

Position Paper

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)

28. July 2023

Introduction

Bitkom, representing the heterogeneous finance ecosystem, voices the industry perspectives of various financial entities, including banks, exchanges, insurers, and other financial institutions, as well as FinTechs, third-party providers, and tech companies. As such Bitkom has been a staunch supporter of the main objectives outlined in PSD2: creating a more integrated and efficient European payments market, that fosters competition and innovation, whilst ensuring a high level of security and consumer protection, in a technology and business model-neutral way that allows for the development of new types of payment services. This increased data sharing facilitates the development of new and innovative financial services and products, benefiting both consumers and businesses.

Impact of PSD2 and needed improvements: Overall, PSD2 has partially fulfilled its goal in increasing competition, providing legal certainty, and creating a level-playing field. Across the EU there has not only been a rise in the number of issued licenses for TPPs (AISPs & PISPs) by 5 per cent since 2014 but also a general increased interest in the payments market by Big Techs. Yet, there remain some challenges linked to market fragmentation, consumer experience, or lack of standardization, which shall be resolved under the new frameworks: PSR, PSD & FIDA.

Above all, we are delighted to see that the EU Commission has incorporated feedback from market participants to disentangle current political debates regarding financial data sharing and payment services. We believe that the establishment of a payment service regulation will reduce fragmentation to the benefit of the market while leaving national competent authorities in the driver's seat by maintaining the PSD. Bitkom has defined three core principles that should serve as guiding principles for the revision process of PSD2:

Kevin Hackl

Bereichsleiter Digital
Banking & Financial
Services

T +49 30 27576-109
k.hackl@bitkom.org

Lukas Marschallek

Referent Digital Banking
& Financial Services

T +49 30 27576-551
l.marschallek@bitkom.org

Albrechtstraße 10
10117 Berlin

- Futureproof SCA to rebalance security, convenience, and transparency,
- Ensure legal requirements cater for all payment methods and payment service users, and
- Ensure regulatory and supervisory coherence across Europe by eliminating a fragmented interpretation of legal requirements.

Suggested measures in greater detail

Strong Customer Authentication: Balancing Security, Convenience, and Transparency

- **SCA and credit card payments:** While Strong Customer Authentication (SCA) has successfully reduced fraud levels and increased security, it rendered online card payments for consumers more complex and less convenient, paired with a costly and delayed implementation for issuing banks and card schemes. 2FA is not only a question of convenience and UX; it has also led to increased drop-off rates due to overwhelmed consumers (e.g. two separate 2FAS for account verification and payment initiation). **The problem for existing payment solutions, like cards, is that they're not built to support SCA by default. In order to discuss implications and potential solutions Bitkom recommends a deep-dive with the card-industry.**

Such a deep-dive should be carried out in a timely manner to ensure a positive impact on EBA's drafting process of new RTSs and further standardization. Finding measures to strike a right balance between security and convenience will be key to further the payments market, e.g. by focusing on developing a framework for M2M payments regarding SCA. Exemplary: Bitkom recommends abolishing the usage of arbitrary thresholds, as they are not very effective and different flags for fraud control exist. **Bitkom calls for the implementation of an outcome-based framework, that still provides the customer security and the feeling thereof, while granting a PSP with low fraud rates more leeway in setting their thresholds based on how they're able to manage their fraud levels.**

- **SCA and Behavioral Biometrics:** Bitkom calls for the explicit regulation of usage of behavioral scoring for SCA purposes and the use of behavioral biometrics for authentication. The current restrictive approach to biometrics could hinder innovation and hamper efforts to reduce fraud. We would welcome the adoption of an outcome-focused approach to authentication factors, as there are solutions within the industry that operate behind the scenes to authenticate the customer with a high degree of accuracy. For example, behavioral biometrics and transaction risk analysis contribute to less friction, equal or higher security levels and benefit the customer experience in general. These are especially beneficial to vulnerable or elderly groups who may struggle to complete other authentication steps. Other simplifications of SCA (e.g. allowing TPPs to manage SCA) or explicit exemptions

from SCA should be assessed, as it is proposed in EBA's Opinion of June 2022. Whilst we see an indication of this approach in the draft, a clearer commitment is needed as well as an open discussion about what areas will need SCA and what areas may be allowed to apply a different means of authentication.

- **SCA and MOTO:** Bitkom welcomes the clarification of exemptions for MOTO transactions in Article 85 (7) of the proposed PSR. The proposed “adequate security measures to protect the confidentiality, authenticity and integrity [...] of the transaction” (Article 85 (10)), however, needs further clarification. One challenge will relate to uphold “confidentiality” as payers need to convey authentication data via – for instance – the telephone. **Bitkom calls for a deep-dive with the various involved stakeholders such as the card-industry, banks, and relevant industries (e.g. travel) in order to pinpoint the specific needs for a regulation.** Bitkom furthermore calls for stricter rules on issuers to close the customer enrolment gap and fix the customer abandonment rates.
- **Harmonizing the 180-day SCA renewal:** Bitkom welcomes the extension of the SCA re-authentication period for account information services to 180 days. The extension of the authentication period saves time and reduces friction for customers while further fostering automation of business processes by reducing the chance of errors.

Bitkom furthermore calls for an examination on the handling of the RTS by banks with regards to the renewal of SCA authorization. The specific time frame for SCA renewal can vary greatly among banks resulting in customer confusion. Hence, we call for creating the needed clarity in PSR to overcome continued fragmentation in the handling of SCA renewals. Article 86 (3) and (4) are too vaguely formulated. Clearer rules for “reasonable grounds to suspect fraud” need to be formulated to not opening the backdoor to arbitrary misuse.

- **Facilitating SCA for AISPs:** The proposed changes for AISPs to only carry out SCA for the “first access to payment account data” will facilitate SCA handling to the benefit of consumers. Given the fact that AISPs can then do SCA themselves can furthermore help to clarify questions with regards to liability.
- **Delegation of authentication to digital wallet providers:** These provisions should be aligned with the technical reality of digital wallet services. The outsourcing provisions, especially with regards to digital wallets, appear to be unclear with regards to what type of involvement would account for outsourcing. Differing depictions in the recitals and the text need to be aligned. Also, it should be made clear that it is the duty of the regulated PSPs to assess whether or not an involvement of the digital wallet provider constitutes outsourcing and whether such outsourcing is seen as critical or not by such regulated PSP (in its own diligent assessment).
- **Digital identities as key to resolve SCA:** To become the spearhead of the digital economy – and this most definitely goes beyond financial services – Europe and its member states must intensify their focus on digital identities. **Thus, resolving PSD2/SCA as well as furthering digital identities (eIDAS) is essential to see an uptake and integration of new and existing services.** EBA's latest efforts regarding digital customer onboarding to reduce inner-European fragmentation are

welcomed in this context. Digital identity solutions, such as European Digital Identity Wallets will help identify a customer online and authenticate consent.

To achieve a state of frictionless, intra-European financial services, however, we need solutions that go beyond mere insular onboarding processes for distinct services. Fully fledged digital SSIs (self-sovereign identities) will be key to use and seamlessly combine different services for consumers without media switches and disruptions.

It must be highlighted that digital identities extend beyond consumers. Verifying identities should be streamlined along consumers and corporations as such they also must cater to machines as well for corresponding B2B use cases. Currently the PSD2 is a hinderance towards these innovative business models. The question of identity must also relate to machines given the growing importance of M2M payments.

Enabling viable business models for all market participants

- **Data Sharing:** Overall, there is a need for increasing transparency for consumers in terms of guiding through the process of data sharing as well as managing consent by providing easily understandable and standardized text information. Against this background the exploration of dashboard solutions is highly welcomed. A more detailed explanation can be found in our Position Paper on FIDA.
- **API Quality:** To enhance API quality, Bitkom proposes adopting a market-driven approach in order to establish standardized reporting and Service Level Agreement (SLA) standards. A more detailed explanation can be found in our Position Paper on FIDA.
- **Data sharing business models:** Bitkom call for a debate about questions linked to liability and costs, regarding the provision of data sharing infrastructures, to allow for sustainable business models across the value chain. In the interest of an efficient open data ecosystem in the EU and in line with the EU Strategy for data and the EU Data Act we encourage the Commission to review its approach under PSD2. This would enable the industry to have a constructive basis to take open banking to the next level.
- **Improving the implementation of SEPA:** Bitkom calls for improvements in the implementation of the Single Euro Payments Area (SEPA). Despite significant progress, differences between Member States persist, hampering the efficiency of cross-border payments. We would like to highlight the persistence of IBAN discrimination across industry sectors and Member States which is mainly due to technical limitations of IT systems that do not cater for the multiple formats of IBAN numbers.

For a practicable implementation of real-time transfers within the ecosystem and its market participants, adjustments to PSD2 are also necessary, e.g.: In order to make optimal use of real-time transfers also in the context of Open Banking, PISPs should be informed about the payment status by ASPSPs.

Legal requirements that cater for all payment methods and payment service users

- **Different payment service user groups:** PSD2 is focused on retail payment use cases which typically involve consumers, merchants and small businesses. Use cases in the business-to-business context and payment services for large corporates or global enterprises are not in the focus of the overall objectives of PSD2. These use cases are typically very tailored and do not fit into the pre-defined scope of access to payment accounts. In the past years, FinTechs increasingly partner with corporates and their banks to provide dedicated API-solutions for all types of financial services, i.e., not limited to payments. **The PSD2 revision should therefore clearly define its user groups, including and excluding specific groups:** Corporates not qualifying as small and medium enterprises (SME as per EU Definition 2003/361) should be excluded from the PSD2 requirements and regulation for access to accounts by account information service providers and payment initiation services providers.
- **IBAN Name Checking:** IBAN verification should remain voluntary for corporates. According to our information, the European Payments Council is currently working on a verification scheme which would exclusively focus on IBANs for payee verification. This would not properly account for e-money institutions and payment institutions who work with partner banks to help merchants accept payments. EMIs and PIs typically hold an account with the partner bank and funds are allocated to merchant sub-accounts that may be referenced by identifiers other than IBANs (e.g. PANs, e-mails). In this case, banks and EMIs/PIs would have to be able to register second level data with the verification scheme to match merchants. The PSR currently references the verification of account identifiers which are broader than IBANs and this should be maintained as well as efforts made to ensure any EU verification scheme reflects the identifying information needed to correctly verify beneficiaries. Lastly and importantly, there should be alignment in referencing the account identifier between the PSR and Instant Payments Regulation (IPR) as the verification scheme will ultimately apply to both SEPA Instant and SEPA Regular Credit Transfers.
- **Clarity for ‘Commercial agent exclusion’:** The “commercial agent exclusion” in the proposal of the PSR is important for business models such as gas stations, ticketing, travel agencies, etc. The current draft of the PSR changes the concept of the commercial agent exemption as now the application of the exemption depends upon the counterparty’s leeway to negotiate or to enter into the agreement. EBA will be responsible for formulating respective RTSs yet, however the general logic of the level 1 text should be revisited to actually achieve the desired outcome.
- **“Agents” and ‘E-Money Agents’:** According to the new proposal, there would be a need to report all sub (payment) agents and changes thereof to the NCAs. This would not only exceed the industries’ but also the NCAs’ capacities. Bitkom suggests to not report sub (payment) agents if the overarching agent or e-money agent is already reported and identified (e.g. think of a company with well over 10,000 gas stations).

- **Safeguarding requirements for customers' funds (I):** In some member states the safeguarding requirements pursuant to Art. 10 PSD2 (now Art. 9 PSD3-proposal) have not been transformed such that payment institutions and e-money institutions have been given the full leeway granted by this provision. Some lawmakers have so far not adapted the local insolvency laws in order to transfer each aspect of Art. 10 (1) PSD2 into national law, in particular the t+1 requirement for separate (trust) accounts. In some member states local insolvency law does not permit payment institutions to hold funds of customers separately (in terms of distinguishable in the account ledger from own funds) but in an own account. In consequence this leads to the requirement in such member states to transfer not on t+1 but upon receipt (t0) the customer funds to the separate account. This poses an obstacle for the conduct of business of payment institutions and e-money institutions.
- **Safeguarding requirements for customers' funds (II):** The EU is asked to clarify that customer funds deposited in separate accounts with credit institutions fall into the deposit guarantee schemes as provided by directive 2014/49/EU and into the scope of the national laws transforming this directive, in spite of recital 29 of that directive.
- **Safeguarding requirements for customers' funds by agents (III):** Bitkom recommends clarifying that agents within the meaning of Art. 2 (28) draft PSD3 may be allowed to set up ring-fenced accounts ("separate account" within the meaning of Art. 9 (1) draft PSD3) in their own name and fulfil the safeguarding requirements for customer funds on behalf of the payment institution having engaged this agent. Such separate accounts should be maintained such that in the event of insolvency of the payment institution or the agent, the secured funds will neither fall into the insolvency estate of the payment institution nor the insolvency estate of the agent and neither creditors of the payment institution nor creditors of the agent shall have access to such funds. Insurance or bank guarantees should also be permitted as a means of protecting customer funds by agents on behalf of the payment institution.
- **Specifying the Intragroup Payment Exemption:** Bitkom welcomes that the Commission has apparently followed the German approach defined by BaFin and industry member in its argumentation (recital 15 of PSR). Yet, this clarification is also needed in the text of Article 2 (2) (m) draft PSR; especially, with regards to payments from clients or to suppliers of a group-company via a central payment factory of such group. Ideally, it is clarified that payments can be carried out company-wide (including subsidiaries) via a group-wide service unit. This aligns with the rationale of Recital 17 PSD2, harmonizes with established principles, and allows for the same interpretation as the intra-group exemptions under MiFID II, MICAR and the German Banking Act. The exemption is tied to the recipient of the payment service as the intra-group payment service user, without affecting the interests of third parties in the relevant tripartite relationship. Such a specification will promote operational efficiency and reduce administrative burdens for companies operating within a corporate group.
- **Specifying the telecoms exemption:** From the perspective of telecommunications companies, it is essential that the view expressed in the BaFin's information sheet

to the ZAG on the PSR remains valid even after the PSR enters into force. In view of the fact that the PSR is an EU Regulation, there is a great deal of uncertainty among the member companies concerned. In this respect, we propose the inclusion of a clarifying provision in the PSR, i.e. "per telephone number" instead of "per subscriber" in Art. 2 (2) (k) (ii) of the PSR and that the procedure developed by BaFin for determining the threshold may continue to be applied. Furthermore, we reiterate that the limits of EUR 50 and EUR 300 should be adjusted against the background of the development of the market for digital goods and rising inflation.

Ensure regulatory and supervisory coherence:

- **Avoiding Double Definitions:** In general, Bitkom has identified some overlaps regarding definitions within PSD3 and PSR. Such double definitions can lead to incoherence even if the wording is alike.
- **Clarifying Definitions:** It is unclear whether the e-money definition applies if there is only one acceptant. The definition of payment accounts fails to clarify whether accounts that can only send or only receive money do qualify as payment accounts (e.g. important for credit card accounts).
- **Harmonizing EMD with PSR:** The proposed merger of the EMD and PSD was expected and is generally welcomed by Bitkom. As laid out in the current proposals, EMIs need to enter an "reauthorization process" with respective NCAs. Article 44 (2) states that companies operating under the current EMI may be eligible to "be authorized automatically [...] if the competent authorities have evidence that those payment institutions already comply [...]." This is a reasonable approach to reduce red tape and avoid frictions. Yet, the process need to be clarified to ensure an EU-wide regime for automated authorization. Otherwise, market fragmentations will decrease competition and the offered set of services within the EU.
- **Aligning PSD2 and GDPR:** As it has been stated by Bitkom before: GDPR in its general essence is one of Europe's biggest achievements. Its importance for economy and society, especially in the digital environment, cannot be overstated. In fact, we have seen international companies implementing the standard globally, which is why GDPR can be regarded as a prime example of setting international standards. **Yet, the interplay between PSD2 and GDPR continues to challenge the industry.** For the provision of payment services personal data is needed to ensure secure payments and hamper fraudulent activities, but GDPR put into practice has led to increased legal uncertainty. To underpin this assessment: In Germany alone, we see unnecessary fragmentation among the 16 federal states and their differing interpretations of GDPR. This lack of clarity is further intensified by different interpretations of data protection offices in the individual Member States.

An aligned approach and common supervisory practices of the NCAs responsible for PSD2 and data protection across the 27 Member States is required. This should be further underlined by a mechanism that clarifies that GDPR does not counter the very ideas of PSD2. That said, Bitkom has no interest in weakening GDPR or its goals. In fact, PSD2 has strengthened the consumers' rights concerning their own data, granting them the right to decide themselves which entities they want to share

data with. Still, in actual business use cases there is conflicting potential between PSD2 and GDPR which should be clarified to the benefit for both the consumers as well as service providers. Bitkom recommends for the exclusive provision of data protection roles only in the GDPR, not in a revised PSD.

- **BNPL & Overlaps with CCD:** according to the PSD3 proposal, the leeway for payment institutions to grant credit in the context of payment services has been further limited. No efforts have been made to clarify what constitutes a credit within the meaning of the PSD. Instead, the proposal of PSD3 states that BNPL products shall no longer be considered as payment services but shall fall under the Consumer Credit Directive (CCD). Given the fact that BNPL products come in different way, shape or form, such a “CCD-only” approach appears to be invalid. Thinking of B2B (i.e. non-consumer) BNPL solutions underpins this argument.
- **Aligning MiCA with PSD2:** On MiCA an alignment to include payment transactions using crypto assets as defined in MiCA, including Stablecoins, is desirable. In particular for transactions in e-money token, which constitute e-money within the meaning of PSR and PSD3, the provisions in Art. 49 through 79 PSR should be adapted in order to cater for machine to machine payments and other transactions using crypto currencies and PSR should provide sufficient and viable exemptions from SCA for such transactions.
- **The issuance of electronic licenses and alignment with eIDAS:** We propose a different system for the issuance of electronic certificates and licensing. Currently, NCA licensing and authorization processes are not directly linked to the issuance of electronic certificates. This is problematic as TPPs require an electronic certificate to identify when accessing payment accounts through ASPSP interfaces. These electronic certificates are issued by trust centers regulated under the eIDAS Regulation as “trust service” or “qualified trust service”. To obtain such certificates, the TPP has to prove to be authorized or licensed by an NCA. Hence both processes should be closely linked. We propose that: TPPs should provide their electronic certificate ID and the details of the issuing trust service to the NCA, which in turn should directly interact with the trust center and immediately provide updates and changes to an authorization or license. **In this regard Bitkom would also like to highlight the need to improve digital processes for the license applications.**