EBA CLEARING response to the proposed Payment Services Regulation

As the private sector operator of the pan-European SEPA payment systems STEP2-T and RT1, EBA CLEARING welcomes the opportunity to provide feedback on the proposed Payment Services Regulation.[1]

For your consideration, in Annex 1, EBA CLEARING has suggested specific amendments to the proposal wording, along with the reasoning behind each proposed amendment. We have also made available below a summary of our main observations for your convenience.

EBA CLEARING looks forward to continued dialogue with the European Union institutions, and to contributing towards the realisation of the Commission's objectives.

Summary

Fraud detection and prevention

- EBA CLEARING appreciates the Commission's desire to enhance the ability of payment systems and payment service providers (PSPs) to process personal data and share information for the purpose of the prevention and detection of fraud. In this sense, it is our view that the proposal could go further, in particular by broadening the type of information PSPs can share with each other, as well as with third party providers of fraud prevention and detection mechanisms/solutions.

IBAN/Name verification

- It is essential that the Commission's legislative proposals maintain a level playing field between all digital payments, i.e. SCT, SCT Inst, and any new central bank digital currency. For example, as currently drafted, there are unnecessary differences between:
    - the proposed Instant Payments Regulation and the proposed Payment Services Regulation, as regards the IBAN/name-check requirement; and
    - the proposed Payment Services Regulation and the proposed legislative framework for a digital euro, as regards fraud detection and prevention.

- Legislative proposals should leave space for the market to develop innovative solutions and products and should avoid being overly prescriptive in terms of the technical approach the industry should take.
    - For example, an IBAN/name-check can use real-time feedback from the payee PSP, historical data from transactions previously sent by this payee PSP, or a combination of both. The advantages of historical transaction data are that (1) there is no dependency on the availability of the Payee PSP to provide a response (it might take time before the market has implemented these responses); and (2) the response could be complemented with pattern and anomaly information. Such information is not only useful to assess the actual risk but could also limit false negatives, for example when matching a payee's name against a reference name of a joint account.

[1] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010

- Similarly, while the European Banking Authority can propose guidance on the types of transaction monitoring mechanisms PSPs should implement, it is important that PSPs retain the ability to implement new solutions in response to evolving fraud risks.

Access to payment systems

- It is not necessary for the Payment Services Regulation to regulate the access criteria of payment systems that are already regulated by the Principles for Financial Market Infrastructures (PFMI), the SIPS Regulation, and/or the Revised Oversight framework for retail payment systems. These oversight frameworks already contain requirements regarding the access criteria of payment systems.

Annex I: Detailed EBA CLEARING proposals regarding the Payment Services Regulation

Article	Proposed EBA CLEARING amendment	Justification for proposed amendments
Access to payment systems		
Article 31(2)	*A payment system operator shall make publicly available its rules and procedures for admission to participation to that payment system ~~and the criteria and methodology it uses for risk assessment of applicants for participation~~.*	The Commission appears to foresee a two-step process, comprising first, a set of access/participation criteria (Article 31(1)) and, in addition, a risk assessment of the prospective participant (Article 31(3)). In EBA CLEARING's experience as a system operator, the assessment of compliance with the system's access rules is the same exercise as the risk assessment. Because retail payment systems in the EU are already required to apply risk-based access criteria under the Principles for Financial Market Infrastructures, compliance with these criteria should already ensure that an entity would not bring undue risk to the system. On this basis, it should not be necessary to conduct an *additional* risk assessment of each entity. For example, for instant payment systems, for which the Commission foresees a significant increase in participation,[2] it will not be operationally or economically feasible for system operators to conduct an individual risk assessment of each applicant, in addition to an assessment of the prospective participant's compliance with the access rules.
Article 31(3)	*Upon receiving an application for participation by a payment service provider, a payment system operator shall assess ~~the relevant risks of granting~~whether the applicant payment service provider ~~access to the system~~meets the conditions for admission to participate in that payment system. A payment system operator shall only refuse participation to an applicant payment service provider where the applicant ~~poses risks to the system, as referred to in paragraph 1~~does not meet the conditions for admission to participate in the system. The payment system operator shall notify that applicant payment service provider in writing whether the request for participation is granted or refused and shall provide full reasons for any refusal.*	
Article 31(4)	*Paragraphs 1, 2~~, and~~ 3 and 5 shall not apply to payment systems composed exclusively of payment service providers belonging to the same group, to payment systems designated*	Certain payment systems are already regulated under the Principles for Financial Market Infrastructures (PFMI),[3] as transposed in the EU by the

[2] *Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro* ("Instant Payments Regulation").
[3] https://www.bis.org/cpmi/publ/d101a.pdf.

Article	Proposed EBA CLEARING amendment	Justification for proposed amendments
	under Regulation (EU) No 795/2014, or to payment systems otherwise subject to Eurosystem oversight under the Revised oversight framework for retail payment systems.	SIPS Regulation[4] and the ECB's *Revised oversight framework for retail payment systems*[5], as well as the Settlement Finality Directive. Systemically important payment systems (SIPS) are subject to the SIPS Regulation. Under Article 16 of the SIPS Regulation, SIPS operators must have participation criteria that are (inter alia) "*objective, non-discriminatory and proportionate*" and "*justified in terms of the safety and efficiency of the SIPS and the markets it serves, and be tailored to and commensurate with the SIPS's specific risks*". Further, "*a SIPS operator shall set requirements that restrict access to the minimum possible extent. If a SIPS operator denies access to an applying entity, it shall give reasons in writing, based on a comprehensive risk analysis*". In other words, the Commission's objectives are already accomplished by the SIPS Regulation, and it is not clear to EBA CLEARING what can be further achieved in this respect through the PSR. For payment systems that are not (yet) designated as systemically important, the ECB's *Revised oversight framework for retail payment systems* requires retail payment systems to have participation criteria that are (inter alia) "*objective, risk-based, and […] which permit fair and open access*" (see further, PFMI 18). As above, the Commission's objectives with regard to the access criteria of payment systems have already been achieved through the implementation of the global Principles for Financial Market Infrastructures in the EU, via the *Revised oversight framework for retail payment systems.*

[4] Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (ECB/2014/28), as amended.

[5] https://www.ecb.europa.eu/pub/pdf/other/Revised_oversight_framework_for_retail_payment_systems.pdf.

Article	Proposed EBA CLEARING amendment	Justification for proposed amendments
		Analogies can be drawn with the Digital Operational Resilience Act (DORA)[6] which has a specific carve-out for payment systems that are already overseen.
Article 31(7)	*For payment systems that are not covered by Eurosystem oversight, pursuant to Regulation (EU) No 795/2014 or another oversight framework, Member States shall designate a competent authority responsible for oversight of payment systems to ensure enforcement of paragraphs 1 2, 3, 5 and 6 by payment systems governed by their national law, in coordination with other competent authorities via the Eurosystem to ensure consistent application across jurisdictions.*	Article 31(7), as drafted, creates a risk of forum shopping whereby each competent authority could interpret Article 31 differently, leading payment service providers to join, or not to join payment systems on this basis, impacting the level playing field. Further, as explained above in relation to Article 31(4), in addition to the SIPS Regulation, certain payment systems in the EU are already overseen via the ECB's *Revised oversight framework for retail payment systems.* It is important that the PSR remains coherent with these frameworks.
Article 93(2)	*In the event of infringements or suspected infringements of Titles II and III by technical service providers, ~~payment system operators~~ ATM deployers which do not service payment accounts, electronic communications services providers or by their agents or branches, the competent authorities shall be those of the Member State where the service concerned is provided.*	The only part of the PSR that regulates payment system operators is Article 31. Article 31(7) already provides that Eurosystem or Member State oversight is responsible for enforcing compliance with Article 31. Article 93(2) conflicts with Article 31(7), by assigning a different competent authority the responsibility to enforce compliance with the PSR vis-à-vis payment system operators (i.e., the enforcement of Article 31). Therefore, payment systems should be removed from the scope of Article 93(2).
Fraud detection and prevention		
Article 83(3)	*To the extent necessary to comply with paragraph 1, point (c), payment service providers may exchange ~~the unique identifier of a payee~~ the information referred to in paragraph 2 with other*	The PSR should establish the principle that PSPs should be authorised to share information for the purpose of preventing and detecting fraud. To ensure effective, dynamic, and evolving fraud prevention and

[6] Under Article 31(8)(ii) "*ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union*" are exempt from DORA.

Article	Proposed EBA CLEARING amendment	Justification for proposed amendments
	payment service providers who are subject to information sharing arrangements as referred to in paragraph 5, as well as with the provider of the information sharing arrangement, as applicable ~~when the payment service provider has sufficient evidence to assume that there was a fraudulent payment transaction. Sufficient evidence for sharing unique identifiers shall be assumed 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 transfer~~. Member States shall ensure that national law does not restrain payment service providers from exchanging information, including across an EU border, under such information sharing arrangements.	detection, PSPs should be able to share information other than unique identifiers, and in a broader range of scenarios than the proposed definition of "sufficient evidence". EBA CLEARING draws attention to the legislative proposal for a digital euro, for example, which would allow PSPs to share: *(i) information on digital euro payment accounts, including the unique digital euro account identifier; (ii) information on online digital euro payment transactions, including the transaction amount; and (iii) information on the transaction session of a digital euro user, including the device internet protocol address-range* (Digital Euro proposal, Article 32(4)). Further,Article 32(4) of the Digital Euro proposal explicitly allows PSPs to share information with a "*fraud prevention and detection mechanism*". There is no objective justification for differences between the regulatory regimes for a new digital euro and existing forms of digital euro, particularly as the PSR is intended to cover both. It is also useful to compare the PSR proposal with AML/CFT legislation. AML/CTF legislation allows PSPs to share with other PSPs the existence of a reported suspicion or ongoing analysis for money laundering/terrorism financing (Article 39(5) AML Directive). This type of information would also be relevant for the detection and prevention and fraud. Overall, EBA CLEARING believes that a higher level of legal certainty about the legality of the information exchange between PSPs would be welcome. Such comfort could be reached if PSPs that choose to join any information sharing arrangement as foreseen by the PSR had an *obligation* (rather than mere permission) under the PSR to exchange information on fraud with the other participants in such arrangement.

Article	Proposed EBA CLEARING amendment	Justification for proposed amendments
		PSPs should also be protected, in sharing information under these arrangements, from no-tipping off or banking secrecy obligations, in particular where such rules would restrict EU cross border exchanges.
Article 83(4)	~~*The information sharing arrangements shall define details for participation and shall set out the details on operational elements, including the use of dedicated IT platforms.*~~	The purpose and meaning of this provision – in particular, the reference to "dedicated IT platform" and "details on operational elements" – are not clear.
Article 83(4)	~~*Before concluding such arrangements, payment service providers shall conduct jointly a data protection impact assessment as referred to in Article 35 of the Regulation (EU) 2016/679 and, where applicable, carry out prior consultation of the supervisory authorityas referred to in Article 36 of that Regulation.*~~	The obligations of controllers or joint controllers, as applicable, to carry out a data protection impact assessment and to consult authorities already exist under the GDPR and would apply to information sharing arrangements, with controllers accountable to assess whether to enter the information sharing arrangement. The PSR is more restrictive than the GDPR, by: (1) imposing a joint controllership model; and (2) requiring a data protection impact assessment. Regarding the requirement to potentially consult with a supervisory authority, it is not clear which authority PSPs using a pan-European information sharing arrangement should consult.
Article 89(g)	*The EBA shall develop draft regulatory technical standards which shall specify […]* *(g) the* ~~*technical requirements for*~~*objectives of the transaction monitoring mechanisms referred to in Article 83.*	As noted above in relation to Article 83(3), fraud patterns evolve, and fraud detection and prevention must be a dynamic process. It is important that the EBA RTS allow the industry to continue to innovate with respect to fraud detection and prevention, and allow PSPs to take any necessary actions to comply with the spirit of the PSR.
IBAN / name verification		
Article 50(1) and 50(2)	*In case of credit transfers, the payment service provider of the payee shall, free of charge,* ~~*at the request of*~~*if requested by the payment service provider of the payer, verify whether or not the*	EBA CLEARING supports a level playing field between SCT and SCT Inst transfers. It therefore makes sense to extend the IBAN/name-check

Article	Proposed EBA CLEARING amendment	Justification for proposed amendments
	unique identifier and the name of the payee as provided by the payer match, and shall communicate the outcome of this verification to the payment service provider of the payer. Where the unique identifier and the name of the payee do not match, the payment service provider of the payer shall notify the payer of any such discrepancy detected and shall inform the payer of the degree of that discrepancy. *The payment service providers shall provide the service referred to in paragraph 1 immediately after the payer provided to its payment service provider the unique identifier and the name of the payee, and before the payer is offered the possibility to authorise the credit transfer.*	requirement to SCT transactions, assuming that the Instant Payments Regulation becomes law. At the outset, EBA CLEARING notes that there are differences in the proposal in the Instant Payments Regulation and PSR Article 50. These differences should be eliminated. Article 50 should allow Payer and Payee PSPs to achieve the objectives of the regulatory proposal – IBAN/name verification – in the most efficient and effective manner, leaving room for the development of user-driven schemes.[7] As currently drafted, Article 50 is prescriptive in terms of the technical approach. It is preferable that the legislation remains agnostic as the technology and processes that can be applied. For example, it should be possible that the payer and payee PSP can use historical data for the purpose of complying with requirement to verify the unique identifier against the name of the payee, as an alternative to a real-time verification against the Payee's customer database. Historical data has two benefits. First, it is available to the Payer PSP, even where the Payee PSP is offline. Achieving 24/7 Payee PSP availability is likely to take time and historic data can alert payers that their intended payment may be to a

[7] This view is also expressed in the Impact Assessment of the Instant Payments Regulation: "*EU PSPs would be allowed to decide on the best implementation approach. Solutions already provided by fintech companies in some Member States could be used by PSPs in other Member States, and this could open up the market for more providers of such services. Solutions could also be collectively implemented through an industry-wide arrangement or scheme, which could to a certain extent leverage on advances made in the context existing industry-wide initiatives*" (page 48, emphasis added) https://ec.europa.eu/finance/docs/law/221026-impact-assessment_en.pdf.

Article	Proposed EBA CLEARING amendment	Justification for proposed amendments
		fraudulent account, even in the absence of verification by the Payee PSP. Second, historical data is particularly useful in a pan-European context in with different languages, character sets and customs as regards names can result in false negatives for cross-border payments. Historical data, demonstrating for example that non-fraudulent payments have already been made to a beneficiary with that particular spelling, can reduce such false negatives. PSPs should also be explicitly authorised to rely on third party service providers to provide the IBAN/name check service, on the understanding that the liability under the regulation remains with the PSPs. Reliance on a central third-party provider is an efficient option, as the third-party provider can normalise the validation of different algorithms from different PSPs.