German Banking Industry Committee

Die Deutsche Kreditwirtschaft

Comments

on the draft Directive of the European Parliament and the Council on payment services in the internal market (PSD 2) in relation to third party payment providers (TPPs)

Contact:
Matthias Hönisch
Telephone: +49/30/2021-1810
Email: m.hoenisch@bvr.de

Berlin, 14 November 2014

Coordinator:
National Association of German Cooperative Banks
Schellingstrasse 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-191900

The **German Banking Industry Committee** is the joint committee comprised of 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. Collectively, they represent more than 2,000 banks.

Pending the start of trialogue negotiations on the draft Directive of the European Parliament and the Council on payment services in the internal market (PSD2), the German Banking Industry Committee (GBIC) would like to share its assessment of the proposed rules relating to third party payment providers.

1. Background to the Commission proposal on third party payment providers (TPPs)

Security is key to a well functioning payment system. Today, multiple technical measures as well as a clear, contractual allocation of responsibilities between the various actors guarantee a high level of security of payment systems. This allows banks and other payment service providers to offer a broad range of reliable and cost-efficient payment products, whilst ensuring a low number of fraud cases.

According to the Commission's proposal for a PSD2, banks should in future be obliged to make their customer-bank interface accessible to third parties. Customers would share their personalised security credentials (PIN and/or TAN) with third parties to enable payment initiation services and provide third parties with the right to access their bank accounts. Banks incur liability for any damage caused by third parties during this process. This proposal is unacceptable for the following reasons:

- Following years of campaigning and awareness raising by banks and public authorities, customers know today that they are not allowed to share their PIN and/or TAN with anyone. The PSD2 in its current form makes this principle null and void. It breaks through customers' mental barrier of keeping bank credentials confidential. This is highly worrying, in particular as customers - due to the professionalism of criminals - will have difficulties to differentiate between licensed TPPs and criminal organisations. **Consequently, the Commission's proposed approach increases the reputational risk for all online and mobile banking services with customers ultimately loosing trust in the digital economy.** For this reason, the European Central Bank as well as various Member States have rejected the proposal of sharing any personalised security credentials with third parties.

➔ **EU policymakers have to ensure that innovation does not come at the cost of the protection of customers' data, privacy and the security of payment systems.**

Coordinator:
National Association of German Cooperative Banks
Schellingstrasse 4 | 10785 Berlin | Germany
Telephone: +49 30 2021-0
Telefax: +49 30 2021-191900

- The Commission's proposal does not respect fundamental legal principles governing liability rules of the EU Member States. Banks have absolutely no control over third parties and the way they provide their services. Nonetheless, **banks will be made liable for any wrongdoing of a third party payment provider**. This is inappropriate and poses uncontrollable risks to banks.

- Companies which have to make their infrastructure, deemed as "essential", accessible to competitors - this practice is widely known, for instance, in the telecommunications and the railway sectors - have a right to request a remuneration for the service of providing other parties with access to their infrastructure. **It is unacceptable that banks should allow third parties to use their infrastructure and data for free.** The TPP on the other hand charges for the provision of its service.

2. Request by the German Banking Industry Committee: no sharing of personalised security credentials

The level 1 text of the **PSD2 should explicitly state that the sharing of any personalised security credentials is forbidden**.

In contrast to proposals made by e.g., the Council, **the sharing of "only" non-reuseable credentials does not solve the security issue** because even the sharing of e.g., the TAN can provide access to numerous personal information over the one-time account access (snapshot). All transactions of the last three months are visible, including debits and savings. On that basis, further abuses are possible, i.e., the ordering of SEPA direct debits or physical attacks such as extortion or burglary. Whenever credentials are shared, **strong customer authentication and strong transaction authentication are further insufficient.** Once the TPP has access to a client's account, the TPP places the payment order without (as per current market practice) the client seeing the final order. This paves the way for fraudulent behaviour. Additionally, most fraud cases do not happen due to a weak Two-Factor-Authentication but due to fraud driven by social engineering: when offered the payment initiation service, the vast majority of customers is highly unlikely to verify whether a TPP is licensed and supervised.

If the high level principle of prohibiting the sharing of credentials is not included in the PSD2, customers' data, their privacy and the security of payment systems are put at considerable risk. Sharing of credentials would further make it extremely complex and difficult to allocate the responsibility in case of e.g., an unwanted transaction. To ensure that customers' data are protected, **the same principle should apply to account information/ aggregation service providers.**

3. Workable alternatives to the sharing of credentials

The sharing of customers' credentials is not the only way that would allow TPPs' to continue their services. In line with the opinion of the European Central Bank from 5 February 2014[1], the client of the payment initiation service provider could be **re-directed to his/her bank's website to insert his/her**

[1] Opinion of the European Central Bank of 5 February 2014 on a proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC (CON/2014/9): https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2014_09_f_sign.pdf

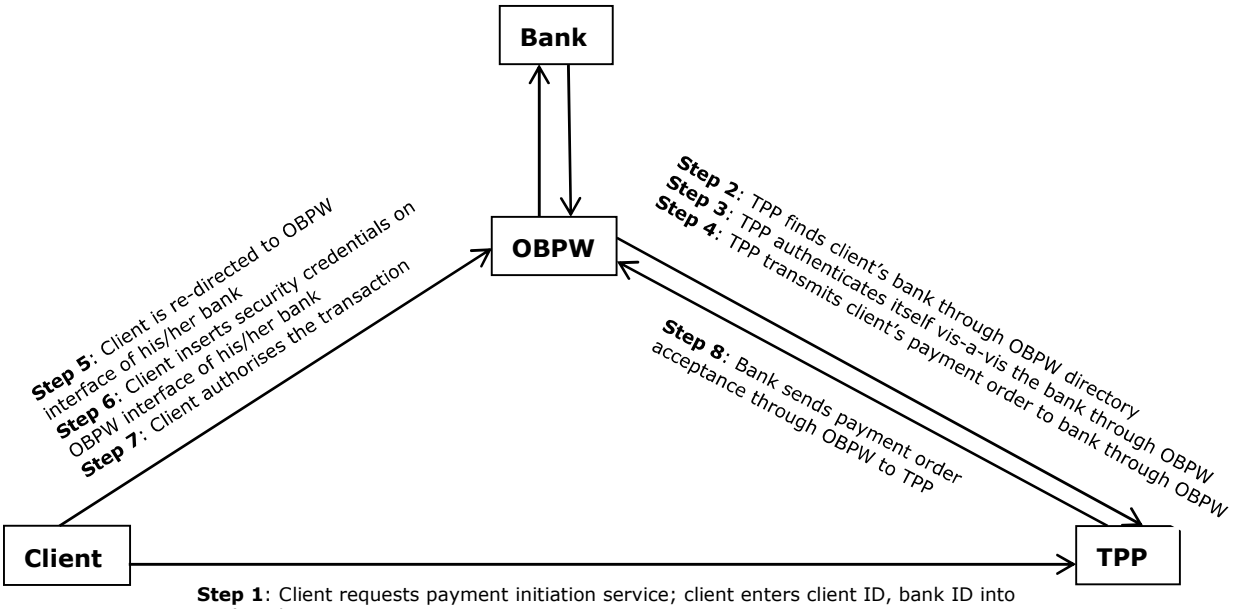
credentials for authentication and authorisation purposes. Credentials would in this way only be shared between the customer and the bank. The GBIC has developed a concept, i.e., the Online Banking Payment Website[2]. This concept is already used in practice and is based on the online banking user interface which enables the direct communication between the bank and the customer. Authorised TPPs are given access to the interface of the participating banks so that they can render their services.

Alternatively, **TPPs could issue their own credentials** to their customers and communicate with the bank via a secured mechanism which could be defined by the European Banking Authority and/or the European Central Bank during the implementation phase of the PSD2.

Hence, **the prohibition of sharing credentials does in no way hinder TPPs' business model.**

ANNEX

Redirect model according to the proposal by the GBIC for an Online Banking Payment Website (OBPW)



Step 1: Client requests payment initiation service; client enters client ID, bank ID into TPP's website
Step 9: TPP confirms payment initiation

[2] See enclosed proposal by the GBIC for an Online Banking Payment Website.