Position Paper

2023 November

On the Proposal for a Regulation on payment services in the internal market and amending Regulation (PSR) & On the Proposal for a Directive on payment services and electronic money services in the Internal Market (PSD3)

Introduction

Bitkom already published a detailed position papers on its members' view on PSD3 and PSR in August 2023[1]: in this position paper we clearly underpinned our general positive assessment of PSD2 and its beneficial impact on increasing competition in the European payments ecosystem.

In the light of the current debates within the council and the European Parliament, we wanted to revisit our existing initial position and propose concrete amendments regarding the EU Commission's proposal of PSD3 as well as PSR. As in our previous paper our focus pivots on:

- Futureproofing SCA: currently, we particularly perceive several shortcomings that include a lack of needed clarity regarding SCA exemptions, a lack of contemplation regarding technical solutions and biometrics, and a lack of practicality for delegated SCA as well as third party hardware relations.
- Securing a level playing field among players: this relates to unclear considerations regarding licensing of EMIs and PIs or questions regarding liability.
- Maintaining legal coherence: existing definitions partly fall short accuracy, which may lead to unintended outcomes for existing services (e.g. credit granting by PIs) or may cause intra-European fragmentation.

We appreciate the European Parliament's ambition of moving toward an agreement before the upcoming election 2024. Yet, with an European payment ecosystem that faces increasing complexity also in relation to other acts, such as FIDA or MiCA, it is crucial to provide the needed room for negotiations. Reaching premature agreements would considerably harm future developments in the field of payments.

[1] Bitkom Position Paper on Payment Services Regulation & Payment Services Directive, see: https://www.bitkom.org/Bitkom/Publikationen/Regulation-Directive-on-Payment-Services-PSR-PSD

Position Paper

PSD 3: Proposed Amendments

Issue	Problem & Solution Statement	Section	Proposed Amendments
Licensing	**Specification for reauthorization of existing PIs and EMIs under PSD3 is needed:** Existing PIs and EMIs should be allowed to continue to provide their services under their current PSD2/EMD2 licenses without the need to seek a new PSD3 license. A presumption of automatic re-authorisation is needed as well as specification that firms should provide only the information required to assess whether they comply with newly introduced requirements under PSD3.	Recital 19	To ensure more consistency in the application process for payment institutions, it is appropriate to mandate the EBA to develop draft regulatory technical standards on authorisation, **including on the information to be provided to the competent authorities in the application for the authorisation of payment institutions, a common assessment methodology for granting authorisation or for registration including a proportionately designed process for grandfathered e-money institutions based on relevant factors such as the existing level of supervision and adherence to regulatory requirements**, what can be considered as a comparable guarantee to professional indemnity insurance and the criteria to be used to stipulate the minimum monetary amount of professional indemnity insurance or a comparable guarantee.”
		Article 44 (1), (2)	Member States shall allow payment institutions that have been authorised pursuant to Article 11 of Directive (EU) 2015/2366 (PSD2) **or E-Money-Institutions pursuant to Art. 3 (1) of Directive 2009/110/EG in connection with Art. 11 PSD2** by [OP please insert the date = 18 months after the date of entry into force of this Directive] to continue to provide and execute the payment services for which they have been authorised, without having to having to seek authorisation in accordance with Article 3 of this Directive or to comply with the other provisions laid down or referred to in Title II of this Directive until [OP please insert the date = 24 months after the date of entry into force of this Directive]. Member States shall require such payment institutions as referred to in the first subparagraph to submit to the competent authorities ~~all~~ **the** information **pursuant to Art. 3 (3) (e) second half sentence (DORA-compliance), (f), (h), (j) No. (iii), and (s) of this Directive** ~~that enables those~~

Issue	Problem & Solution Statement	Section	Proposed Amendments
			~~competent authorities to assess~~, by [OP please insert the date = 24 months after the date of entry into force of this Directive]~~, either of the following:~~. ~~(a) whether those payment institutions comply with Title II and, where not, which measures need to be taken to ensure compliance;~~ ~~(b) whether the authorisation should be withdrawn.~~ Payment institutions as referred to in the first subparagraph **which will have submitted the complete information required under the second subparagraph hereof and by the date specified therein** ~~upon verification by the competent authorities comply with Title II~~ shall be **automatically** authorised as payment institutions pursuant to Article 13 of this Directive and shall be entered in the registers referred to in Articles 17 and 18. ~~Where those payment institutions do not comply with the requirements laid down in Title II by [OP please insert the date = 24 months after the date of entry into force of this Directive], they shall be prohibited from providing payment services.~~ 2. ~~Member States may provide for payment institutions as referred to in paragraph 1 to be authorised automatically and be entered in the register referred to in Articles 17 if the competent authorities have evidence that those payment institutions already comply with Articles 3 and 13.~~ The competent authorities shall inform the payment institutions concerned of ~~such~~ the ~~automatic authorisation and~~ registration **granted under the preceding paragraph subparagraph 3** ~~before the authorisation is granted~~.
		Article 45 (2)	Member States shall require the electronic money institutions referred in paragraph 1 to submit to the competent authorities all information that those competent authorities need to assess, by [OP please insert the date = 24 months after the date of entry into force of this Directive], whether those electronic money institutions comply with **the new requirements introduced under** this Directive. **Licensed electronic money institutions referred to in paragraph 1 shall be considered as compliant with the preserved requirements of Directive 2009/110/EC, which are already subject to supervision.** Where such assessment reveals that those electronic money institutions do not comply with **the new** requirements, the competent authorities shall decide which measures need to be taken to ensure such compliance, or to withdraw the authorisation.

Issue	Problem & Solution Statement	Section	Proposed Amendments
Scope	Sphere of Application is not regulated: A new article 1 (5) PSD3 should state, that PSD3, except for articles 37 and 38 PSD3, shall not apply to the services listed in article 2 (2) PSR. Reference to article 2 (2) PSR to be corrected: In various articles of PSD3 (e.g. Art. 39) references made to article 2 (1) PSR should instead refer to article 2 (2) PSR.	Article 1 (5)	
	Clarification of definition of agents and use of agents in multi-processor set-ups: Specify that marketplaces and platforms supported by PSPs which remove them from control or possession of funds for third parties are not by default agents of the PSP. In addition, every agent only acts on behalf of one acquirer as their principal (PSP) and not in respect of all payment services provided to the payment services user	Recital 45 (a new) Recital 45 (b new)	**Recital 45 (a new)** **When acquirers use an agent to deliver payment services, it should be noted that the agent only acts on behalf of one acquirer as the principal payment service provider and not in respect of all payment services provided to the payment services user.** **Recital 45 (b new)** **To take into account evolving market realities, marketplaces and platforms supported by payment service providers, that remove the latter from the control or the possession of funds for third parties, shall not be considered by default agents of the payment service providers.**
	Credit Granting by PIs	Art 10 (4)	Add in Art 2 (definitions) (40) “credit” means lending including, inter alia: consumer credit, factoring, with or without recourse, financing of commercial transactions (including forfeiting). [cf. Annex I No. 2 CRD IV]

PSR: Proposed Amendments

Issue	Problem & Solution Statement	Section	Proposed Amendments
Scope	**Payment transactions within groups of companies** are insufficiently outlined and needs thus to be amended.	Art. 2 (2) (m)	[...] and the collection of payment **orders and the provision of funds** on behalf of **companies belonging to the same** group by a parent undertaking or its subsidiary for onward transmission to a payment service provider **and the collection of funds from payers out-side of the group for onward transmission to group companies**.
Cross-European Supervisory Coherence	For payment service providers active in multiple EU member states, obtaining supervisory exemptions is inefficient as it has to be granted by each individual national competent authority. This conflicts with the overall vision of a single market. **<u>Alternative solutions:</u>** Add the requirement for the EBA and the relevant national competent authorities to take a coherent exemption decision which applies equally across all Member States for which the payment service providers applies.	Art. 39 (1)	By way of derogation from Article 35(1), on request of an account servicing payment service provider, the competent authority may exempt the requesting account servicing payment service provider from the obligation to have in place a dedicated interface and allow the account servicing payment service provider to either offer, as interface for secure data exchange, one of the interfaces that the account servicing payment service provider uses for authentication and communication with its payment services users or, where justified, not to offer any interface at all for secure data exchange. **For the purpose of the first paragraph, and where justified, for those account servicing payment service providers providing payment services to payment services users in multiple Member States and applying for the exemption in multiple Member States with identical justification, the EBA together with the relevant national competent authorities should take a decision on the exemption that coherently applies in all of the relevant Member States.**
Liability	**Auhtorisation vs. Authentication:** The Commission considers that, with impersonation scams, the difference between authorised and non-authorised transactions is becoming more blurred and complex to apply in practice. We disagree as even in the case of authorised push scams, there is no ambiguity surrounding the fact that the payer intends to carry out the transaction at that	Art. 55	Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the burden shall be on the payment service provider to prove that the payment transaction was ~~authorised~~ **authenticated**, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider. If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence,

Issue	Problem & Solution Statement	Section	Proposed Amendments
	moment (it is only afterwards that they realise they have been misled and subjected to a scam). **Article 55 PSR must refer to "authentication" rather than "authorisation" as the "authentication" (Option 1)** of a payment transaction is something that PSPs are able to demonstrate. "Authorisation" means the payer's consent to carry out the payment transaction as outlined in the contract, encompassing the customer's expression of will. Typically, this 'will' is expressed through the authentication process. On the other hand, "authentication" relates to the procedure enabling the PSP to verify the identity of a payment service user. Whilst PSPs lack the means to demonstrate whether a payment transaction has been authorised (as they are not able to analyse the customer's state of mind and prove the 'client's will'), they are able to demonstrate whether the payment transaction has been authenticated or not. **A clear definition of "authorisation" in the regulation would avoid ambiguities (Option 2)** It is important to have legal certainty about the authorisation and thus the finality of the transaction. Under PSD2, a payment transaction is considered unauthorised in the absence of consent. Whilst Art.49 states that payment transactions shall be authorised only if the payer 12 has given its permission for the execution of said transaction, it should also include a definition of authorisation. Such a definition could look like: "The expression of the permission given by the payer to his PSP to execute a transaction, through the process		the payment transaction was ~~authorised~~ **authenticated**, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

Issue	Problem & Solution Statement	Section	Proposed Amendments
	and in the form agreed between the payer and his PSP. Permission can be given by the payer by using the personalised security credentials.”		
	Impersonation Fraud, Social Engineering & Spoofing:	Art. 59 (1) Art. 59 (2)	**Art. 59(1)** (1) Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer’s payment service provider using the name **and** e-mail address or telephone number of that payment service provider unlawfully and this manipulation gave rise to subsequent fraudulent authorised payment transactions, **the payment service provider shall refund the** consumer **who shall be entitled to request the refund of the** full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without any delay, **submitted reasonable documentation to prove the occurrence of the impersonation fraud, can demonstrate the fraud was** reported ~~the fraud~~ to the police and notified its payment service provider. **Art. 59 (2)** (2) **If all the conditions listed under paragraph 1 apply, within 15**~~10~~ business days after **the consumer has presented to the payment service provider the confirmation of the report submitted to the police, and has submitted reasonable documentation to prove the occurrence of the impersonation fraud as requested by the payment service provider noting or being notified of the fraudulent authorised payment transaction**, the payment service provider shall do either of the following: a. refund the consumer the amount of the fraudulent authorised payment transaction; **b. not refund the consumer where:** ~~b.~~ **i)** where the payment service provider has reasonable grounds to suspect a fraud or a gross negligence by the consumer **ii. the consumer has fallen victim of a similar fraud and obtained a refund from a payment service provider previously, or** **iii. the payment service provider can demonstrate that the consumer has not observed obligations established in the framework contract or communicated in the form agreed within**

Issue	Problem & Solution Statement	Section	Proposed Amendments
			the framework contract, such as, not providing credentials to third parties, not clicking on links included in SMSs or emails, or having entrusted payment instrument to a third party. **Payment service providers shall** provide a justification for refusing the refund and indicate to the consumer the bodies to which the consumer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the consumer does not accept the reasons provided.
SCA	**Differentiation between consumers, SMEs & larger companies:** PSD2 taught the lesson that despite neutrality in terms of technology and business models, a regulatory framework requires a certain level of flexibility to efficiently distinguish between the different payment service user groups. In its Opinion on the review of PSD2 published on 23 June 2022, the European Banking Authority acknowledged the need for a more targeted approach and a more flexible supervisory mandate that considers different business models and user groups. Alternative Solution Enable the EBA to differentiate between consumers, small/micro enterprises, medium enterprises and large corporates when drafting the regulatory technical standards as per Art. 89 (2) to ensure a more targeted definition of strong customer authentication requirements and reduce existing friction caused by the different payment behavior of these user groups.	Recital 39 Recital 116 Art. 89 (2)	**Recital 39:** As consumers and undertakings are not in the same position of vulnerability, they do not need the same level of protection. While it is important to guarantee consumer rights by provisions from which it is not possible to derogate by contract, it is reasonable to let undertakings and organisations agree otherwise when they are not dealing with consumers. **This should include the level of strong customer authentication to be applied where the payer is a corporate payer, and is making payments in a corporate environment.** Micro-enterprises, as defined in Commission Recommendation 2003/361/EC, may be treated in the same way as consumers. Certain rules should always apply, irrespective of the status of the user. **Recital 116:** Security measures should be compatible with the level of risk involved in payment services. To allow the development of user-friendly and accessible means of payment for low-risk payments, such as low value contactless payments at the point of sale, whether or not these payments are based on mobile phone, the exemptions to the application of security requirements should be specified in regulatory technical standards. Safe use of personalised security credentials is needed to limit the risks relating to spoofing, phishing and other fraudulent activities. The user should be able to rely on the adoption of measures that protect the confidentiality and integrity of personalised security credentials. **Individuals, corporate users, and platform businesses have different needs in relation to strong customer authentication. For a corporate payer, using company information as a knowledge factor to verify that the payer works for the company could, for example, be more useful to**

Issue	Problem & Solution Statement	Section	Proposed Amendments
			mitigate corporate fraud than using the payer's personal information. Similarly, treating each individual seller on a platform as a separate payee can make the application of certain SCA exemptions impractical compared with approaching the issue with the platform model in mind, where the platform can be identified as the payee. The EBA should therefore take into account the nature of the transaction, and its counterparts, when defining regulatory technical standards. **Art. 89 (2) (f new)** **(f) the need to allow for different standards depending on the needs of payment service users which are** **(i) consumers** **(ii) micro, small and medium-sized enterprises (SMEs) (as per EU recommendation 2003/361)** **iii) large corporates falling outside the scope of that EU recommendation**
	Increase flexibility in SCA and allow for behavioural biometrics: Reference to the use of behavioral biometrics and environmental factors in the provision on transaction monitoring should be extended to SCA. Recognize behavioral biometrics as a valid authentication factor of 'inherence'.	Art. 83 (1)	**Article 83** [...] (d) session data, including the device internet protocol address-range from which the payment account has been accessed. Payees' payments service providers shall provide the data required for the purposes referred to in paragraph 1 to the payment service providers involved in the transaction. Payment service providers shall not store data referred to in this paragraph longer than necessary for the purposes set out in paragraph 1, and not after the termination of the customer relationship. Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors: [...] (e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

Issue	Problem & Solution Statement	Section	Proposed Amendments
			Payment service providers are allowed to use the data listed in the first subparagraph of Article 83(2) for strong customer authentication as an element of 'inherence' (something the user is) pursuant to Article 3(35). […].
	There is a need to mandate EBA to differentiate between SMEs & corporates.	Art. 85 (11)	**Art. 85 (11) (d new)** Any exemptions from the application of strong customer authentication to be designed by the EBA under Article 89 shall be based on one or more of the following criteria: (a) the level of risk involved in the service provided; (b) the amount, the recurrence of the transaction, or both; (c) the payment channel used for the execution of the transaction ; **(d) whether the transaction is made on behalf of or by consumers or corporate payers.**
	Delegating SCA & certification of third party devices: In general, there is a need for a critical discussion that SCA delegation shall never be considered as critical outsourcing. Regarding (Art. 89 (1)) there is a dire need to create a certification scheme and process that certifies third party devices. Otherwise, SCA will simply not be manageable for financial institutions which would be in need to enter contractual agreements not only with each supplier but for each and every device as well.	Art. 87 Art. 89 (1)	**Art. 87** **1.** A payer payment service provider shall enter into an outsourcing agreement with its technical service provider in case that technical service provider is providing and verifying the elements of strong customer authentication **and the payer payment service provider is not in control of strong customer authentication**. A payer's payment service provider shall, under such agreement, retain full liability for any failure to apply strong customer authentication and have the right to audit and control security provisions. **2. A payer payment service provider's outsourcing of strong customer authentication pursuant to paragraph 1 is not outsourcing of a payer payment service provider's critical or important functions.** **3. A payer payment service provider is allowed to enter into multilateral or scalable outsourcing agreements for authorizing technical service providers to provide and verify the elements of strong customer authentication pursuant to paragraph 1.**

Issue	Problem & Solution Statement	Section	Proposed Amendments
			4. Paragraph 1 does not apply to technical services for strong customer authentication that are provided by operators of payment schemes.”
	SCA Exemptions: Clarify SCA Exemptions for low risk and low-value use cases (contactless up to EUR 250), machine payments, payment solutions for corporates without further condition as well as for crypto payments in context of the DLT pilot regime.	Recital 114 Art. 89	**PSR Recital (114)** Under the exemption from SCA under Article 18 of Delegated Regulation (EU) 2018/389, payment service providers were allowed not to apply SCA where the payer initiated a remote electronic payment transaction identified by the payment service provider as posing a low level of risk evaluated on the basis of transaction monitoring mechanisms. Feedback from the market showed however that, in order to have more payment service providers implementing transaction risk analysis, it is necessary to adopt appropriate rules on the scope of transaction risk analysis, introducing clear audit requirements, providing more detail and better definitions on risk monitoring requirements and data to share, and to assess the potential benefits of allowing payment service providers to report fraudulent transactions for which they are solely liable. The EBA should develop draft Regulatory Technical Standards laying down rules on transaction risk analysis. **These should consider additional thresholds for the transaction risk analysis exemption to increase the use of this exemption. In addition, they should consider clarifying whether payment service providers should only count liability towards the payer in their fraud rates, (or liability for financial damages that they owe to other payment service providers also).** PSR 89 (1).... For the purposes of point (b), as regards the exemption from the application of strong customer authentication for payment transactions, based on transaction risk analysis the draft regulatory technical standards shall specify, inter alia: (i) the conditions that have to be met for a remote electronic payment transaction to be considered as posing a low level of risk **including through considering expanding the relevant set of thresholds**; (ii) the methodologies and models to implement transaction risk analysis;

Issue	Problem & Solution Statement	Section	Proposed Amendments
			(iii) the criteria for the calculation of fraud rates, **and in particular, clarity around whether payment service providers should only count liability towards the payer in their fraud rates (or liability for financial damages that they owe to other payment service providers also);** (iv) detailed and proportionate reporting and audit requirements.
Fraud Prevention	**Unconditional refund right from SEPA Direct Debits** to MITs / Maintaining the current balance of consumer and merchant rights under Article 76 (PSD2): The rules should continue to grant an unconditional 8-week refund right to SEPA Direct Debit only. The text could stipulate accelerated timelines for merchants to resolve disputed chargebacks. We welcome the clarification provided by the EU PSR that SCA is not required for transactions initiated 'by the payee only'. However, we are of the view that an unconditional ('no question asked') refund right should not apply to MIT as this would significantly increase fraud and MIT already ensure a very high level of consumer protection.	Art. 62 (1)	Without prejudice to paragraph 3 of this Article, in addition to the right referred to in the first subparagraph of this paragraph, for ~~authorised payment transactions which were initiated by a payee, including~~ direct debits as referred to in Article 1 of Regulation (EU) No 260/2012, the payer shall have an unconditional right to a refund within the time limits laid down in Article 63 of this Regulation.

Bitkom represents more than 2,200 companies from the digital economy. They generate an annual turnover of 200 billion euros in Germany and employ more than 2 million people. Among the members are 1,000 small and medium-sized businesses, over 500 start-ups and almost all global players. These companies provide services in software, IT, telecommunications or the internet, produce hardware and consumer electronics, work in digital media, create content, operate platforms or are in other ways affiliated with the digital economy. 82 percent of the members' headquarters are in Germany, 8 percent in the rest of the EU and 7 percent in the US. 3 percent are from other regions of the world. Bitkom promotes and drives the digital transformation of the German economy and advocates for citizens to participate in and benefit from digitalisation. At the heart of Bitkom's concerns are ensuring a strong European digital policy and a fully integrated digital single market, as well as making Germany a key driver of digital change in Europe and the world.

Published by
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Contact persons
Kevin Hackl | Head of Digital Banking & Financial Services
T 030 27576-109 | k.hackl@bitkom.org

Lukas Marschallek | Policy Officer Digital Banking & Financial Services
T 030 27576-551 | l.marschallek@bitkom.org

Responsible Bitkom committee
AK Digital Payments

This publication is intended to provide general, non-binding information. The contents reflect the view within Bitkom at the time of publication. Although the information has been prepared with the utmost care, no claims can be made as to its factual accuracy, completeness and/or currency; in particular, this publication cannot take the specific circumstances of individual cases into account. Utilising this information is therefore sole responsibility of the reader. Any liability is excluded. All rights, including the reproduction of extracts, are held by Bitkom.