Complior

Whitepaper

PSD2

What are the implications, problems, possibilities, challenges and opportunities

Intro

The growth of internet payments and a rapid evolving fintech sector in the European market has caused the European Union to revise their Payment Service Directive (PSD). The new directive, that will effectively replace the PSD, is conveniently called PSD2. The deadline for member states to transpose PSD2 into national legal and regulatory frameworks is 13 January 2018. The PSD2 has already managed to cause a big stir in the European banking and payment service sector. Greater legislation and governance requirements are coming soon.

What are the objectives of the PSD2?

Like its predecessor, the PSD2 aims to harmonize internet payments across the European space, increasing the scope and ambition of the previous directive. The PSD2 has a stronger focus on consumer security and is opening the payment service market for so called Third Party PaymentService Providers (TPPs).

These are the most fundamental changes of PSD2:

» Third party Access to Accounts (XS2A)
» Prohibited surcharging
» Enforced two factor authentication

As a whole, the PSD2 aims to push for more innovative payment services by enforcing regulations that will increase the competition and security of payment services.

The third party providers

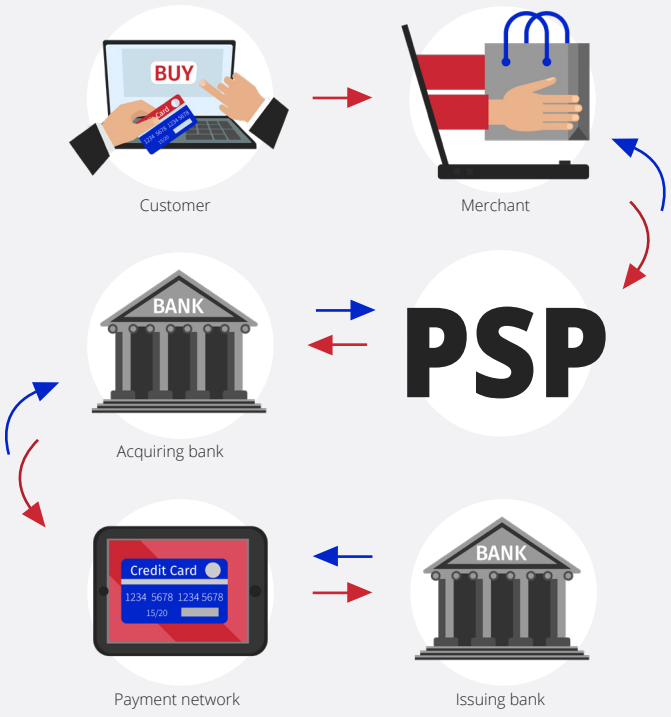
Since the PSD was adopted in 2007, new services have emerged in the area of internet payments. So called Third Party Payment Service Providers (TPPs) offer specific payment solutions or services to customers. These TPPs are a new category of Payment Service Providers (PSPs) which are divided into Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) respectively.

Account Information Service Providers provide services to consumers that let them see an overview of their financial situation between multiple banks. The AISPs typically offer services that help consumers analyze their spending patterns, expenses and financial needs, all in a user-friendly manner.

Payment Initiation Service Providers act as a link between a payer's bank account and a merchant's banking platform.

Today, there are several PISPs active in the European market such as Sofort, IDeal and Trustly. Imagine a pre-PSD2 scenario where you would like to buy products from two different online merchants. In order to complete a purchase, you have to fill in your personal details and credit card information on both sites, often entailing an additional authentication measure administered by your card issuer. Before the purchase is completed, the card data has to travel between PCI intermediaries. (Figure 1)

Figure 1: Pre PSD2



Now let's look at how a post-PSD2 scenario can play out.

The first time, you (the customer) must give permission to a PISP to access your bank account. The next time you make a purchase online you just access your bank account with your PISP through the merchant website, use your bank login, and the PISP will make a direct debit from your account. No need to provide the merchant with any card data or personal details. This transaction process is made in real-time, meaning that the transfer of money between the consumer's bank account to the merchant's bank account is instant. As seen in the illustration (Figure 2), there is no longer any need for an acquirer or a payment network, so there is no interchange fee to account for.

The PISPs will essentially provide the same services as the payment card institutions, but without the need for acquirers and the payment network. Merchants will like the payment model that the PISPs operate from, since they will not have to pay any interchange fee to an acquirer. Consumers might also benefit from this as it may cause merchants to lower prices, unless the merchants simply keep the increased profit margin.

Figure 2: Post PSD2

How is the PSD2 opening the market for these new TPPs?

Until now, entering the market of financial services was complicated for TPPs, as their solutions required access to consumer bank accounts. Not all banks have been very cooperative with TPPs since they are often in direct competition with the financial services the banks offer. This leads us to the most controversial and most debated issue of the PSD2, Third party Access to Accounts (XS2A).

With PSD2, banks are forced by law to give TTPs access to customer accounts if the customer has given their consent.

The TPPs will gain this access through an Application Programming Interface (API). An API is a software-to-software interface that allows web-based applications to communicate with each other and share data. Have you ever been to a website that has presented you with the option to login using your Facebook account? These websites are in fact making use of Facebook's open API. The TPP's access to the bank's API is referred to as Third party Access to Accounts (XS2A) in the directive, and will have huge implications on businesses and banks alike.

Prohibited surcharging

In 2015, the European regulation on interchange fees (Regulation (EU) 2015/751) was enforced. The regulation imposed interchange fee caps on card-based transactions within the European Economic Area (EEA) at 0.2% for debit cards and 0.3% for credit cards respectively. Before the interchange fee caps were enforced, interchange fees varied considerably between member states in the EEA. They were often grossly higher than the current caps, which upset many merchants.

Even though the interchange fees became significantly lower, some merchants still insisted on surcharging customers in order to off-set some of the costs related to interchange fees. Surcharging refers to when merchants charge customers extra for paying with debit or credit cards; airlines are notorious for surcharging customers who use payment cards, for instance. When the PSD2 is enforced, surcharging will not be allowed for those consumer cards affected by the Interchange fee cap (roughly 95% of all payment cards in the EEA). Considering the reduction of the interchange fee, it would be unreasonable for merchants to charge their customers extra for accepting payments using these cards.

The Problems with the PSD2

Many European banks are faced with a big challenge because their role in internet payments as an intermediate is being both questioned and threatened. They must also make radical changes in their IT-environments in order to comply with the PSD2. The problem is that many banks use old legacy systems and not modern IT-architecture like that of the Service Oriented Architecture (SOA). Providing the necessary API's for the TPPs might therefore be difficult. The API's will also be an additional security issue for banks to take into consideration as they provide the services to see and transfer money from customer accounts.

On the other hand, some TTPs are worried about the XS2A since it is vaguely defined in the directive and the European Banking Authority (EBA) guidelines. The EBA is currently in the process of drafting standards and guidelines as to how the directive should be implemented technically. Trustly's CEO, Oscar Berglund, is one of many that has raised concerns regarding the XS2A and how it is formulated in the proposed EBA guidelines. Today, already established TPPs like Trustly use the same APIs as the banks for their own services. The problem is that the guidelines can be interpreted in a way that will force TPPs to have their own separate APIs. The banks will have no incentive to make these separate APIs work properly, and can instead focus on their own APIs, thus improving the availability for their own services and neglecting the competition. This will give the banks a lot of power over competing players. The PSD2 may in fact have an opposite effect when it comes to increasing the competition in the European market.

Security of PSD2

With the PSD2 enforced, Payment service providers will have to apply so called strong customer authentication (SCA) when a customer initiates an electronic payment transaction. Strong customer authentication is what the directive basically calls two-factor authentication (2FA). One-factor authentication typically just requires the customer to type in a username and password to validate their identity.

Two-factor authentication requires at least two of the following parameters to be present during authentication:

» Something you know (e.g. username, password, PIN)

» Something you possess (cellphone, card or authentication code generating device)

» Something you are (biometrics authentication such as the use of fingerprints, voice recognition and retinal scanner)

2FA is a big improvement from a security standpoint.Passwords can be easily cracked or stolen from a database, but simultaneously stealing the same target's fingerprints or cellphone is much harder.

How will the payment card industry cope with PSD2?

Firstly, it is clear that card brands are starting to diversify their payment flows. MasterCard, for instance, has recently acquired VocaLink – the biggest payment processor in the United Kingdom that receives 90% of its revenue from non-card payments. There is also a recent trend where fintech companies are purchasing both PSPs and acquirers so that they can merge the institutions to streamline the payment flow, e.g., Bambura, Braintree, and Stripe. All to make their payment service cheaper compared to having two separate contracts with a PSP and an acquirer. This will give these payment processors a greater edge when it comes to adapting to the interchange fee cap.

Smartphones have become a large part of our daily lives, and the companies that manage to conquer the mobile payment service market will make tremendous amounts of money for a long time to come. Card brands like Visa, MasterCard and American Express are now working together with Apple on establishing Apples mobile payment application Apple Pay. Apple Pay offers a revolutionary way of providing payment card transactions:

» Payment initiation is quick and secure, using 2FA by combining Touch ID (finger print sensor) and password.

» Cardholder data such as the Primary Account Number (PAN) is exchanged with a token from the payment network.

» Near Field Technology (NFC) for point-of-sales transactions.

Customers want payments to be quick and easy. With Apple's Touch ID, 2FA will be fast and easy and makes the payment application already PSD2 compliant in this regard. Although not within the scope of PSD2, Apple Pay uses Near Field Technology to make purchases very fast at physical stores. Customers simply have to put their IPhone near a payment terminal for the tokens to be transmitted through radio waves to the terminal, completing the purchase in a matter of seconds.

The payment networks (VISA, MasterCard, Amex etc.) are providing tokenization services for Apple Pay and have established their own token vaults. Tokenization is a relatively old technique, but the payment card institutions have recently opened their eyes to this simple, yet very effective technique. Tokenization works in essence by substituting valuable or sensitive data with non-valuable surrogate equivalents, i.e., tokens. For example, in the physical world we use tokens in the casino when we replace money with casino chips.

With Apple Pay, the cardholder data such as the Primary Account Number (PAN) and expiration date are not sent when a customer initiates a payment with a merchant.Instead, tokens replace the cardholder data until the payment flow reaches the payment network. Only now do the tokens get replaced with the real cardholder data from the payment network's tokenization vault. This greatly enhances the confidentiality of payment card transactions. Apple Pay and similar payment applications are the future of payment card transactions.

Closing Words

The PSD2 will certainly be a game changer in the European fintech industry and banking sector. It will be enforced shortly before another major revised directive, the General Data Protection Regulation (GDPR). Administrative pressure on banks and payment service providers will be immense in 2018. Will the EU manage to streamline online payments and improve competition in the European market? Or have they opened a Pandora's box that will cripple the European market with overregulation?