PSD2 – The Rough "Diamond" of EU

PSD2 is often mentioned in relation to innovation, open banking, improved customer experience and so forth. But what does it really offer and is it truly a wildcard to the payment services of the banks?

This article aims to highlight some of the challenges that banks and 'third party providers' face, when implementing PSD2 and the objective of bringing improved payment products to the customers. And is it possible for both banks, 'third party providers' and customers to benefit from PSD2?

The bar is high

In January 2018, PSD2[1] (EU) 2015/2366 (the revised payment service directive), came into force and is implemented locally in the different member states.

The objective with PSD2 is to enhance competition, facilitate innovation, protect consumers, increase security and contribute to a single EU market in retail payments (EBA Opinion on SCA and CSC). This is partly aimed to be achieved by opening up the banks' payment services to authorized 'third party providers' (TPP).

The 14th of September 2019 the RTS (regulatory technical standards), describing *how* to develop a PSD2 compliant TPP access interface, will come into force. The RTS presents technical standards for strong customer authentication (SCA) and common and secure open standards of communication (CSC).

The EBA has after the publication of the RTS in March 2018, published a range of opinions and consultation papers specifying the different articles in the RTS. Though the specifications remain open to various interpretations. Therefore, you see a range of different payments interoperability standard initiatives including; Berlin Group, UK Open Banking, STET etc. All with the objective to accommodate the risk of a highly fragmented marked of TPP (third party provider) access interfaces.

Berlin Group and UK Open Banking are among the most adopted standard initiatives across the EU. Though these standards still call for various interpretations creating fragmented solutions across the different banks (ASPSP – account servicing payment service providers).

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

So, does this really meet the objective of a single EU market in retail payments? And how does PSD2 meets the objectives of enhanced competition, innovation, consumer protection and increased security? These are obviously objectives created with the customer in focus, though it can seem challenging to meet those objectives with requirements open for interpretation. This will require TPPs and banks to collaborate and have a mutual approach in order to create a solution that will benefit the end customer, as security and usability are not famous for being soul mates.

A walk down a bumpy road

Today TPPs gain access to information services of the banks through so called screen scraping. Screen scraping is where a TPP application uses customer (PSU – payment service user) credentials to access transaction data for a specific purpose, approved by the customer. This is often used to aggregate an overview of the customer's accounts held at different banks and to access information about transactions.

When the RTS comes into force in September 2019 the banks must develop a TPP access interface that complies with article 30(1) in the RTS. According to the RTS the bank will have two options for a TPP access interface (RTS, art. 31):

- **Dedicated interface:** a new developed interface specifically for the TPPs, based on ISO 20022 standards. This is the option that most banks are opting for and will in most cases be based on REST APIs.
- **Existing customer interface:** The bank reuses an already existing customer interface - could be the 'web bank', though enabling the TPP to identify themselves towards the bank (RTS, art.30(1))

A third option is a fallback solution. If the bank does not manage to develop a dedicated interface that comply with the contingency measures set out in article 33(6) of the RTS, a fallback solution is required. But what is required from a fallback solution, is not specified further than this:

"As part of a contingency mechanism, payment service providers referred to in Article 30(1) shall be allowed to make use of the interfaces made available to the payment service users for the authentication and communication with their account servicing payment service provider, until the dedicated interface is restored to the level of availability and performance provided for in Article 32" (RTS, art. 33(4)).

This does not explicitly out-rule screen scraping, but as you need to perform SCA (strong customer authentication), screen scraping will not be a viable option on

payment information, from September 2019 ((EU) 2015/2366, PSD2, art. 97). Though screen scraping will still be a viable option on other, not yet regulated, financial information services, thereby enabling TPPs to continue screen scraping in other areas than payment information.

Today several TPPs has built their product and user experience (UX) around the screen scraping process. With PSD2, and the RTS coming into force in September 2019, the TPPs will now have to access data through a PSD2 compliant bank interface. But will they still be able to offer a customer journey without any big bumps in the road, as they have been able to do it through the screen scraping solution?

SCA exemptions

It could very much be argued that *strong customer authentication* goes against current payment trends, where the customer journey should be as smooth as possible to create a frictionless user experience.

Several areas exist where SCA will increase friction throughout the customer journey. Many banks are developing a redirect solution for performing SCA. This means that if the customer has accounts at three different banks it will be redirected away from the TPP application to perform SCA at the bank interface, three times, in order to authorize that the TPP can access their payment data at every account provider.

Though exceptions for performing SCA exists. But it is up to the bank to decide whether or not to provide exemption to SCA or not: "'*The personalized security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers'…the PSP applying SCA is the PSP that issues the personalized security credentials. It is consequently also the same provider that decides whether or not to apply an exemption in the context of AIS and PIS.*" (EBA Opinion on SCA and CSC, para 37-38).

This means that EBA has made SCA exemptions depended on goodwill from the bank. It can fairly be questioned if this is to be considered sustainable competition.

Following areas are subject to SCA exemption (EBA Opinion on SCA and CSC, p. 9):

Table 2. Summary table on who may apply an exemption

RTS article	Exemption	Payer's PSP	Payee's PSP	
			Credit transfers	Cards
Access to information	Access to payment account information	Yes	N/A	N/A
Article 11	Contactless payments at POS	Yes	No	Yes*
Article 12	Unattended terminal for transport and parking	Yes	No	Yes*
Article 13	Trusted beneficiaries	Yes	No	No
Article 14	Recurring transactions	Yes	No	Yes*
Article 15	Credit transfers to self	Yes	No	N/A
Article 16	Low-value transactions	Yes	No	Yes*
Article 17	Secure corporate payment processes and protocols	Yes	No	N/A
Article 18	Transaction risk analysis	Yes	No	Yes*

*The payer's PSP always makes the ultimate decision on whether or not to accept or apply an exemption; the payer's PSP may wish to revert to applying SCA to execute the transaction if technically feasible or decline the initiation of the transaction.

One important possible exemption is the one based on 'trusted beneficiaries'. If this is supported by the bank, the TPP could be able to provide a payment solution where the customer will not have to perform *strong customer authentication* if the payment is targeted a 'trusted beneficiary'. This list of 'trusted beneficiaries' is controlled in the bank's interface and can thereby not be accessed by the TPP. But this function could be a critical function for many TPPs initiating payments, as this would enable them to offer the famous 'one-click'- buy solution without the customer having to authenticate through a redirect solution at the bank interface.

This dependency on bank goodwill has a risk of causing high fragmentation of UX across different banks, as some might offer this as an exemption and others won't. This will make it troublesome for TPPs to communicate to customers, as some customers will have to provide SCA when initiating a payment and others won't, as their bank offers the 'trusted beneficiaries' exemption. This will also make it difficult for TPPs to brand their product, as their UX will be dependent on the different bank solutions.

Strong customer authentication is just one of the areas that can cause bumps in the customer journey, there are several other areas that also calls for attention;

- *Consent management*: who and how is the consent managed, can vary from one bank to another again causing a fragmented user experience for the customer, depended on their affiliated bank.

- *Rate transparency:* Is this transparent only to the customer at the bank interface or is it also communicated to the TPP? This can vary from the different banks making it difficult for the TPP to set prices and to provide sufficient and transparent communication around rates to their customers.

- *payment types:* Not all banks will support the same payment types which could make it challenging for the TPP when requesting a payment to be initiated on behalf of the customer. If the requested payment type is not supported by the bank the payment will be rejected and thereby create yet another bump in the road for the customer.

It can be strongly questioned if this dependency, on bank solutions, is meeting the objectives of enabled competition, integrated EU payment market and innovation. You can argue that this will directly limit TPPs' ability to develop independent and innovative solutions.

Approaching PSD2 in isolation, without any strategy around open banking, is mainly a cost for the banks. It can thereby be encouraged that the banks have a strategy of how to approach Open Banking in order to offer services beyond PSD2 with the purpose of; creating new business models, new revenue streams and to keep themselves competitive in the future. An option also to be considered by the banks is to act as a TPP themselves, as this would give them great insights and incentives to create PSD2 interfaces that will enable a customer journey without any unnecessary bumps in the road.

The banks should design a solution that accounts for these inappropriate bumps in the road, making it easier for the TPP to create a product with transparency around rates, sufficient error messages, consent management etc. The banks should provide some goodwill in their PSD2 solution thereby offering a competitive service enabling the TPP to build customer products with a high level of UX.

Conclusion

It is clear that the objective with PSD2 is centered around the customer, in order to provide them with improved, greater variance, and more safe payment solutions. From only looking at the objectives the bar is set high, though the requirements from the EBA does not reflect that picture. It is obvious that PSD2 is a rough diamond, that will need some extra polish to truly shine and meet those objectives. The EBA has made the technical standards open in the hopes of seeing new and innovative solutions with great collaboration across the market,

but it instead seems to cause unneeded fragmentation, calling for increased regulatory support for convergence on the technical standards.

This is an encouragement for the banks and TPPs to bring the customer in focus when developing their solution. It is a possibility for the banks to go beyond the PSD2 requirements and exploit various business opportunities within Open Banking. The TPPs should have a greater voice in the push for the banks to develop TPP access interfaces that will enable customer friendly products.

It can be strongly assumed that PSD2 will be followed by a regulatory push towards open banking, not limited to simple payment products in the future. For all parties to benefit, PSD2 should be attacked with a long-term strategy of how to provide value to the end customer in order to reserve a spot in the future field of fintech.

References

RTS, regulatory technical standards for strong customer authentication and common and secure open standards of communication, COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017, Official Journal of the European Union, Published 13. March 2018

PSD2 Directive (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015, Official Journal of the European Union, Published 23. December 2015

Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC, EBA-Op-2018-04, Published 13. June 2018

Consultation Paper, Draft Guidelines on the conditions to be met to benefit from an
exemption from contingency measures under Article 33(6) of Regulation (EU) 2018/389 (RTS on SCA & CSC), EBA/CP/2018/09, Published 13. June 2018

Open Banking APIs Under PSD2 – Security Threats and Solutions, White paper, One Span, April 2018