SwissBanking

SBA position paper | September 2017

Payment Services Directive (PSD2)

With its second Payment Services Directive (PSD2), the EU is reconfiguring the ground rules for banking and in particular for payment services. Among other things, the banks in the EU will be obliged to grant third parties (so-called third party payment service providers, TPPs) access to bank accounts. Should screen scraping be accepted, these providers would de facto be handed a blank check and could execute payments directly from the customer account or obtain account information in the name of the client. Should screen scraping not be permitted, the type and method of access will depend to a high degree on the implementation and configuration of the bank's interface.

The EU's PSD2 rules do not apply for Switzerland. Nevertheless, discussions are also taking place in Switzerland about whether a PSD2-equivalent regulation should be introduced. In Switzerland, the banks already grant third party providers access to accounts and open the customer interface if this is in the mutual interest of the bank and the customer. There is, however, no legal obligation for the banks to do so. Switzerland is therefore pursuing market-based solutions.

The Swiss Bankers Association (SBA) rejects the introduction of regulation analogous to PSD2 or a legally imposed opening of access rights to third parties for the following reasons:

- In Switzerland, regulation analogous to PSD2 is **unnecessary** because there is no action required in this area, competition is functioning effectively and the banks already (irrespective of PSD2) offer a large number of innovative solutions. A regulatory obligation to open interfaces would be an unnecessary intervention in what is a functioning market and would result in competitive distortion to the disadvantage of the banks.
- The issue of **customer data security** plays a key role in electronic banking. The highest level of security can only be guaranteed if customers and banks cooperate. A forced opening by the state is dangerous because bank-specific security principles are not fully addressed and this creates security gaps.
- **Additional efforts and costs** would arise for financial institutions in the areas of security infrastructure and compliance, which in the end would have to be paid for by the customer.

A one-sided opening of access rights for third parties as required within the EU under PSD2 is an **experiment at the expense of bank customers that creates dangerous confusion and undermines the customer's data security.**

What is PSD2?

PSD2 aims to create a uniform legal framework for electronic and mobile payment initiation service providers and account information service providers that is to be implemented by the EU member states at the beginning of 2018. PSD2 provides for the opening of secure payment services to TPPs. Non-banking providers will receive access to sensitive customer data. To this end, the banks must provide these third party providers with interfaces that give free access to customer data. Under PSD2, new payment service providers are considered so-called payment initiation service providers (PISPs) on the one hand, and on the other hand, so-called account information service providers (AISPs). Even in the EU, however, there remain many unresolved matters relating to PSD2 such as the technical specifications of the interfaces, assessments of the ensuing costs or how security-related concerns can be properly taken into account.

The devil is in the details

In the winter of 2017, the European Banking Authority (EBA) submitted the final draft of the Regulatory Technical Standards (RTS), in which it formulated technical standards for strong customer authentication. According to this draft, access for the new service providers will only be permitted by means of a separate interface (with an additional emergency interface). Screen scraping[1], which is the collection of data using the customer's interface, is no longer to be permitted. The beneficiary and the payment amount are now also to be linked to authentication. At the end of May 2017, however, the European Commission requested that the EBA once again examine the admissibility of screen scraping. There continue to be a number of unresolved questions in the EU arising from the work being conducted on implementation. The technical specifications (EBA standards) will come into force in May 2019 at the earliest. This results in a gap between PSD2 and the EBA standards.

An economic experiment at the expense of security and data protection

Customers are entitled to a high level of security in electronic and mobile banking. A forced opening of interfaces by the government, however, holds great risks in terms of security. For example, the question arises as to whether the payment initiation service providers should receive full access to electronic bank accounts. If so, this would mean that these service providers would also have access to all the bank and securities accounts tied to the customer relationship. This would be akin to handing over a blank cheque together with all of the customer's account statements. The third party provider would have information about all the assets held, as well as access to the entire spectrum of incoming and outgoing payments such as rent and salary, insurance and health insurance payments, and mobile phone providers. In addition, it would become increasingly difficult for customers to understand what is happening with their data, where it is being saved and what their rights are. The consequences of the forced opening of bank accounts are difficult for customers to gauge.

Target missed

PSD2 will not first and foremost be helpful to European, never mind Swiss startups. Instead, it will play into the hands of the global tech giants. They can aggregate customer data on their widespread platforms. This means that PSD2 misses its target. The Swiss tradition of voluntary in-

[1] Screen scraping is the term for a technology used to take information from websites through direct extraction of the relevant and desired data.

vestments in the future represent an alternative approach: the Swiss banks are investing in fintech solutions and to this end work closely together with startups and service providers of all kinds. The Swiss banks are therefore – irrespective of PSD2 – working on developing possible applications themselves, or with partners and fintech companies, in order to increase customer value through innovative solutions.

Market-based solutions in Switzerland even without PSD2

- Banks can already open their customer interfaces if it is in the interests of the bank and the customer.
- Switzerland is not obliged to implement PSD2 (directly or indirectly) as it is neither a member of the EU, nor of the EEA, and there is also no corresponding commitment in the bilateral agreements with the EU.
- Swiss banks already offer a large number of innovative payment and wealth management solutions without any regulatory obligation to do so. Examples thereof include:
  - Using e-banking, the **e-invoice** function allows for pre-entered invoices to be reviewed and paid electronically. E-invoices are very secure because the invoice issuer is authenticated by the bank, which is not the case for paper invoices.
  - Starting in 2019, **payment slips** will feature a **QR code** containing all payment information. This is an innovation that builds an ideal bridge between the old, paper-based world and the new digital world.
  - There are a number of examples in the market of successful partnerships focussed on secure, standardised interfaces. For example the automatic exchange of information between e-banking and accounting programmes.
  - Payment app **TWINT**: already gives the customer the possibility to make P2P, e-commerce and POS payments securely and comfortably, directly from their accounts.