German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

on the European Commission's legislative proposals of 28 June 2023 to revise the Second Payment Services Directive

Lobby Register No R001459
EU Transparency Register No 52646912360-95

Contact:

Axel Schindler
Senior Advisor,
Payments Systems Department
Telephone: +49 30 2021-1813
E-mail: a.schindler@bvr.de

Dr. Alexander Scheike
Attorney at law
Legal Department
Telephone: +49 30 2021-2321
E-mail: a.scheike@bvr.de

Berlin, 25 October 2023

The **German Banking Industry Committee** is the joint committee operated by the central associations of the German banking industry. These associations are the Bundesverband der Deutschen Volksbanken und Raiffeisenbanken (BVR), for the cooperative banks, the Bundesverband deutscher Banken (BdB), for the private commercial banks, the Bundesverband Öffentlicher Banken Deutschlands (VÖB), for the public-sector banks, the Deutscher Sparkassen- und Giroverband (DSGV), for the savings banks finance group, and the Verband deutscher Pfandbriefbanken (vdp), for the Pfandbrief banks.

Coordinator:
National Association of German Cooperative Banks
Schellingstraße 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-1900
www.die-deutsche-kreditwirtschaft.de

Preliminary remark

On 28 June 2023, the European Commission presented its legislative proposals for the revision of the Second Payment Services Directive (PSD2) together with the planned "Framework for Financial Data Access (FIDA)", namely the drafts of a third Payment Services Directive (PSD3) and a new EU Payment Services Regulation (PSR). In the following, the German Banking Industry Committee presents its assessment to date of what it considers to be the most important points in these legislative proposals. A more detailed assessment as well as additional detailed amendments, also on other topics, if applicable, will be successively introduced in the further course of the legislative process.

Extensive changes of payment services law lead to high complexity and potentially unintended adverse effects

In line with the objectives pursued with the First Payment Services Directive (PSD1), it is now important for the further development of payment services law to further develop the existing legal framework for payment services in line with the needs of consumers, companies and payment service providers, while not losing sight of the objective of stability and continuity. A renewed unilateral or further increased **regulatory burden** on banks and savings banks in favor of individual business models or market participants does not take into account the idea of competition, the creation of European sovereignty in payment transactions or a balanced distribution of risk.

Contrary to the EU Commission's announcement that its regulatory proposals only aim to further develop payment services law (**"no revolution / rather evolution"**), the banking industry's initial assessment is that there are surprisingly many changes in detail in relation to the previous regulatory texts. All in all, these changes lead to a high degree of complexity and potentially unintentional adverse effects. Examples include significant changes in the definitions in Article 2 PSD and Article 3 PSR and important provisions on payment execution and liability in Article 49 et seqq. PSR. For example, the definition of "execution of a payment transaction" in Art. 3 (8) PSR does not take into account the previous separation of the duties of the payers' bank and the payees' bank (cf. in particular Article 69 PSR). In Article 55 PSR, the term "authentication" is exchanged with "authorisation", which can lead to a significant change in the evidence situation for the payment service provider. Consequently, the planned changes must be subjected to a comprehensive and detailed assessment.

At the same time, it is regrettable that the European Commission has not taken into account what is actually a necessary, improved **differentiation between offers for consumers and non-consumers**. This aspect must also be considered in the further course of the legislative process. However, we welcome the fact that the legislative proposals hardly open up any significant new regulatory areas and thus provide a certain degree of stability for business policy decisions.

Consider the consequences of the change from directive to regulation and the splitting into two legal acts

According to the EU Commission's ideas, the provisions of PSD2 are to be fanned out into two distinct legal acts, namely PSD3 with primarily supervisory requirements and PSR with the essential civil law requirements. As the definitions in Article 2 PSD3 and Article 3 PSR make clear, this leads in part to unnecessary duplication and questions of demarcation.

Especially the change from a directive to a regulation must be carefully considered regarding the civil law provisions. Since the implementation of PSD1 more than 15 years ago, Germany has a civil law on payment services (as part of the transposition of PSD and PSD2) that is well integrated into the German Civil Code (Bürgerliches Gesetzbuch – BGB), which builds on the law on contracts and the law on the provision of services as well as other principles of civil law (e. g. on liability in section 280 BGB). Based on this, there is now a mature body of legal literature and a large number of supreme court rulings. For reasons of **legal certainty**, the change to the EU regulation and the resulting extensive deletion of the provisions in sections 675c et seqq. BGB must not be allowed to render legal literature and case law obsolete with a stroke of the pen. Therefore, the current legal basis in the form of a EU directive covering all scope areas comprehensively and conclusively should be retained. In addition, it is also questionable whether the objective of EU-wide harmonization of the law intended by the EU Commission could be significantly achieved by means of a regulation: This is particularly true in light of the fact that the proposed regulation continues to allow a large number of national deviations in various regulatory areas. Similarly, in light of the proposed change of legal instrument, it does not seem plausible that a high number of delegated acts is nevertheless envisaged: After all, experience from PSD2 has shown that it can lead to further fragmentation in terms of time and geography during implementation and increase planning uncertainty.

From the point of view of the German banking industry, changes should only be made where there is a justified need for adjustment. Otherwise, payment services law should remain unchanged in order to ensure legal certainty, stability and continuity, to limit the adjustment

effort for payment service providers such as banks and savings banks and their users (customers) to what is strictly necessary, and to preserve the functionality of the established payment services offering - especially in retail payments (Single Euro Payments Area, SEPA). This is the only way to provide the market with the necessary regulatory and innovation-promoting stability.

Stability in the technical specifications for the use of third-party services only partially given

It is to be welcomed that access to customers' payment accounts by means of third-party service providers will in future only be possible via the technical infrastructures and **dedicated interfaces (APIs)** created by the banking industry and that the requirement for a so-called "fallback interface" is to be dropped (Article 35 (1) PSR). This increases transparency and security for the consumer as well. In this context, the orientation towards international industry standards, as already implemented today by the German banking industry with the Berlin Group interface, is particularly welcome. Nevertheless, this is counteracted by the requirements for alternative interfaces in the event of a failure of the dedicated interface pursuant to Article 38 (2) PSR. Moreover, this is not appropriate against the background of the associated potential double investments.

For banks and savings banks, protecting their customers and the customers data is a top priority. To this end, the further use and expansion of overviews of which authorizations have been granted (**"dashboards"**) can lead to better transparency for the increasingly complex payment services ecosystem (Article 43 PSR). Many German credit institutions already offer such an overview.

However, the expansion of the **offerings to be supported free of charge** vis-à-vis third-party services is viewed very critically. This means that legislation once again interferes with the freedom of credit institutions to design their products without there being any need for this. This is because the free offers reduce the motivation to optimize the offers of the credit institutions and at the same time hinder their ability to innovate. Under no circumstances should services be required for retail customers which they do not need or which are not yet offered today and which in turn may result in additional risks for customers and banks, such as "multiple beneficiaries" or the requirements for direct debits (Article 36 (4) PSR). Last but not least, such an extension would make the development of and participation in market-based procedures less attractive. This contradicts the declared goals of the legislator.

Improve fraud prevention without creating disincentives to the detriment of customers and the banking industry

The EU Commission intends to introduce additional instruments to counter certain fraud scenarios in connection with payment transactions in order to protect consumers. Against the backdrop of the growing importance of digital services and the need for trust in their security, this is to be welcomed in principle. However, it is important to bring the instruments into a reasonable balance and to find a coherent approach. In particular, considerations of more far-reaching requirements in terms of liability and reimbursement rights that go beyond the actual processing of payments require careful balancing. Otherwise, disincentives could be created that effectively lead to an increase in fraud instead of curbing it.

From the perspective of the German banking industry, special attention must be paid to the following aspects:

Liability law, in particular Article 56 (2) as well as Article 59 PSR:

- The PSD2 already contains a balanced liability regime that comprehensively protects the payer in the event of unauthorised payments (cf. now Article 56 PSR-E). On the other hand, the proposals for more far-reaching provisions with regard to liability that go beyond the general processing of payments, such as the liability of the payer bank for payments authorised due to fraudulent manipulation of the payer ("social engineering") according to Article 59 PSR-E, are unbalanced. This is because a risk that lies solely in the sphere of the customer/payer is shifted to his credit institution and thus to all other customers of this institution ("socialization" of fraud losses).
- For banks and savings banks, customer protection has always been a major concern. The corresponding systems are therefore regularly adapted to the current framework conditions, and the education and information of customers in this context is already very extensive.
- By contrast, extending liability for authorized payments through "social engineering" (Article 59 PSR) would burden credit institutions with **further risks outside their own sphere of responsibility** and create false incentives for clients to be less diligent, as they then have the impression that the credit institution is always liable ("full coverage mentality"). This is also extremely problematic in view of the envisaged distribution of the burden of proof. It is unclear how this would effectively prevent fraud: On the contrary, there is a risk that fraudsters will exploit these provisions and that the related losses - to the detriment of the banking industry and its customers - could increase and also exacerbate other risks, for example in the area of money laundering.

- The supplementary proposal to include other affected actors (telecommunications companies, see Article 59 (5) PSR) in order to prevent "spoofing" (concealment of caller data) is welcome in principle. However, it remains completely unclear how this can be implemented in practice. The concrete obligations of telecommunications companies to cooperate with payment service providers must be defined by law.
- If the legislator were to retain the problematic Article 59 PSR, it would be essential to consider the following points, among others:
    - The payer bank would have to be granted the right in Article 65 PSR to either not execute payment orders at all if there is suspicion of fraudulent manipulation of the payer or to execute them only after a thorough check (e. g. by consulting the payer). If the payer bank has information that the payee account indicated by the payer has already been misused for fraudulent purposes, the payer bank must have the right - as in the case of sanctions and gambling law - to reject all payment orders in favour of fraudulently used accounts.
    - Credit institutions cannot bear unlimited liability risks outside their sphere, especially since these are not insurable. Therefore, the reimbursement claim under Article 59 PSR must be limited by a cap.
    - If the customer is comprehensively informed by his credit institution according to Article 84 PSR about precautionary measures to prevent fraud, the customer must also be contractually measured against this. If he violates his contractual duty of care, this should be able to be classified as gross negligence in Article 59 PSR.
    - Also, the de facto reduction of the review time and processing time of unauthorized payments in case of a reasonable suspicion of fraud against the payer himself to 10 days (Article 56 (2) PSR) does not meet the challenges in practice, such as the necessary determination of the actual factual situation by the payment service provider.

"IBAN name matching" of the payee, in particular Articles 50, 57 PSR:

- Full consistency in terms of functionality and liability rules with the parallel requirements for instant credit transfers (amended SEPA Regulation) is mandatory.
- The interaction with the other proposed anti-fraud regulations should be clarified by law: For example, it would be desirable that discrepancies resulting from reconciliation can be used for data exchange between payment service providers under Article 83 PSR. The payer’s bank should also be enabled to use the findings from the "IBAN name comparison" for its own fraud prevention mechanisms. If it turns out that certain IBANs are likely being used by payees for fraudulent purposes, the payers bank should be

granted the right in Article 65 PSR to reject further payment transactions in favour of such a "fraud IBAN" altogether.
- Likewise, it should be clarified that due diligence obligations for payment service users may arise from the offering of the matching service, which may have an impact on liability rules (in particular Article 59 PSR).
- The liability in Article 57 PSR, which also includes consequential damages, should be able to be designed and limited by the national legislator in analogy to the provisions in Article 56(6) PSR. Whether a credit institution should be liable for any consequential damages is a question of attribution. A credit institution would only be able to assess this question if it were to inquire about the "loss potential" of each credit transfer. However, this is not possible in the mass business of payment transactions. The credit institutions would therefore have to insure themselves against such risks, which would increase costs and ultimately be to the disadvantage of the customer. This disadvantage can only be avoided by the possibility of limiting liability for consequential damages, as has been codified in German payment services law for over 15 years (cf. section 675 z BGB).

"Fraud Data Sharing" (Article 83 PSR):

- An effective and legally secure possibility to communicate possible fraud cases between payment service providers is welcome. However, it is questionable whether the concrete regulatory proposal is already fully developed with regard to the following two aspects and leads to meaningful results. This must be examined and sharpened in the further course of the legislative process.
- The requirements must ensure adequate protection of customers' personal data and at the same time enable efficient EU-wide implementation. Possible differences in national views and consultation requirements at the level of the member states could jeopardise this goal. This argues in favour of linking the requirements for data protection impact assessment to the operator of the multilateral "platform" solutions. In addition, it must be taken into account that a corresponding exchange of information can take place not only through the multilateral "platform" solutions addressed in the proposed regulation, but also bilaterally between payment service providers.
- It must be made clear that the given requirements for data protection impact assessment must not make this more difficult and can thus only apply to multilateral platform solutions.
- In addition, the options for action for banks that can result from the exchange of information should be evaluated and, if necessary, concretised. One example of this is that in practice fraudulent payments are often quickly "forwarded" or otherwise disposed of.

- The requirements for transaction monitoring and information exchange do not ultimately take into account that, due to the mechanisms used and/or the exchange of information, the legal possibility of a delay or rejection of the transaction execution without a breach of duty must exist on the part of both the institution commissioned with the payment and the receiving institution. In this respect, an adequate regulation for the implementation of the regulatory purpose is missing here, namely the possible prevention of the occurrence of damage in cases of suspected fraud by the taking of suitable additional measures on the part of the credit institutions. In concrete terms, this means that there is a need for a legally secure possibility to reject payment orders and "block" payments received in cases of suspected fraud in order to be able to counteract fraud. Article 56 PSR must therefore be supplemented by the reason for rejection on suspicion of fraud, namely the payers bank should be entitled to reject the payment order of the payer on suspicion of fraud. The blocking of credit in the case of suspected fraud should be anchored in Article 69 (2) and Article 73 PSR.

Education of customers and employees (Article 84 PSR):

- Raising awareness of fraud risks is an important tool and is already widely provided by payment service providers.
- The proposals of the EU Commission are to be welcomed. Nevertheless, they must also be placed **in relation to the other proposals on fraud prevention** (in particular the liability rules and associated customer due diligence requirements). This is because the information and warnings given to the customer co-determine his contractual duties of care. In the event of damage, the client must be judged on whether he has complied with his contractual duties of care.

Proposed changes to strong customer authentication do not meet market needs

It is welcomed that the European Commission recognizes the success achieved in combating fraud with the use of strong customer authentication. However, the proposed changes require critical evaluation:

- A combination of the same authentication categories (Article 85 (12) PSR) negatively affects the security level and the previous customer communication. The exceptions to the previous requirements must be regulated in a future RTS, taking into account the potential risks.
- We support the aim of inclusion underlying Article 88 PSR. However, the smartphone has high customer convenience, offers high security and is particularly suitable for

meeting the requirements of the Accessibility Directive. Only a small proportion of customers who use online banking do not have a smartphone or do not wish to use one for authentication. If the PSR mandates the provision of alternative methods, i.e. non-smartphone-based, market-based pricing must still be possible.

- The shift of the customer's consent to access account data away from the account-holding payment service provider to the third-party service provider by means of its SCA (Article 86 (4) PSR) has the effect that the customer can no longer obtain clear rules for the SCA from the account-holding institution. The liability issues for this also remain open. Credit institutions should continue to have the possibility to verify the customer's will on a regular basis. Although the future dashboard is a useful addition, it is not seen as sufficient because it is the customer alone who must take action here. If account information service provider (AISP) conduct their own SCA, the same obligations and requirements regarding SCA procedures as for account-holding institutions must apply to AISs for consumer protection reasons. The procedures must be regularly reviewed by the regulator.
- The PSD3/PSR still does not make a clear distinction between consumers and non-consumers. The provisions of PSD2 are based on the need for protection and the technical designs in the retail customer sector. Communication protocols commonly used in the corporate customer sector and forward-looking developments, for example in the context of DLT-based business processes and machine-to-machine payments (M2M), cannot always be reconciled with this. This innovation-inhibiting effect of regulation must be countered by better differentiation: The corporate customer sector should be exempted from the rigid requirements for strong customer authentication.

Usage of customers' own ”off-the-shelf”-devices in the context of strong customer authentication is not a case of outsourcing

The wording of Article 87 PSR is misleading because it could lead to the inaccurate conclusion that the customer's own terminal device (e. g. smartphone) used in the context of strong customer authentication could also constitute an outsourcing offence for which the credit institution is responsible. It is already questionable whether the banking supervisory construct of outsourcing control would offer any effective added value at all against the background of already existing security-related possibilities. At the same time, there is a danger that significant restrictions could arise for equipment manufacturers, banks and their customers.

An "outsourcing" situation should therefore only exist if - as is common today - the bank selects the service provider itself. This is not the case if an end customer decides to use a

customer device from a certain manufacturer. The use of a customer device cannot be regarded as a service provided by a technical service provider on behalf of the credit institution.

Should the requirement for "outsourcing agreements" apply to all infrastructure used for offerings regulated by the PSD3/PSR, the existing offering will be significantly restricted, especially in the case of customer premises equipment. This has an impact in particular on customer devices, which are generally used by customers for online banking, whether as a customer terminal or as a security medium with corresponding apps (so-called commercial-of-the-shelf - (COTS) devices).

In fact, it is to be expected that the credit institution

a) cannot reach all manufacturers/providers at all (for example because of language barriers, different legal understandings in the countries of the providers or a lack of willingness to communicate on the part of foreign manufacturers) and
b) that the manufacturers/providers have no interest in contractual agreements with a (German) credit institution, which they are not obliged to do.

For these reasons, it is likely that contractual agreements cannot be reached with all third parties that come into consideration, so that the credit institutions would have to actively restrict the use of the hardware and software of these providers that are possible at the customers' premises - if the obligation were established by PSR.

For example, the support of Apple/Google Pay and the use of financial software products on the customer's own PC/tablet/smartphone would then no longer be possible if the bank does not have an outsourcing agreement with the corresponding technical manufacturers/providers.

Regulations on third-country payments not to be extended due to lack of influence

Due to the fact that the EU payment services legislation is limited to the EU Member States, provisions for payments involving third countries are currently the exception. An extension of the information obligations of payment service providers regarding execution times and currency conversions for credit transfers to third countries, as foreseen by the EU Commission, is not appropriate (Articles 13 and 20 PSR). **Due to the lack of global effect of EU payment services legislation**, a payment service provider cannot provide information on certain

aspects that are outside its controllable sphere of influence. Likewise, this additional information would lead to possible confusion among customers and overload currently appropriate customer information in this field.

Making access to cash more flexible is the right way forward

Complementary services, where cash is provided in retail shop without the purchase of goods or services, are generally sensible as this puts the possibilities of accessing cash on a broader basis and complements current possibilities (Article 37 PSD3). The principles of a given level playing field must be generally observed.

Maintain risk-adequate access arrangements to payment systems

The Settlement Finality Directive (SFD) was intended to expand the range of participants in payment systems (Article 46 PSD3) in order to **maintain a fair competitive environment** (level playing field) **and to prevent systemic risks by providing adequate specifications for the system operators**. One such "SFD payment system" is the TARGET system of the Eurosystem. So far, only credit institutions are allowed to participate directly in this system. Payment institutions have so far only been able to participate indirectly, e. g. by means of a mandated credit institution. The different supervisory requirements for credit institutions and payment institutions beyond the scope of payment services legislation can nevertheless result in different risk profiles with corresponding effects on payment systems and their participants. Payment system operators must be given the opportunity to compensate for this through supplementary participation requirements or restrictions.

Realistic implementation deadlines required

With regard to the requirements for the planned implementation periods (Article 112 PSR), the German banking industry believes that **appropriate implementation periods** are fundamentally necessary. These should be based on the experiences gained from the implementation of PSD2 and should therefore generally be at least 24 months instead of 18 months. Supplementary implementations with comprehensive IT related effects, such as the proposed requirements under Articles 50 and 57 PSR, require an implementation period of at least 36 months in our opinion.

Moreover, the experiences from the implementation of PSD2 have shown that early planning certainty is also necessary, especially for the implementation of so-called "Level 2 regulations". If corresponding standards or supplementary delegated acts (e. g. RTS) are necessary, the corresponding implementation deadlines must be linked to the publication of the corresponding RTS standards. **Divergent implementation deadlines** for regulatory areas that involve dependencies with regard to their technical or customer-contractual implementation **must be avoided** in order to enable efficient implementation for the benefit of the institutions and their customers. This applies in particular to the areas of fraud prevention, strong customer authentication and access to payment accounts by third-party services and, above all, to those topics that also require changes to the contractual terms and conditions in the customer relationship.

Anticipate perspective relationship between payment law and FIDA

In addition to the revision of the legal framework for payment services, the European Commission has proposed a "Framework for Financial Data Access (FIDA)". Compared with the existing requirements for the use of data from payment accounts under PSD2, more market-oriented rules are to apply under FIDA. Under FIDA, for example, it is to be possible to charge financial information service providers for the provision of data. With the amendment of the legal framework for payment services, a way must be shown how this can be transferred to the specifications for interaction with third-party services in payment transactions. Finally, an appropriate legal framework for the use of financial services data offers long-term benefits for the entire payment ecosystem.