withdrawn in all cases, as this will depend on the contractual relationship between the TPP and the user. These requirements would appear to go beyond the current features of permission dashboards used in the market, and may indicate a significant change to APIs and services for both TPPs and ASPSPs.

Art 43(2)(a) also specifies that the '*purpose*' of permission and '*categories*' of data accessed must be shared on the dashboard. Without some standard classifications of purpose and data clusters being shared it could in fact lead to more confusion for customers as each API standard, or ASPSP, could use their own terms to classify purpose and data clusters shared. The Commission have not indicated that the EBA will be required to specify further details on the dashboard data to ensure consistency across ASPSPs. The EBA should be required to define (in an ITS) a common set of dashboard data terms to ensure consistent implementation and achieve the benefits to users that the Commission anticipate.

In addition, the ability to withdraw permission or reconnect to a TPP within the ASPSPs domain moves away from the PSD2 concept that granting permission to access an account is managed within the TPP's domain. The EMA suggests that this could be resolved by including only permission data provided by the TPPs in the dashboard.

Recommendations: The provision of permission dashboards for customers is supported. We suggest that the EBA should be required to develop a common set of criteria for permission dashboards to ensure a consistent approach is developed and support ease of use by customers in all jurisdictions.

Obstacles

Article reference: PSR Article 44

EMA comment: the draft regulations provide a non-exhaustive list of 'prohibited obstacles' to providing AIS or PIS, with the objective of providing clarity to market participants and competent authorities in identifying prohibited practices.

The EMA welcomes the proposed inclusion in legislation of prohibited obstacles to enabling TPP access to accounts, including incorporating the EBA's previous opinions on obstacles (the EBA's Opinion on Obstacles (4 June 2020). However, we consider that codifying a list of obstacles in the legislation (albeit with the 'non-exhaustive' caveat) may risk that NCAs interpret these as the only obstacles which can occur which could lead to inflexibility and a lack of future-proofing as new obstacles emerge. An outcomes-based approach could be adopted whereby undesirable outcomes are listed, and any obstacles which cause those outcomes would indicate that the ASPSP's dedicated interface did not meet PSR obligations.

Recommendation: we suggest an outcomes approach to obstacles, making specific examples but indicating the outcome was the objective. This may also require a definition of 'obstacles' to be included in PSR Article 3 to clarify the undesired outcomes.

SCA for AIS

Article reference: PSR Article 86(4)

EMA comment: a key change on applying SCA to AIS access to accounts; requiring ASPSPs to conduct SCA only on the first access to an account, and thereafter the AISP must conduct SCA at least 180 days after the last SCA.

While this proposal may enable TPPs to manage AIS services on a continuous unattended basis, the potential costs of implementing the provision of full SCA by AISPs seem disproportionate. The EMA proposes utilising permissions dashboards to provide this functionality. Permissions Dashboards, as provided under Art 43 PSR, give customers a clear indication of the permissions they have granted to TPPs, and obviate the need to use SCA

to (i) assess their awareness of continued access to the data, and (ii) indicate continued consent to such use. The dashboard will provide a means of both (i) indicating service providers with access (Article 43(2)(a)), and (ii) a means of terminating such access (Article 43(2)(b)).

Recommendation: the features required of the ASPSP dashboard under Article 43 PSR achieve the same outcomes as those for an AIS provider under Article 86(4) PSR, and obviate the need for the AIS provider undertaking ongoing SCA.

Role of competent authorities, and monitoring the Open Banking Market

Article reference: PSR Article 48

EMA comment: recognising the need to improve national competent authorities (NCA) understanding of the open banking market, in order to robustly enforce the relevant rules, the proposal places new requirements on NCAs to employ dedicated staff and formally liaise with market participants. This will be underpinned by market data which NCAs will collect from industry participants in order to support better understanding of consumer and business take-up of Open Banking services, and also facilitate improved enforcement action.

The EMA welcomes the aim to improve NCA's understanding and interaction with open banking market participants.

Whilst this Article does introduce reporting requirements for industry participants, the provision of meaningful data on the functioning of the market will improve transparency and should enable issues to be tackled more efficiently. However, we note that the proposal does not include the requirement for NCA's to publish data on the performance of the market in their jurisdiction, which may provide an incentive to improve the resolution of issues that are identified in a timely manner rather than within the two year reporting cycle from the EBA to the Commission.

Recommendation: The EMA supports increased NCA visibility of the open banking eco-system through the collection of data.

RTS on SCA and CSC

Article reference: PSR Article 89

EMA comment: PSR Article 89 includes a mandate on the EBA to consider user-friendliness as a key criteria for the RTS. We consider that user experience and user-friendliness are

fundamental in order to ensure that open banking can be successful, and to stimulate adoption.

Recommendation: The EMA supports the revised EBA mandate to consider user experience when developing regulatory technical standards for the PSR.

12. Conduct of Business provisions

Article reference: PSR Article 61

EMA comment: The conduct of business rules are set out in Title I1 PSR (Transparency of conditions and information requirements for payment services), i.e. Articles 4 to 26 PSR, and Title III PSR (Rights and obligations in relation to the provision and use of payment services), i.e. Articles 27 to 104 PSR.

In Article 61 PSR, it is proposed that where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction and ***the exact future amount is not known at the moment when the payer authorises the execution of the payment transaction***:

- The payer's PSP may only block funds on the payer's payment account if the payer has given their permission to that precise amount of funds to be blocked.
- The amount of the funds blocked by the payer's PSP shall be in proportion with the amount of the payment transaction ***which can reasonably be expected by the payer***.
- The payee shall inform its PSP of the exact amount of the payment transaction immediately after delivery of the service or goods to the payer.
- The payer's PSP shall release the funds blocked on the payer's payment account immediately after receipt of the information about the exact amount of the payment transaction.

We note that the proposed requirement that "the amount of the funds blocked by the payer's PSP shall be in proportion with the amount of the payment transaction which can reasonably be expected by the payer" is an onerous requirement which assumes that the payer's PSP has the institutional knowledge of what is a reasonable amount in the payee's business and the payer's expectations, which, in practice, would not be the case as the payer's PSP may not have any knowledge of the payee's business and the payer's expectations of the value of the goods or service they are about to receive. We suggest that this requirement be removed.

We note that the payer's rights are already secured by the requirements placed on the payer's PSP (i) to obtain secure customer consent for the exact amount to be blocked, and (ii) to release blocked funds without undue delay after receipt of a payment order/confirmation of the final amount.

Possibility for Member States to provide for more favourable refund rights and stricter fraud prevention measures

Article reference: PSR Article 107

EMA comment: Article 107 allows Member States to provide for more favourable refund rights to the payment service user and stricter fraud prevention measures. The EMA understands the objectives here but suggests that a harmonised approach to fraud at EU level, will be more effective operationally and enable the implementation of EU-wide fraud prevention policies and measures by PSPs. This will also reduce the incident of fraudsters targeting specific Member States based on their specific legislation. We therefore recommend the deletion of Article 107.

Recommendation: we propose a single EU wide refund policy, and the removal of Article 107.

Requests for refunds for payment transactions initiated by or through a payee

Article reference: PSR Article 63

EMA comment: The proposed 8-week unconditional refund right extension from SEPA DD to MITs gives rise to some concerns. MITs can have very broad application and an automatic refund right may not be an appropriate means of redress. Such transactions can for example relate to the provision of digital goods or other services that could be consumed, and therefore leave the merchant exposed to fraud at a significant scale.

Recommendation: We suggest refraining from extending the refund right to MITs in general.

EBA intervention powers

Article reference: PSR Article 104

EMA comment: This is a new power similar to the EBA's existing power in Article 9 of the EBA Regulation (Regulation (EU) No 1093/2010), which would apply to e-money and

payment services. The EBA would have the temporary power to directly intervene in the market and restrict or prohibit products where:

- the intervention addresses a significant number of payment service users (including e-money service users) or a threat to the orderly functioning of the payment or e-money markets, and the integrity of those markets or to the stability of the whole or part of these markets in the EU;
- regulatory requirements under EU law that are applicable to the relevant payments service or e-money service do not address the threat;
- the relevant competent authorities have not taken action to address the threat or the actions that have been taken do not adequately address the threat.

The exercise of this power by the EBA could have a significant disruptive impact on the functioning of a payment institution. There is a need for clarity on what criteria would be used by the EBA in determining when there is a significant number of PSUs or a threat to the orderly functioning of the payment or e-money services markets, and the integrity of these markets or to the stability of the whole or part of these markets in the EU.

Recommendation: In order to understand how the EBA would use this power, the Commission's planned delegated acts to specify criteria and factors to be taken into account by the EBA should be published prior to the implementation of the PSR.

13. SCA

We note the migration of the many of the Strong Customer Authentication (SCA) implementation provisions currently in Level 2 text (*EBA Guidelines, EBA Opinions, EBA responses to industry questions submitted to the Q&A section of the EBA website*) to Level 1 Payment Services Regulation. The industry has invested significant resources in implementing SCA requirements set out in PSD2. We are in favour of minimal amendment to these provisions, providing only for the evolution of technology, new approaches to security and increased implementation.

(i) **PSR versus level 2 text**: The provisions should also allow for the expansion of the permitted mix of authentication factors to mirror technological developments, and these may be better set out in Guidelines or in other level 2 text. Codifying low value exemption thresholds for remote and for NFC transactions for example or transaction risk assessment limits will act as a barrier to reacting to market/technology developments or to evolving fraud patterns. Such limits are better addressed in level 2 text.

We welcome the ability to utilise two factors from the same category, improving firms' ability to develop innovative authentication solutions that are better integrated in payers' purchase interactions.

(ii) **Outcomes and risk-based approach**: We continue however to be in favour of a more flexible risk and outcomes-based regime that would enable the deployment of a range of authentication mechanisms that cater for the level of risk associated with the transaction, the customer and the circumstances. This could be accommodated in the provisions of Article 85(1).

It can also be reflected in a revised RTS that is open to different technical solutions and which allows PSPs to apply the level/type of authentication that is appropriate to achieve particular security and fraud outcomes, whilst maintaining a positive and superior customer experience.

The range of SCA tools can be described whilst providing PSPs with the flexibility of applying the most effective technologies for their specific user journeys and product/service profiles. These should include both active and passive means of authentication, that may be less disruptive and equally effective.

One area where greater flexibility would deliver significant benefits is in the treatment of corporate customers and of payments they initiate; such payments currently experience very low levels of fraud. The circumstances of such payment transaction services, such as continuous payments over an extended period of time, as well as the regular use of hardware credentials means that PSPs can implement SCA rules that better meet user needs, without compromising security. The 5-minute inactivity log-off rule for example is often inappropriate, disrupting working practices and introducing delays and inefficiencies in complex operational processes. This is consistent with the provisions of Recital 39, and could be more strongly reflected in the provisions of the main text of the Regulation.

Other PSPs serving corporate customers have experienced difficulties implementing API-based SCA processes as described in the current RTS, and would benefit from greater technical flexibility in implementing SCA. A more limited solution could be achieved by extending *Article 17 of the current SCA-RTS (CDR 2018/389) to also apply in respect of actions "through a remote channel which may imply a risk of payment fraud or other abuses".*

(iii) EBA Mandates: we are supportive of the role of level 2 text and appreciate the need to elaborate or set/change specific parameters from time to time. We remain cautious as to whether transaction monitoring is a subject that would benefit from more specific rules or guidance.

Recommendations: we propose giving greater consideration to adopting a more risk and outcomes- based approach to the application of SCA, enabling greater flexibility as to when it applies, how it is applied and the means of implementation, particularly for different user groups. Limits and parameters are best addressed within Level 2 text to ensure a more dynamic response to technical developments as well as evolving fraud patterns.

14. Application of PSD3/PSR provisions to a DLT based payment product

It is envisaged that PSD3 and the PSR will apply to electronic money tokens ("EMT") and potentially to any other DLT structured payment system that enables payment transactions using electronic money or scriptural money.

It merits therefore considering the impact of DLT on the regulatory structure envisaged under both PSD3 and the PSR and whether the payment services regulatory provisions can be simply applied mutatis mutandis, or whether further considerations are required.

(i) Governance of the PSP and the locus of supervisory provisions

Under a centralised structure, the PSP is and its management are responsible for the technical infrastructure (whether outsourced or not), the payment services operations and the user relationship, including dispute resolution, liability etc.

Under a DLT arrangement, the payment service and the product offering may be shared by a number of parties, the issuer of a token for example that makes it available to distributors, distributors who sell it to users, and then users who may either transfer it bilaterally with other wallet holders, or who may utilise custodians to hold and transfer the value.

Each of those entities will undertake part of the regulated service or in the case of users, may perform payment transactions independently of any regulated entity. The relative roles and the responsibilities that attach to each party therefore merit elaboration, and mapping onto the regulatory obligations.

(ii) The use of public IT infrastructure to create tokens, record transfers and identify ownership is novel in the payments' space, and poses questions around the extent of responsibility for the IT infrastructure, the limitations of outsourcing versus collaboration and the ability to initiate and achieve changes to the infrastructure, whether to facilitate product development or to mitigate risk.

(iii) The nature and extent of the user relationship, service levels and liability

In the case of an EMT, the user relationship may be split up as follows:

The issuer of the EMT, has an obligation to the user for redemption, even if this is undertaken indirectly in practice; they have the obligation because they hold the safeguarded funds

- A distributor or crypto exchange may offer access to the EMTs but without undertaking any payment services, they may sell the token for fiat, and deliver it to the user in fulfilment of a purchase obligation, acting as principal and not as a payment service provider.
- Similarly custodians may host the tokens for the user without offering payment services.
- Alternatively, an exchange or custodian -(crypto asset service provider ("CASP")) may facilitate the transfer of the tokens to the user or to third parties, acting as a payment service provider, and needing to comply with obligations in relation to framework contracts, disclosure and liability etc. Note however that each CASP will have its own user terms, service levels, means of undertaking SCA, dispute resolution mechanisms etc. and will apply these to the different crypto asset products that it offers. This means that a single EMT may be subject to a range of service levels, depending on the CASPs used to access and transact it.

The locus of the different PSD3/PSR obligations will therefore need to be better understood and the manner in which they will attach to the different ecosystem participants will need to be elaborated. This could impact some of the definitions, the authorisation requirements, the focus of service level expectations, the scope of outsourcing, and governance expectations.

We continue to consider the impact and will elaborate the issues over the next months.

15. Access to NFC services set out under the Digital Euro ("DE") Regulation and access for other payment services.

Recital 69 and Article 33 of the draft DE Regulation sets out expectations on access to NFC services for the DE, and it would be welcome to extend similar access to other payment products that will coexist with the DE.

16. IBAN Discrimination

This issue has been high on the European Commission's priority list and could benefit from support in the PSR. This could take the form of (i) setting out expectations of non-discrimination on the one hand, whilst also (ii) providing examples of unacceptable practices on the other. (iii) These can then be backed with explicit enforcement provisions that include NCA expectations on addressing complaints and SLAs for addressing such discrimination. It

could also be appropriate to ensure that enforcement powers extend to non-regulated entities perpetuating IBAN discrimination.

Members of the EMA, as of November 2023

AAVE LIMITED
Airbnb Inc
Airwallex (UK) Limited
Allegro Group
Amazon
American Express
ArcaPay UAB
Banked
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network EMEA Limited
Boku Inc
Booking Holdings Financial Services International Limited
BVNK
CashFlows
Circle
Citadel Commerce UK Ltd
Contis
Corner Banca SA
Crypto.com
eBay Sarl
ECOMMPAY Limited
Em@ney Plc
emerchantpay Group Ltd
Etsy Ireland UC
Euronet Worldwide Inc
Facebook Payments International Ltd
Financial House Limited
First Rate Exchange Services
Flex-e-card
Flywire
Gemini
Globepay Limited
GoCardless Ltd
Google Payment Ltd
HUBUC
IDT Financial Services Limited
Imagor SA
Ixaris Systems Ltd
J. P. Morgan Mobility Payments Solutions S. A.
Modulr Finance Limited
MONAVATE
MONETLEY LTD
Moneyhub Financial Technology Ltd
Moorwand
MuchBetter
myPOS Payments Ltd
Nuvei Financial Services Ltd
OFX
OKG Payment Services Ltd
OKTO
One Money Mail Ltd
OpenPayd
Own.Solutions
Park Card Services Limited
Paymentsense Limited
Paynt
Payoneer Europe Limited
PayPal Europe Ltd
Paysafe Group
Paysend EU DAC
Plaid
PPRO Financial Ltd
PPS
Ramp Swaps Ltd
Remitly
Revolut
Ripple
Securiclick Limited
Segpay
Skrill Limited
Soldo Financial Services Ireland DAC
Square
Stripe
SumUp Limited
Swile Payment
Syspay Ltd
Transact Payments Limited
TransferMate Global Payments
TrueLayer Limited
Trustly Group AB
Uber BV
VallettaPay
Vitesse PSP Ltd
Viva Payments SA
Weavr Limited
WEX Europe UK Limited
Wise
WorldFirst
Worldpay
Yapily Ltd